A product of the C2M2 Program

Energy Sector Cloud Cybersecurity Profile

Version 1.0

September 2026

U.S. DEPARTMENT of ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

DISCLAIMER

This work was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or any third party's use or the results of such use of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof or its contractors or subcontractors. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof, its contractors or subcontractors.

This guidance is not intended to replace or subsume other cybersecurity-related activities, programs, processes, or approaches that organizations have implemented or intend to implement, including any cybersecurity activities associated with legislation, regulations, policies, programmatic initiatives, or mission and business requirements. Additionally, this guidance is not part of any regulatory framework and is not intended for regulatory use. Rather, the guidance in this publication is intended to complement a comprehensive enterprise cybersecurity program. Please consult your compliance authority for any questions on regulatory compliance.

Artificial intelligence (AI) technologies were used in a limited capacity during development of this document. The content in this document is based on collaborative research, analysis, and review performed by government, technology-sector, and energy-industry cybersecurity practitioners. All content was reviewed by a human author prior to publication.

EXECUTIVE SUMMARY

Energy sector organizations increasingly face pressure to integrate cloud technologies into their operational technology (OT) environments. Cloud technologies can provide efficiency, scalability, and resilience benefits. At the same time, vendors are using cloud-based delivery models for products that support OT functions. These factors may make cloud integration a strategic opportunity, an operational need, or both.

Cloud integration represents a significant shift for OT environments. These environments have historically relied upon strong segmentation and isolation from the internet to support secure, safe, and reliable operations. Cloud integration can fundamentally change these environments by introducing significant dependencies on external connectivity and third-party services. It can also change who is responsible for key cybersecurity activities.

The Energy Sector Cloud Cybersecurity Profile (the Profile) provides practical guidance for navigating this shift. It does not assume that cloud integration is appropriate for every OT use case. Instead, it helps energy organizations make informed, risk-based decisions about cloud integration while maintaining the safe and reliable operations that our communities, infrastructure, and daily lives depend on. The Profile combines a four-step implementation lifecycle with guidance organized around the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0. It addresses potential risks introduced by cloud integration, cloud-specific considerations for OT environments, example mitigating controls, and informative references to related standards and frameworks.

The Profile was developed by a working group of representatives from energy sector owners and operators, cloud and technology providers, government departments and agencies, and national laboratories. This team brought together operational, cybersecurity, engineering, policy, and research perspectives. This guidance was developed in support of the U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response (DOE CESER) goal of strengthening the security and resilience of U.S. energy infrastructure.

The Profile is intended for use primarily by cybersecurity and OT practitioners, but it also informs procurement, compliance, risk, and leadership stakeholders. Applying the Profile can help an organization produce a documented cloud integration decision, defined requirements, implementation and risk management plans, and processes for ongoing monitoring and improvement. These results can help energy organizations use cloud capabilities where appropriate while maintaining the safety, reliability, and resilience of the systems that support energy delivery.

TABLE OF CONTENTS

Disclaimer ii
Executive Summary iii
Table of Contents iv
1 INTRODUCTION 6
1.1 Structure of This Document 6
2 HOW TO USE THE PROFILE 8
2.1 Step 1: Evaluate 8
2.1.1 Engage Stakeholders 9
2.1.2 Define the Problem or Opportunity 9
2.1.3 Analyze Options 10
2.1.4 Select an Option 11
2.2 Step 2: Plan 12
2.2.1 Define Requirements 12
2.2.2 Develop a Risk Management Plan 12
2.2.3 Develop an Implementation Plan 13
2.2.4 Build Consensus with Stakeholders 13
2.3 Step 3: Implement 13
2.3.1 Execute the Implementation Plan 14
2.3.2 Test and Validate 14
2.3.3 Transition to Operations 14
2.4 Step 4: Maintain 15
2.4.1 Monitor and Improve 15
2.4.2 Mature Processes 15
3 RISKS AND MITIGATIONS 16
3.1 Govern (GV) 17
3.1.1 Organizational Context (GV.OC) 17
3.1.2 Risk Management Strategy (GV.RM) 23
3.1.3 Roles, Responsibilities, and Authorities (GV.RR) 30
3.1.4 Policy (GV.PO) 37
3.1.5 Oversight (GV.OV) 40

3.1.6 Cybersecurity Supply Chain Risk Management (GV.SC) 43
3.2 Identify (ID) 58
3.2.1 Asset Management (ID.AM) 58
3.2.2 Risk Assessment (ID.RA) 71
3.2.3 Improvement (ID.IM) 88
3.3 Protect (PR) 97
3.3.1 Identity Management, Authentication, and Access Control (PR.AA) 97
3.3.2 Awareness and Training (PR.AT) 110
3.3.3 Data Security (PR.DS) 114
3.3.4 Platform Security (PR.PS) 123
3.3.5 Technology Infrastructure Resilience (PR.IR) 138
3.4 Detect (DE) 147
3.4.1 Continuous Monitoring (DE.CM) 147
3.4.2 Adverse Event Analysis (DE.AE) 159
3.5 Respond (RS) 170
3.5.1 Incident Management (RS.MA) 170
3.5.2 Incident Analysis (RS.AN) 179
3.5.3 Incident Response Reporting and Communication (RS.CO) 186
3.5.4 Incident Mitigation (RS.MI) 189
3.6 Recover (RC) 194
3.6.1 Incident Recovery Plan Execution (RC.RP) 194
3.6.2 Incident Recovery Communication (RC.CO) 204
Appendix A: Future Considerations 209
Appendix B: Glossary 212
Appendix C: List of Abbreviations 218
Appendix D: References 223
Appendix E: Bibliography 227
Appendix F: Acknowledgements 231

1 INTRODUCTION

This document—the Energy Sector Cloud Cybersecurity Profile (the Profile)—was developed to provide sector-specific guidance that supports cybersecurity risk management during the integration of cloud technologies into operational technology (OT) environments. It includes potential risks, example mitigating controls, and key considerations for energy organizations planning and implementing secure cloud integrations with OT environments.

The Profile focuses on OT capabilities that rely on externally provided cloud services. One or more third parties operate the infrastructure or service components supporting these capabilities, often including a public cloud provider. The Profile addresses two common ways organizations use these services. In the first, the organization acquires public cloud services, such as infrastructure as a service (IaaS) or platform as a service (PaaS). The organization then configures and operates its own OT workloads on these services. In the second, the organization acquires a cloud-based service or tool from a vendor, such as a software as a service (SaaS) OT application. These vendor offerings may themselves rely on infrastructure and services supplied by another cloud provider. Both approaches create dependencies on external connectivity and third-party services and allocate some cybersecurity responsibilities to external providers. The organization remains responsible for understanding these dependencies and managing the responsibilities and risks that remain with it.

The Profile was developed by a working group that included representatives from energy sector owners and operators, cloud and technology service providers, government departments and agencies, and national laboratories. The working group brought together operational, cybersecurity, engineering, policy, and research perspectives to address cloud integration in OT environments.

The Profile is organized based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) [NIST 2024a]. The guidance in the Profile was developed to support the U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response (DOE CESER) goal to strengthen the security and resilience of the U.S. energy sector and harden the U.S. energy infrastructure [CESER 2026].

1.1 Structure of This Document

The Profile has two primary components:

- ***How to Use the Profile*** A high-level process for evaluating, planning, implementing, and maintaining cloud technologies in OT environments.
- ***Risks and Mitigations*** Potential risks and example mitigations, organized by NIST CSF Subcategories along with informative references to related frameworks and standards.

The Profile is also available in spreadsheet and website formats at https://cloudcybersecurityprofile.pnnl.gov/. Please send comments, corrections, and suggestions to C2M2@doe.gov with "Cloud Profile Feedback" in the subject line.

Organizations translating these NIST CSF Subcategories into technical architectures and implementation plans may also benefit from consulting other related cloud security resources. For example, the Cybersecurity and Infrastructure Security Agency's (CISA) Secure Cloud Business Applications (SCuBA) resources provide secure configuration baselines, assessment guidance, and automation resources for select software as a service (SaaS) business application environments [CISA 2026]. Also, the National Laboratory of the Rockies' (NLR's) CloudZero project examines the reliable and secure use of cloud technologies to support complex energy systems and OT use cases, including technical, operational, and risk considerations [Wallace 2024].

2 HOW TO USE THE PROFILE

This section describes a process for using the Profile to support the secure integration of cloud technologies into OT environments. It highlights important activities for planning, implementing, and maintaining cloud technologies that support OT functions. The specific application of this process varies significantly from organization to organization.

At a high level, the process involves four steps:

- ***Evaluate*** Decide whether and how to pursue a cloud-supported capability before committing resources.
- ***Plan*** Turn the selected option into an actionable implementation and risk plan with stakeholder consensus.
- ***Implement*** Execute the plan, validate that controls work as intended, and transition the capability into operations.
- ***Maintain*** Monitor the capability in operation and mature initial processes into repeatable procedures.

Figure 1 identifies each step in the process.

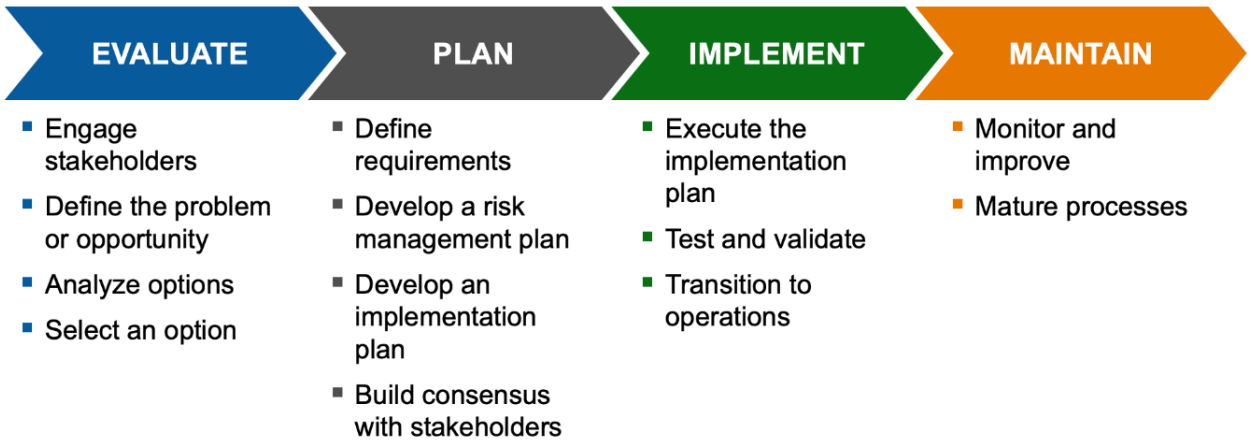


Figure 1: Steps in the Process for Using the Profile

2.1 Step 1: Evaluate

Figure 2: Evaluate—Steps in the Process for Using the Profile

This step supports deciding whether and how to pursue a cloud-supported capability before committing resources. It involves engaging stakeholders, defining the problem or

opportunity driving the effort, and analyzing options against the organization's mission, goals, operational requirements, risk tolerance, and regulatory obligations. The step concludes by selecting an option through a formal go or no-go decision. To weigh each option, review the *Potential Risks and Considerations* described in Section 3 to inform problem definition, option analysis, and option selection.

2.1.1 Engage Stakeholders

Many individuals or groups may provide useful input to the evaluation process. Consider when to engage stakeholders and how to capture and adjudicate their feedback. Use the cloud customer and cloud provider roles identified in the *Potential Risks and Considerations* and *Example Mitigating Controls* in Section 3 to help conceptualize which responsibilities apply and how to share them. Organizations may seek input from stakeholders who represent internal functions such as the following:

- Cybersecurity
- Security Operations Center
- Operations and Engineering
- Operational Technology
- Information Technology
- Cybersecurity Threat Intelligence
- Enterprise Risk Management
- Business Continuity and Disaster Recovery
- Legal
- Compliance
- Internal Audit
- Procurement
- Human Resources
- Finance
- Facilities Management
- Physical Security

2.1.2 Define the Problem or Opportunity

Prepare and document an analysis that explains why a change may be necessary. The reason may be to solve a problem or seize an opportunity. External factors, such as a vendor moving a product from on-premises deployment to cloud hosting, may drive the change. Internal initiatives that assess whether cloud technology could provide operational or cost benefits may also drive it. This analysis helps decision makers understand the value of the proposed change. Start by documenting the current situation. Then define the problem or opportunity, focusing on potential impacts on the organization's mission and goals. Identify, at a high level, the potential risks, costs, and

benefits of making a change. Use the *Potential Risks and Considerations* in Section 3 to help identify the risks that may arise when integrating cloud technology into OT environments. Include high-level descriptions of potential options and supporting information, such as the organizational functions, systems, data, users, and processes that may be affected.

2.1.3 Analyze Options

Perform and document an *options analysis* that compares different ways to address the problem or opportunity. This analysis helps decision makers understand and select the option most aligned with the mission and goals of the organization.

Begin by identifying the different options that could address the problem or opportunity. Options may include alternative service models, cloud providers, or architectures (using the status quo as a baseline). Consider a range of options and actively work to identify and avoid potential bias or premature focus on a specific option.

For each option, identify the costs, risks, and benefits it presents. Consider what other background information or evaluation criteria may be useful. Use the *Potential Risks and Considerations* and *Example Mitigating Controls* in Section 3 to help identify potential risks and benefits of options that include cloud technology. The following subsections provide example considerations, such as resilience requirements and legal obligations, to help evaluate each option.

2.1.3.1 Resilience Requirements

Create an inventory of key resilience requirements for the organization. Consider how each option may affect safe and reliable operations during normal and degraded conditions. Determine how a degraded or unavailable capability under each option could affect the organization's essential functions. Consider whether the emerging technologies or dependencies described in Appendix A may change availability, failover, restoration, or degraded-mode operating assumptions.

Assess existing resilience measures, such as manual processes, backup solutions, and recovery processes, and determine the potential changes required to enable the organization to maintain its essential functions and recover them within acceptable timeframes. Use the *Potential Risks and Considerations* and *Example Mitigating Controls* in Section 3 to identify how integrating cloud may affect existing processes.

2.1.3.2 Legal Obligations and Stakeholder Expectations

Evaluate the legal, regulatory, contractual, and customer-specific obligations for each option. Consider requirements for data handling, data location, auditability, access to evidence, incident notification, reliability, safety, and service continuity. For regulated systems, the organization may need to determine whether the proposed cloud architecture affects compliance obligations or requires engagement with legal,

compliance, or regulatory stakeholders. Understanding these obligations early also shapes who needs to be involved. Some requirements may trigger legal review, regulatory engagement, or supplier coordination that the organization should initiate before completing the evaluation.

Identify the internal and external stakeholders affected by each option. Internal stakeholders may include operations, engineering, cybersecurity, procurement, legal, compliance, enterprise risk management, and executive leadership. Use the *Potential Risks and Considerations* and *Example Mitigating Controls* in Section 3 that focus on cloud customer and cloud provider responsibilities to identify how responsibilities will be shared among stakeholders. External stakeholders may include customers, regulators, reliability coordinators, service providers, and other parties that depend on the organization's critical services.

2.1.3.3 Risk

Evaluate the risks associated with each option. This evaluation identifies and prioritizes new risks as well as any changes to existing risks that each option introduces. Consider how shared responsibility, external dependencies, and changes in control ownership may affect risks. Use the *Potential Risks and Considerations* in Section 3 to support brainstorming about the potential risks associated with cloud integration. Analyze and document areas where existing staffing capacity, expertise, tools, and funding may not be sufficient to manage the risks associated with each option.

2.1.3.4 Suppliers and Dependencies

Identify the cloud providers, OT vendors, managed service providers, and upstream dependencies that may support each option. Evaluate the criticality of each supplier and the potential operational impact of a supplier disruption. Use Section 3 to explore the roles and responsibilities of cloud providers. New or updated contracts and service agreements may need to address security expectations, service levels, information sharing, incident notification, restoration support, data return, termination, and transition planning.

2.1.4 Select an Option

Use the information captured in the options analysis to select an option or determine that no change is needed at this time. This formal analysis and go or no-go decision step helps ensure that the organization has applied due care before committing further resources to changing an existing process.

To reach a decision, compare the analyzed options against the costs, risks, benefits, and evaluation criteria identified in the analysis. Weigh how each option performs against these criteria and against the organization's mission and goals. Document the decision, supporting rationale, key assumptions, and any important follow-up actions.

Consider what components from the analysis, such as identified risks, will inform subsequent planning.

2.2 Step 2: Plan

Figure 3: Plan—Steps in the Process for Using the Profile

This step focuses on developing an actionable plan for implementing the selected option. It involves defining requirements, developing a risk management plan, developing an implementation plan, and building consensus with stakeholders before work begins. The *Potential Risks and Considerations* and *Example Mitigating Controls* in Section 3 can help inform requirements, risk identification, and the actions expected of cloud customers and cloud providers.

2.2.1 Define Requirements

Identify the requirements for the implementation project. Requirements explain what the project plans to accomplish and what it plans to avoid. Start with the inventory of key resilience requirements developed in the Evaluate step. Consider other information from the Evaluate step, such as identified risks, assumptions, cost and benefit considerations, and the evaluation criteria used to compare options. Use the *Potential Risks and Considerations* and *Example Mitigating Controls* in Section 3 to identify cloud-specific considerations to incorporate into requirements.

Develop requirements collaboratively with the stakeholders and subject matter experts (SMEs) who own the affected OT functions. It may be useful to distinguish *must-have* requirements from *nice-to-have* requirements. Also capture constraints (conditions the implementation must work within), including regulatory obligations, operational limits, shared-responsibility boundaries, the cloud provider's upstream dependencies, budget, and schedule.

Requirements define what the implementation plan should address. Elements that leadership may require in the plan include a description of the proposed integration approach, affected systems and processes, new or updated cybersecurity controls, shared responsibility considerations, potential operational impacts, the cloud provider's upstream dependencies, and unresolved risks that require leadership review.

2.2.2 Develop a Risk Management Plan

Identify potential risks to the organization's mission and goals that may arise from the implementation project. Include safety and reliability risks to OT operations and the

implementation project itself, such as cost, staffing, and technical risks. Use the *Potential Risks and Considerations* identified in Section 3 to support risk identification.

For each risk, select a response (such as accept, avoid, mitigate, share, or transfer) and assign a risk owner who is accountable for carrying it out. Involve organizational leadership and project stakeholders in identifying risks and selecting risk responses. Review risks and responses throughout the implementation process as conditions change, new risks emerge, and responses take effect. Cybersecurity risks warrant particular scrutiny in processes supported by cloud technology. Shared responsibility boundaries, evolving attack surfaces, and changes to identity, data flows, and monitoring may introduce exposures that are easy to overlook.

2.2.3 Develop an Implementation Plan

Define how the organization will execute the project. Consider how to manage cybersecurity, operational, compliance, and supplier-related considerations. Use the *Potential Risks and Considerations* and *Example Mitigating Controls* in Section 3 to help identify the actions required by both the cloud customer and the cloud provider. The level of detail for the plan should be proportional to the criticality of the affected organizational functions and the complexity of the project.

At a minimum, the plan should address the major activities needed to integrate the cloud-supported capability and how the organization will maintain safe and reliable operations during implementation. Define local methods the organization will use to sustain operations if the capability is degraded or unavailable. Establish acceptance criteria and identify who has authority to approve implementation decisions and transition to operations. Also consider and plan for the operation and maintenance phase, including additional staff, tools, process documentation, and training.

2.2.4 Build Consensus with Stakeholders

Organizational leadership, risk owners, and other stakeholders review the plan and provide input to improve it. Use the *Potential Risks and Considerations* and *Example Mitigating Controls* in Section 3 to help inform stakeholders about the unique risks and considerations related to integrating cloud technology into OT environments. Document the decision, rationale for updates to the plan, and final approval.

2.3 Step 3: Implement

Figure 4: Implement—Steps in the Process for Using the Profile

This step executes the implementation plan and validates that the cloud-supported capability is ready for use. It includes executing the plan; testing and validating that assets, processes, and cybersecurity controls function as intended without introducing new risks; and transitioning the capability from a development, test, staging, or other non-production environment into operations. The *Potential Risks and Considerations* and *Example Mitigating Controls* in Section 3 can help inform testing plans to confirm that capabilities and controls operate as expected before transitioning to a production environment.

2.3.1 Execute the Implementation Plan

Execute the implementation plan by coordinating with appropriate stakeholders, such as OT, engineering, cybersecurity, IT, operations, and suppliers. Where feasible, implement and configure the capability in a development, test, staging, or other non-production environment before moving it into operations. Apply change management processes to manage the plan, implementation activities, and decisions.

2.3.2 Test and Validate

Test changes to determine whether assets and processes function as intended, satisfy defined security and resilience requirements, and introduce identifiable risks or unintended effects. Document residual uncertainty and monitor the change after deployment.

Use the *Potential Risks and Considerations* and *Example Mitigating Controls* in Section 3 to help develop test plans. Test that cybersecurity controls operate as expected. For example, confirm that logs are available at the needed level of detail, alerts are generated for defined events, access controls restrict access appropriately, backups are created, and restoration processes work as intended. Document test results and provide this information to OT system owners and other designated stakeholders. Confirm that supplier coordination processes and supporting information are ready for use, including incident notification, escalation paths, support contacts, evidence sharing, and restoration coordination.

Confirm that operations, engineering, cybersecurity, and support teams are ready to operate, monitor, and support the capability. Assign or confirm roles and responsibilities for ongoing operation, monitoring, supplier coordination, incident response, and recovery. Develop or update policies, procedures, playbooks, architecture records, inventories, data flow diagrams, and other documentation needed to support operations.

2.3.3 Transition to Operations

Obtain approval from OT system owners and other designated stakeholders before transitioning the cloud-supported capability from the development, test, staging, or other non-production environment into the operational environment. For important operational processes, consider additional controls to help avoid potential problems. These controls

may include additional review, increased coordination, rollback procedures, and heightened monitoring during the initial stages of live operation.

2.4 Step 4: Maintain

Figure 5: Maintain—Steps in the Process for Using the Profile

This step addresses how the organization operates, monitors, and improves the cloud-supported capability after it enters service. It involves monitoring cybersecurity, operational performance, and risk conditions. It also involves maturing initial processes into repeatable, well-documented procedures with clear ownership and training. The *Potential Risks and Considerations*, *Example Mitigating Controls*, and *Informative References* in Section 3 help identify what to monitor and which administrative controls may help increase long-term process maturity.

2.4.1 Monitor and Improve

Integrate monitoring of the cloud-supported capability into existing cybersecurity, operational, supplier management, and risk management processes. Use the *Potential Risks and Considerations*, *Example Mitigating Controls*, and *Informative References* in Section 3 to identify which processes and controls may require additional monitoring. Consider how to apply monitoring to cloud providers, OT vendors, managed service providers, and other upstream providers.

Track incidents, near misses, supplier performance issues, control gaps, operational impacts, and lessons learned. Update procedures, risk documentation, supplier oversight practices, and other controls as needed. Use lessons learned to improve future cloud integration efforts and inform updates to governance, risk management, and planning practices.

2.4.2 Mature Processes

As the new cloud-supported capability stabilizes, evolve the initial processes established during implementation into repeatable, well-documented procedures consistent with other procedures across the organization. Use the *Informative References* in Section 3 to identify administrative controls that may help strengthen process maturity. Increase the durability of processes by assigning clear ownership, providing training, and reinforcing them through leadership expectations and employee performance expectations. These actions help reduce reliance on specific individuals, improve consistency of outcomes, and build resilience over time.

3 RISKS AND MITIGATIONS

For each NIST CSF Subcategory, this section provides the following:

- ***Potential Risks and Considerations*** Key factors to evaluate when applying the Subcategory in cloud-integrated OT environments, including changes in risks, responsibilities, dependencies, and security operations.
- ***Example Mitigating Controls*** Tailorable actions the organization may consider to address the identified potential risks and considerations. Where relevant, a separate Cloud Provider Controls subsection identifies example actions for the cloud provider.
- ***Informative References*** References to common standards and guidelines to inform control selection and implementation.

In this section, the organization acquiring or using the cloud-supported capability is the customer. A cloud-supported OT capability may be provided directly by a cloud provider or by an OT vendor delivering a cloud-based service, such as a SaaS application. In the latter case, the OT vendor or supplier may itself rely on a public cloud provider to deliver its product or service. Cybersecurity responsibilities may therefore be distributed among the customer, the provider with which the organization directly contracts, and one or more upstream providers. Organizations should understand how cybersecurity responsibilities are allocated across these relationships and dependencies. Unless otherwise specified, references to cloud provider responsibilities in this section apply to the provider responsible for the relevant cloud service or component.

3.1 Govern (GV)

The Govern Function comprises six Categories:

- Organizational Context (GV.OC)
- Risk Management Strategy (GV.RM)
- Roles, Responsibilities, and Authorities (GV.RR)
- Policy (GV.PO)
- Oversight (GV.OV)
- Cybersecurity Supply Chain Risk Management (GV.SC)

3.1.1 Organizational Context (GV.OC)

GV.OC-01 *The organizational mission is understood and informs cybersecurity risk management*

Potential Risks and Considerations

Leaders define the mission and operational outcomes for the organization. Identify requirements and constraints necessary to achieve defined outcomes. These may include requirements or constraints related to safety, reliability, environmental protection, regulatory compliance, or service continuity. The organization should use these requirements to guide architecture, procurement, risk assessment, and risk acceptance decisions. For example, to achieve service continuity requirements, an organization may implement redundancy measures (fallback options, local capabilities, or manual processes) that can sustain essential operations when cloud-supported services are degraded or unavailable.

Example Mitigating Controls

- Administrative Controls
  - **Review and update cybersecurity program governance documents.**

    Consider how the cybersecurity program will need to evolve to address cloud-specific risks and leverage cloud-specific opportunities. Review and update cybersecurity program governance documents to ensure that the cybersecurity program will support achievement of the organization's mission.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - GV.OC-01

- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.1: Policies for information security
  - Control 5.2: Information security roles and responsibilities
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Program Management (PM)

GV.OC-02 *Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered*

Potential Risks and Considerations

Different cloud technologies, service models, and contractual requirements may change the makeup of stakeholder groups as well as the responsibilities and needs of each stakeholder group.

Example Mitigating Controls

- Administrative Controls
  - **Identify relevant internal and external stakeholders and their cybersecurity expectations.**

    Identify internal and external stakeholders that support or rely on the delivery of critical OT services. Consider and document the cybersecurity needs and expectations of these stakeholders to support the selection of cloud-based services and the development of secure cloud environments.
  - **Establish requirements that reflect the expectations of internal and external stakeholders.**

    Identify the internal and external stakeholders who support, regulate, or rely on each critical OT service. Record each stakeholder's cybersecurity, safety, reliability, performance, privacy, recovery, reporting, and communication expectations. Resolve conflicts, identify the accountable decision-maker, and convert approved expectations into measurable requirements. Place each requirement in the contract, architecture, operating procedure, policy, or assurance plan that can enforce it.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - GV.OC-02

- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.2: Information security roles and responsibilities
  - Control 5.19: Information security in supplier relationships
  - Control 5.20: Addressing information security within supplier agreements
  - Control 5.31: Legal, statutory, regulatory and contractual requirements
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Program Management (PM)
  - Supply Chain Risk Management (SR)

GV.OC-03 *Legal, regulatory, and contractual requirements regarding cybersecurity—including privacy and civil liberties obligations—are understood and managed*

Potential Risks and Considerations

Legal, regulatory, and contractual requirements may impact requirements and constraints for integrating cloud technologies into OT environments. For example, default cloud-generated logs may not fulfill some regulatory obligations for evidence retention.

Example Mitigating Controls

- Administrative Controls
  - **Identify and manage the legal, regulatory, and compliance obligations governing the integration of cloud in OT environments.**

    Document legal, regulatory, and compliance requirements that apply to cloud-supported OT environments. Map each requirement to the responsible customer, cloud provider, or supplier control. Track changes and resolve gaps before the organization places a cloud-supported OT service into production.
  - **Identify and manage customer-specific obligations affected by cloud technologies.**

    Document customer requirements that apply to cloud-supported OT systems, assess compatibility with proposed cloud architectures, and address constraints that affect service delivery or data handling.
  - **Establish policies that reflect legal, regulatory, and contractual constraints.**

    Cybersecurity and cloud governance policies should define architectural requirements for cloud-supported OT environments, including data location,

access controls, and retention requirements necessary to meet applicable obligations.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - GV.OC-03
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Data Security and Privacy Lifecycle Management (DSP)
  - Governance, Risk and Compliance (GRC)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.20: Addressing information security within supplier agreements
  - Control 5.31: Legal, statutory, regulatory and contractual requirements
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Program Management (PM)

GV.OC-04 *Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated*

Potential Risks and Considerations

Consider how decisions about cloud technologies such as region selection, service model, architecture, and cloud provider responsibilities may affect requirements for availability, monitoring, restoration, and service continuity. Direct engagement with stakeholders may be necessary to understand and address their needs and communicate changes that may impact them.

Example Mitigating Controls

- Administrative Controls
  - **Identify external stakeholder requirements that could govern the integration of cloud technologies.**

    Identify the objectives, capabilities, and services that external stakeholders depend on. These requirements may be identified through a business impact analysis or engineering analysis. Consider how integrating cloud-supported OT systems could affect these requirements.

- **Establish contractual requirements that define the roles and responsibilities for cloud-supported OT environments.**

  Contracts should document resilience responsibilities between the organization and the cloud provider under the selected service model, including availability and recovery expectations and coordination during disruptions.

- Cloud Provider Controls
  - **Provide tools and clear guidance to enable cloud customers to build secure cloud environments.**

    Provide customers with tools and features that will enable them to meet their resilience requirements. Examples include secure default configurations, secure blueprints, and security solutions.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - GV.OC-04
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.30: ICT readiness for business continuity
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Program Management (PM)
  - Risk Assessment (RA)

GV.OC-05 *Outcomes, capabilities, and services that the organization depends on are understood and communicated*

Potential Risks and Considerations

Integration of cloud technologies may create important dependencies on cloud providers. Identify how loss or degradation of cloud technologies could impair important OT functions, such as visibility, support, or recovery. Define acceptable latency and availability thresholds to account for potential network performance and connectivity issues. Determine whether added mitigations such as redundancy, independent fallback capabilities, service degradation monitoring, or other resilience measures may be necessary.

In some cases, the cloud provider may also have impactful upstream dependencies. If so, document and escalate those potential risks as appropriate. If the cloud provider's upstream dependencies are not visible, record the visibility gap as well as potential risks and escalate as necessary.

Example Mitigating Controls

- Administrative Controls
  - **Identify and document cloud-based external dependencies.**

    Identify and document end-to-end dependencies that support OT systems. External dependencies may include cloud resources, telecommunications services, software and hardware vendors, subcontractors, and partner organizations. Use this inventory to identify potential points of failure and document the actions required to reduce their impact on OT operations. Manage unresolved dependency risks through enterprise risk management processes.
  - **Define OT-specific service level agreements (SLAs) and supporting requirements.**

    Define the availability and latency requirements that cloud-supported OT capabilities depend on. Many cloud service SLAs express availability using monthly uptime or request-success commitments; definitions, measurement methods, exclusions, and remedies vary by service. Latency commitments are less common and may be service-specific. Negotiate the terms the cloud provider does offer, such as availability targets, notification timelines, response commitments, and service credits or other remedies for missed commitments. Design cloud and supporting on-premises architecture and fallback mechanisms to address availability and latency requirements.
- Technical Controls
  - **Identify and implement fallback processes.**

    Design critical functions so they maintain an approved operating state when cloud technology or external connections fail. Define how the organization detects failure, who authorizes transition to fallback processes, and how the system returns to normal service. Fallback processes may include local alarming, local data buffering, redundant communications paths, on-premises monitoring or historian capabilities, degraded-mode operating procedures, manual operator actions, and restoration procedures. Keep fallback mechanisms independent of the service whose failure triggers them. Test fallback processes regularly to confirm that they work as intended and that operations, engineering, cybersecurity, and supplier support teams understand their roles.
- Cloud Provider Controls
  - **Describe service dependencies and failure scope.**

    Describe the boundaries within which a failure of each service is contained. For example, document whether the service operates within a single availability zone, within one region, or across regions. Identify the shared services a customer workload depends on, such as identity services, control planes, and network services. Describe how the service behaves when one of these

dependencies is impaired and identify customer configurations that can limit the impact. Where an upstream dependency is not disclosed, state that a limit exists, so customers can record the visibility gap.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - GV.OC-05
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Business Continuity Management and Operational Resilience (BCR)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.19: Information security in supplier relationships
  - Control 5.21: Managing information security in the ICT supply chain
  - Control 5.30: ICT readiness for business continuity
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Program Management (PM)

3.1.2 Risk Management Strategy (GV.RM)

GV.RM-01 *Risk management objectives are established and agreed to by organizational stakeholders*

Potential Risks and Considerations

The organization should develop objectives for management of risks in collaboration with stakeholders. Consider objectives related to safety, reliability, operational visibility, support functions, recovery, and data protection. Risk management objectives should reflect dependencies on cloud providers and their upstream dependencies. Because responsibilities vary by service model, architecture, and contract, the objectives should reflect the outcomes expected from both organization-managed and provider-managed controls.

Where feasible, develop measurements to assess achievement of cybersecurity risk management objectives. Potential measures include cloud provider service availability, recovery performance, incident notification timeliness, access to required evidence, and the status of organization-managed cloud controls.

Example Mitigating Controls

- Administrative Controls
  - **Update cybersecurity risk management objectives to address cloud-based risks.**

    Update cybersecurity risk management objectives to address cloud-specific risk, including external dependency and supply chain considerations.
  - **Update cybersecurity risk management measurement objectives to address cloud-based risks.**

    Expand measurement objectives for cybersecurity risk management to include, where feasible, metrics that assess risk inherited from cloud products and services, cloud providers, and their critical subcontractors and partners.
  - **Confirm senior management and Board cybersecurity risk oversight includes cloud environments.**

    Oversight responsibilities should consider current and planned cloud arrangements and resulting changes to the cybersecurity risk profile. Senior management and the Board should receive regular updates on these arrangements and associated risks so that oversight roles, priorities, and decisions can be adjusted as needed.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - GV.RM-01
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Governance, Risk and Compliance (GRC)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.1: Policies for information security
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Program Management (PM)
  - Supply Chain Risk Management (SR)

GV.RM-02 *Risk appetite and risk tolerance statements are established, communicated, and maintained*

Potential Risks and Considerations

Cloud technologies can redistribute, reduce, increase, or introduce new cybersecurity risks. Examine how these changes may result in misalignment between actual risk and

risk tolerance. Consider how integration of cloud technologies may impact important requirements for latency, availability, recovery, and loss of connectivity. For example, some electric grid teleprotection and protective relaying functions require deterministic responses measured in milliseconds. As another example, emergency shutdown (ESD) systems in the oil and gas sector may have defined response time requirements to account for specified operational hazards.

If cloud integration inhibits the achievement of important requirements, misalignment of risk and risk tolerance may occur.

Example Mitigating Controls

- Administrative Controls
  - **Reexamine risk appetite and risk tolerance statements relative to cloud operations.**

    Recalibrate risk appetite and tolerance statements to reflect the organization's changed risk profile. These updates should account for the balance between assumed risks and operational gains in efficiency and effectiveness from cloud engagements. Ensure that senior leaders and Board members are fully informed of and concur with these recalibrations.
  - **Identify and communicate potential variances to risk appetite and risk tolerance relative to cloud operations to senior leadership and Board members.**

    Identify and communicate risks associated with cloud operations that deviate from existing risk appetite and tolerance levels. Present these variances to senior leadership and Board members for evaluation and decision making.
  - **Define engineering criteria that protect safety functions.**

    Identify the protection, safety, and control functions that depend on precise timing, continuous availability, or trusted data. Keep these functions within the engineered protection or safety architecture, which may include deterministic communications-assisted or remote trip schemes designed to meet timing, safety, and availability requirements. Preserve local fail-safe or fallback operation that works when cloud connectivity is lost.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - GV.RM-02
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.1: Policies for information security

- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Program Management (PM)

GV.RM-03 *Cybersecurity risk management activities and outcomes are included in enterprise risk management processes*

Potential Risks and Considerations

Significant risks associated with integration of cloud technologies in OT functions should be managed through enterprise risk management (ERM) processes. For example, disruptions to cloud technologies that support essential OT functions could impact operational reliability, safety, finances, regulatory compliance, or reputation. At the same time, cloud technologies can also reduce certain risks in many ways, including provider-managed hardening, patching, monitoring, and resilience features. The organization should identify which hardening, patching, monitoring, and resilience controls are managed by the cloud provider and which it retains under the service model, architecture, and contract. ERM processes should include evaluation of both increases and decreases in risk to understand how cloud integration may affect overall enterprise risk.

Example Mitigating Controls

- Administrative Controls
  - **Ensure that cloud-related cybersecurity and supply chain risks are included in ERM processes.**

    Assess how reliance on cloud providers and their upstream dependencies could affect critical OT functions, cybersecurity, and resilience requirements. Update risk assessment, reporting, and escalation criteria to reflect those third-party dependencies and their potential operational impact. Update normalization and aggregation methods to ensure these risks are communicated effectively. Consider how risks to cloud-supported OT systems impact the organization’s objectives and mission-essential functions.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - GV.RM-03
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Governance, Risk and Compliance (GRC)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.1: Policies for information security

- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Program Management (PM)
  - Supply Chain Risk Management (SR)

GV.RM-04 *Strategic direction that describes appropriate risk response options is established and communicated*

Potential Risks and Considerations

The organization should define near-term and long-term responses to potential risks related to cloud technologies. Example risk responses include changing tenant configurations or architecture, adding compensating controls, selecting a different service or deployment model, implementing local failover capabilities, deciding not to move certain OT functions to the cloud, or accepting risks deemed to be within approved risk tolerances. Review cloud provider documentation, service commitments, and independent assurance evidence to inform development of risk responses.

Identify who is responsible for selecting risk responses. Communicate approved responses and those responsible for selecting risk responses to stakeholders. Clear direction facilitates effective decision making and helps keep risk within acceptable tolerances.

Example Mitigating Controls

- Administrative Controls
  - **Update risk-treatment policies to address risks to cloud-supported OT environments.**

    Update existing risk-treatment policies to account for risks that involve cloud-supported OT environments. Updates may include criteria for avoiding, mitigating, transferring, and accepting risk; stakeholders who approve risk treatment; and escalation criteria for safety, reliability, and regulatory risks. Consider the service model and related shared responsibility implications. Shared responsibility may influence applicable treatment options for specific risks.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - GV.RM-04
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Governance, Risk and Compliance (GRC)

- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.1: Policies for information security
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Program Management (PM)
  - Supply Chain Risk Management (SR)

GV.RM-05 *Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties*

Potential Risks and Considerations

Document clear processes for internal communication and escalation of cybersecurity risks related to cloud technologies. Include processes for communicating across stakeholder groups such as OT operations, engineering, cybersecurity, IT, procurement, legal, compliance, ERM, and executive leadership. Consider how communication processes should be adjusted to account for responsibilities defined by cloud service models and contracts.

Example Mitigating Controls

- Administrative Controls
  - **Establish cross-functional communication channels to share cybersecurity risk information.**

    Establish communication channels among internal and external stakeholders responsible for managing cloud technologies and cloud provider relationships. Internal stakeholders may include operational, cybersecurity, procurement, legal, and executive functions. External stakeholders may include cloud providers, vendors, and service providers.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - GV.RM-05
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.1: Policies for information security
  - Control 5.2: Information security roles and responsibilities
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Program Management (PM)

GV.RM-06 *A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated*

Potential Risks and Considerations

Document processes for consistent identification and analysis of cybersecurity risks related to cloud technologies. For each significant risk, identify a risk owner and those responsible for selecting risk responses and implementing controls.

Risk analysis should include estimation of potential impacts to the organization's mission and operations. Consider impacts to organizational priorities such as safety, reliability, finances, regulatory compliance, incident response, confidentiality, integrity, and availability. Determine how analysis processes should account for important factors such as cloud providers' upstream dependencies and control implementation responsibilities. Use cloud provider documentation, service commitments, performance data, and assurance artifacts to inform risk analysis. Document important assumptions. Communicate identified risks, processes, and responsible personnel to stakeholders. A complete and accurate understanding of potential risks is important to achieving the organization's mission and goals.

Example Mitigating Controls

- Administrative Controls
  - **Ensure that cloud-related risks are consistently documented in the risk register.**

    The risk register should capture cloud technology dependencies and risk ownership under shared responsibility models. Document risks using the same fields as other risks, such as potential consequences, likelihood, affected function, risk owner, and supporting evidence.
  - **Establish or update risk evaluation methods and apply them consistently across hybrid OT environments.**

    Risk evaluation methods should account for shared responsibility, contractual commitments, and the criticality of supported OT functions. The organization should apply these methods consistently across on-premises and cloud-supported OT systems to support enterprise risk management.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - GV.RM-06
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Governance, Risk and Compliance (GRC)

- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Risk Assessment (RA)

GV.RM-07 *Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions*

Potential Risks and Considerations

Cloud integration can create many opportunities for improved OT cybersecurity and resilience. The organization should identify and analyze these opportunities alongside potential risks when making decisions related to cloud integration.

Example Mitigating Controls

- Administrative Controls
  - **Ensure that strategic opportunities are considered in risk discussions.**

    Consider both the associated risks and the strategic opportunities of cloud integration in OT environments as part of risk management processes.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - GV.RM-07

3.1.3 Roles, Responsibilities, and Authorities (GV.RR)

GV.RR-01 *Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving*

Potential Risks and Considerations

For each significant risk arising from the use of cloud technologies, leadership should designate a risk owner with the authority to manage the risk and a direct escalation path to senior leadership. Risk owners should monitor risks against approved tolerances and escalate when those tolerances are likely to be exceeded.

Before cloud technologies are integrated within OT environments, leadership should ensure that personnel assess the implications for safety, reliability, and operations. Personnel should communicate identified risks to the appropriate risk owners and escalate decisions that exceed their authority.

Leadership should reinforce a risk-aware and ethical cybersecurity culture through its decisions and conduct. This includes encouraging good-faith reporting of concerns, reviewing incidents and near misses, and ensuring that corrective actions are assigned and completed. Leaders should hold themselves and their teams accountable for fulfilling their responsibilities and following approved risk decisions. Lessons learned should inform improvements to cloud-related OT risk management.

Example Mitigating Controls

- Administrative Controls
  - **Establish leadership oversight and accountability for the cybersecurity strategy related to cloud integration in OT environments.**

    Organizational leadership formally approves and oversees cybersecurity strategy that includes cloud integration in OT environments. The strategy defines roles, decision-making authority, and accountability for managing cloud-related risk. It also clarifies how the organization shares responsibility across executive leadership, engineering, cybersecurity, operations, and cloud providers.
  - **Ensure that governance is coordinated across IT and OT leadership for cloud integration.**

    Leadership should establish clear authority and coordination mechanisms to address cybersecurity risks where IT and OT functions converge in cloud platforms.
  - **Ensure that leadership reinforces a risk-aware and ethical security culture.**

    Leadership should communicate expectations for secure cloud adoption and responsible and ethical use of provider-managed services across OT environments.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - GV.RR-01
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.2: Information security roles and responsibilities
  - Control 5.4: Management responsibilities
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Program Management (PM)

GV.RR-02 *Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced*

Potential Risks and Considerations

Document cybersecurity roles, responsibilities, and authorities for the organization and cloud providers. Update policies and procedures to reflect changes to roles, responsibilities, and authorities. Communicate changes to those responsible and to all key stakeholders.

Consider the following activities when documenting roles, responsibilities, and authorities:

- Approval of integration of cloud technologies within OT systems
- Evaluation of provider-managed control performance
- Receipt and disposition of cloud provider notifications
- Coordination during disruption or recovery

Example Mitigating Controls

- Administrative Controls
  - **Identify and document organizational roles, responsibilities, and authorities for cloud-based products and services.**

    The organization should identify roles, responsibilities, and authorities for personnel supporting cloud-based products and services, including those in non-technical roles, such as legal and procurement. Document roles, responsibilities, and authorities in policies. Documentation should clearly define who coordinates with the cloud provider during disruption, who escalates significant OT operational consequences, and who authorizes a return to service for affected functions.
  - **Verify that personnel understand cybersecurity responsibilities.**

    The organization should require personnel to acknowledge their assigned cybersecurity responsibilities and complete role-based training before they exercise those responsibilities. It should periodically review performance expectations to reinforce personnel accountability and alignment with organizational objectives. Test critical decision and coordination roles through exercises, evaluate performance against defined criteria, document decisions, and correct identified gaps.

- Cloud Provider Controls
  - **Establish and communicate the roles and responsibilities for personnel servicing the organization's cloud-based products and services.**

    Define and communicate the roles, responsibilities, and authorities of personnel who operate and secure the cloud hosting infrastructure.
  - **Provide a documented shared responsibility matrix.**

    Document and communicate how cybersecurity roles and responsibilities are allocated for each service model.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - GV.RR-02
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Human Resources (HRS)
- IEC 62443-4-1:2018 [IEC 2018]
  - Practice 1: Security management
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.2: Information security roles and responsibilities
  - Control 5.10: Acceptable use of information and other associated assets
  - Control 5.36: Compliance with policies, rules and standards for information security
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Program Management (PM)

GV.RR-03 *Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies*

Potential Risks and Considerations

Cloud integration may change the number of staff as well as the types of skills needed to manage important cybersecurity controls. Consider changes to monitoring, logging, configuration management, and resilience capabilities. Resourcing plans should also account for the pace of cloud service changes, reliance on provider-managed services, and the operational needs of OT systems.

Example Mitigating Controls

- Administrative Controls
  - **Ensure that personnel assigned roles and responsibilities for supporting cloud-based products and services have the requisite knowledge and skills.**

    Assign roles and responsibilities to personnel supporting cloud technologies used in OT environments. These personnel include not only IT, OT, and cybersecurity personnel, but also subject matter experts and other internal stakeholders in support roles, such as legal, internal audit, and enterprise risk management.
  - **Ensure that sufficient resources have been assigned to support cloud-based products and services.**

    Estimate the people, funding, and tools needed to securely implement and maintain cloud-supported OT systems. The organization should consider factors needed to securely implement the capability, such as staffing levels, backup staff coverage, required training, cybersecurity tooling, and technology upgrades. The organization remains accountable for managing risks arising from its use of cloud services. Responsibility for implementing and operating individual controls is allocated between the organization and the cloud provider according to the service model, contracts, and shared-responsibility documentation.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - GV.RR-03
- IEC 62443-4-1:2018 [IEC 2018]
  - Practice 1: Security management
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Program Management (PM)

GV.RR-04 *Cybersecurity is included in human resources practices*

Potential Risks and Considerations

Plan for changes to internal human resources management processes as well as potential processes needed for management of cloud provider personnel. For example, changes may be needed to notification processes for transfers, role changes, and departures. Consider potential changes to identity and remote access controls, role and

entitlement assignments, and credential management, particularly where centralized or federated identity services provide access across multiple systems and locations.

Human resources practices may need to be updated to address new skills required to manage cloud technologies. Consider potential changes that may be needed for training plans, succession plans, position descriptions, hiring criteria, and onboarding processes.

Cloud provider personnel may operate or maintain infrastructure that supports OT functions. Because the cloud provider is responsible for hiring, screening, training, and overseeing these personnel, the organization should evaluate the cloud provider's workforce practices. Where feasible, contractual agreements may be used to address gaps in existing cloud provider workforce practices. Where appropriate, consider including requirements for performance attestations or other assurance evidence in contractual agreements.

Example Mitigating Controls

- Administrative Controls
  - **Ensure that personnel operating, configuring, and managing cloud-based services have the requisite knowledge and skills.**

    The organization should define knowledge and skill expectations for roles operating, configuring, and managing cloud-based products and services, such as IT, cybersecurity, engineering, legal, internal audit, and enterprise risk management. Update job descriptions to include cloud-specific skills for these roles.
  - **Screen personnel before granting access.**

    Screen and rescreen personnel as applicable policy requires, enforce personnel obligations, and apply sanctions when personnel violate security requirements. Apply these requirements to employees, contractors, temporary personnel, and other external personnel.
  - **Ensure that hiring and training address cloud expertise.**

    Cloud integration should influence hiring and training expectations for roles that interact with cloud-supported OT systems. Update training plans for current employees to address gaps in cloud expertise. Ensure hiring decisions for new employees consider training and experience with cloud technology, in addition to OT.
  - **Update access management processes to include cloud-supported OT environments.**

    Extend processes for granting, changing, and revoking access to cloud systems. Examples include enterprise identity providers (IdPs), IaaS tenant environments, SaaS applications, cloud administrative consoles, code repositories, and automation platforms. Apply access changes when personnel

join the organization, change roles, or leave. Remove permissions, end active sessions, and revoke or rotate affected credentials, as supported. Confirm that changes take effect across connected systems within organization-defined, risk-based time limits.

- Cloud Provider Controls
  - **Apply personnel security practices to staff supporting cloud services.**

    Screen and train employees and contractors before granting access to customer environments or the infrastructure that supports them. Match screening, training, and access to assigned duties and applicable requirements. Promptly adjust or revoke access when duties or employment change. Provide customers with documentation or independent assurance of these practices.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 6: Access Control Management
- CRI Cloud Profile v2.0 [CRI 2024]
  - GV.RR-04
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Human Resources (HRS)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 6.1: Screening
  - Control 6.2: Terms and conditions of employment
  - Control 6.3: Information security awareness, education and training
  - Control 6.4: Disciplinary process
  - Control 6.5: Responsibilities after termination or change of employment
  - Control 6.6: Confidentiality or non-disclosure agreements
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Personnel Security (PS)

3.1.4 Policy (GV.PO)

GV.PO-01 *Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced*

Potential Risks and Considerations

The organization should establish or update cybersecurity policies to govern the use of cloud technologies in OT environments. Policies define permitted and prohibited uses, approval authorities, and high-level cybersecurity requirements. The organization should communicate these policies to affected personnel and enforce them consistently. Without clear policies, personnel may apply cybersecurity practices inconsistently, weakening governance and creating gaps in cybersecurity control implementation.

Cybersecurity policies should address when vendors deliver OT capabilities through cloud-hosted services, including SaaS offerings. Examples include vendors transitioning historians, supervisory control and data acquisition (SCADA) platforms, or remote monitoring tools to cloud-based models incrementally. As a result, personnel may not recognize a product update, integration, or optional feature as a new use of cloud technology. Policies should address approval, access, data handling, service continuity, fallback expectations, and the allocation of responsibilities for these offerings.

Example Mitigating Controls

- Administrative Controls
  - **Develop new policies and revise existing policies to address cloud-supported OT environments.**

    Develop new policies and revise existing policies that cloud integration impacts. Obtain senior management approval for material changes and communicate new and updated policies to affected personnel. Personnel should acknowledge and comply with updated requirements. The organization may find it useful to develop cloud-specific policy supplements or annexes rather than rewriting existing policies in their entirety.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - GV.PO-01
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - A&A-01, AIS-01, BCR-01, CCC-01, CEK-01, DCS-01, DCS-02, DCS-03, DCS-04, DCS-05, DSP-01, GRC-01, GRC-02, HRS-01, HRS-02, HRS-03,

HRS-04, IAM-01, IAM-02, IPY-01, I&S-01, LOG-01, SEF-01, SEF-02, STA-01, STA-02, TVM-01, TVM-02, UEM-01

- IEC 62443-4-1:2018 [IEC 2018]
  - Practice 1: Security management
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.1: Policies for information security
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - AC-01, AT-01, AU-01, CA-01, CM-01, CP-01, IA-01, IR-01, MA-01, MP-01, PE-01, PL-01, PS-01, PT-01, RA-01, SA-01, SC-01, SI-01, SR-01

GV.PO-02 *Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission*

Potential Risks and Considerations

The organization should review and update cybersecurity policies for cloud-supported OT environments at planned intervals and when material changes occur. Reviews should consider changes in architecture, cloud provider service offerings, the cloud provider's upstream dependencies, operational workflows, threats, and fallback or recovery assumptions. After updating a policy, the organization should communicate the changes to affected personnel. Without regular review, policies may diverge from actual practices or fail to support consistent risk management.

Policy reviews should address changes introduced by cloud providers, OT vendors, and new technologies. Examples include expanded use of provider-managed services, vendor transitions to cloud-hosted delivery models, and adoption of automation and artificial intelligence (AI) capabilities. The organization should determine whether these changes affect approval authorities, control responsibilities, access, data handling, monitoring, or service continuity requirements.

The organization should review applicable policies when legal, regulatory, and contractual requirements for cloud-supported OT systems change. This review should address obligations related to privacy, critical infrastructure, data protection, evidence retention, and regulatory reporting. The organization should revise affected policies and communicate the changes to relevant personnel.

Example Mitigating Controls

- Administrative Controls
  - **Periodically review and update cybersecurity policies to reflect changes in cloud-supported OT environments.**

    Regularly review and update cybersecurity policies to address changes in cloud architectures, cloud provider service offerings, the cloud provider's upstream dependencies, and applicable legal, regulatory, and contractual requirements.
  - **Establish and maintain triggers for cybersecurity policy review related to cloud integration.**

    Establish and maintain documented triggers for policy review, such as significant architectural changes, new or modified cloud technology integrations, audit findings, regulatory updates, or changes in mission or operational priorities. Security incidents or near-misses involving a cloud-supported OT system or a supply chain partner should also serve as triggers, as these events may indicate that existing policies no longer adequately govern the current risk environment.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - GV.PO-02
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - A&A-01, AIS-01, BCR-01, CCC-01, CEK-01, DCS-01, DCS-02, DCS-03, DCS-04, DCS-05, DSP-01, GRC-01, GRC-02, GRC-03, HRS-01, HRS-02, HRS-03, HRS-04, IAM-01, IAM-02, IPY-01, I&S-01, LOG-01, SEF-01, SEF-02, STA-01, STA-02, TVM-01, TVM-02, UEM-01
- IEC 62443-4-1:2018 [IEC 2018]
  - Practice 1: Security management
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.1: Policies for information security
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - AC-01, AT-01, AU-01, CA-01, CM-01, CP-01, IA-01, IR-01, MA-01, MP-01, PE-01, PL-01, PS-01, PT-01, RA-01, SA-01, SC-01, SI-01, SR-01

3.1.5 Oversight (GV.OV)

GV.OV-01 *Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction*

Potential Risks and Considerations

The organization should review the outcomes of its cybersecurity risk management strategy for cloud-supported OT environments and use findings to adjust strategic direction. The review should determine whether decisions and investments are meeting operational, resilience, and cybersecurity objectives. It should consider risk assessments, incidents, exercises, service performance, and feedback from operators and engineers. It should also evaluate whether cloud dependencies, provider-managed services, and changes in control boundaries affect its ability to operate and recover effectively.

Example Mitigating Controls

- Administrative Controls
  - **Evaluate the effectiveness of the cybersecurity strategy for cloud-supported OT environments with leadership.**

    With leadership, assess whether strategy outcomes, supported by risk reporting, metrics, and analysis, help leadership make informed decisions, support operational resilience, and achieve organizational objectives for cloud-supported OT environments. Determine whether the organization needs strategic adjustments to address cloud technology dependencies or provider-managed controls. Consider both periodic evaluation of strategy effectiveness and event-driven strategy reviews, such as when a material event occurs.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - GV.OV-01
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Program Management (PM)

GV.OV-02 *The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks*

Potential Risks and Considerations

Oversight findings should inform reviews and adjustments of the cybersecurity risk management strategy for cloud-supported OT environments. Internal assessments, independent audits, incidents, performance results, and reports from cloud providers or other suppliers can indicate whether existing controls, contractual arrangements, and governance mechanisms adequately address identified risks and organizational requirements.

Example Mitigating Controls

- Administrative Controls
  - **Periodically review and adjust the cybersecurity strategy for cloud-supported OT environments.**

    The organization should review the cybersecurity risk management strategy in light of audit findings, incident reporting, oversight results, and performance outcomes related to cloud-supported OT systems. Where reviews identify gaps between expected and actual control effectiveness or coverage of organizational requirements, the organization should update the strategy, obtain appropriate leadership approval, and communicate the changes to affected stakeholders.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - GV.OV-02
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Program Management (PM)

GV.OV-03 *Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed*

Potential Risks and Considerations

The organization should adapt how it evaluates cybersecurity risk management performance to account for reliance on cloud providers and other suppliers. Because the organization may have limited visibility into provider-managed infrastructure, performance measures should distinguish between controls it can assess directly and controls it must evaluate through cloud provider evidence. Cloud provider attestations, certifications, and assessment reports offer useful assurance, but are periodic and may

not reflect current operating conditions. Where available, the organization should supplement them with service health data, performance reports, incident notifications, and logs from its own environment.

Performance measures for cloud-supported OT environments should focus on outcomes significant to operations. Key performance indicators (KPIs) and key risk indicators (KRIs) may address fallback effectiveness, timely alarming, visibility into security and operational events, and the ability to restore capabilities without compromising safe operations. They should also reflect material cloud dependencies and available evidence about cloud provider performance. Without relevant measures, leadership may receive an incomplete view of cybersecurity performance and overlook adjustments needed to support risk management and operational objectives.

Example Mitigating Controls

- Administrative Controls
  - **Define the metric attributes.**

    Define the attributes for each KPI and KRI, such as data source, formula, owner, and collection frequency.
  - **Periodically evaluate cybersecurity risk management performance for cloud-supported OT environments and take corrective action when performance falls short.**

    Review KPIs and KRIs for cloud-supported OT systems to determine whether cybersecurity policies, procedures, and controls are achieving intended outcomes. When results show a performance gap, identify its cause and assess its effect on mission, safety, reliability, and cybersecurity risk. Select an appropriate response, assign an owner and due date, obtain approval from the designated risk authority, and verify that the response produces the intended result. Escalate any gap that exceeds an approved risk tolerance.
  - **Ensure that leadership oversight includes review of cybersecurity risk management performance for cloud-supported OT environments.**

    Provide senior leadership and, where applicable, the Board with performance metrics for cloud-supported OT environments. Use those metrics to guide decisions on strategy, resource allocation, and oversight where performance falls short of defined objectives.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - GV.OV-03
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.35: Independent review of information security

- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Program Management (PM)

3.1.6 Cybersecurity Supply Chain Risk Management (GV.SC)

GV.SC-01 *A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders*

Potential Risks and Considerations

The organization should update its cybersecurity supply chain risk management (SCRM) program to address cloud technologies that support OT environments. Its strategy, objectives, plans, policies, and procedures should account for reliance on cloud providers and their upstream dependencies. It should also account for allocation of control responsibilities, contractual and technical dependencies, and limited visibility into cloud provider upstream dependencies. The program should consider how provider-managed services and changes in suppliers, services, and threats affect OT supply chain risk and resilience.

Operations, engineering, procurement, and cybersecurity stakeholders should agree on supply chain risk management objectives and decision criteria for cloud-supported OT environments. Supplier risk decisions should consider potential effects on safe operations, service continuity, restoration support, and mission-critical functions. Applying agreed criteria helps the organization evaluate and respond to cloud supplier risks consistently.

Example Mitigating Controls

- Administrative Controls
  - **Review and update the SCRM governance documents to address service dependencies in cloud environments.**

    Ensure that SCRM strategy, policies, and procedures reflect cloud service models, reliance on cloud providers and their upstream dependencies, and the allocation of responsibilities under shared responsibility models.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - GV.SC-01
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Supply Chain Management, Transparency, and Accountability (STA)

- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.1: Policies for information security
- MITRE ATT&CK for ICS v19.2 [MITRE 2026]
  - M0817: Supply Chain Management
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Supply Chain Risk Management (SR)

GV.SC-02 *Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally*

Potential Risks and Considerations

The organization should clearly define and coordinate supplier-facing cybersecurity roles for cloud technologies that support OT systems. The allocation of responsibilities varies by service model, architecture, service, and contract. SaaS places greater responsibility for applications and platform operations with the cloud provider. PaaS generally places platform, runtime, and underlying infrastructure operations with the cloud provider and leaves the organization responsible for deployed application code, configurations, identities, and integrations. In IaaS, the organization generally manages workloads, configurations, and application lifecycles. The organization should document responsibility boundaries, escalation paths, and operational handoffs in responsibility matrices, contractual agreements, and internal role definitions. It should communicate these responsibilities to all relevant parties. Without clear coordination, gaps in oversight and delays in response may occur.

Incident and recovery coordination responsibilities should distinguish cloud provider service restoration from the organization's decision to resume OT use. The organization should define who communicates with the cloud provider, assesses operational impacts, validates restored capabilities, and authorizes the cloud-supported OT function to return to service. Although the cloud provider may restore its service, the organization remains responsible for determining whether the OT function can resume safely and reliably.

Example Mitigating Controls

- Administrative Controls
  - **Establish and communicate the cybersecurity roles and responsibilities for cloud-supported OT environments.**

    Document and communicate roles and responsibilities for the personnel supporting cloud technologies, including those in cybersecurity, operations, procurement, legal, and risk management. The organization should clearly

define shared responsibilities with cloud providers, including incident coordination and reporting.

- **Ensure that cybersecurity policies reflect cloud-related supply chain roles and coordination requirements.**

  Cybersecurity policies should address role allocation, shared responsibility models, and information-sharing expectations for cloud technology arrangements.

- **Define the response and resilience responsibilities for mission-critical OT systems.**

  Document the roles and access requirements that support response and recovery for cloud-supported OT systems. Document and test the escalation paths and coordination procedures the organization follows during a disruption. Record which responsibilities the cloud provider accepts in its service agreement and published support terms and identify the activities the organization can perform within its control. Treat unassigned, unclear, or insufficiently supported responsibilities as gaps requiring resolution through supplier coordination, architectural changes, compensating controls, or documented risk acceptance.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - GV.SC-02
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Supply Chain Management, Transparency, and Accountability (STA)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.2: Information security roles and responsibilities
  - Control 5.19: Information security in supplier relationships
  - Control 5.20: Addressing information security within supplier agreements
  - Control 5.21: Managing information security in the ICT supply chain
  - Control 5.23: Information security for use of cloud services
  - Control 5.38: CLD - Shared roles and responsibilities within a cloud computing environment
  - Control 5.39: CLD - Agreement on the roles and responsibilities of the cloud service partner
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Supply Chain Risk Management (SR)

GV.SC-03 *Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes*

Potential Risks and Considerations

As cloud integration in OT environments becomes more integral to mission execution, the organization should integrate SCRM into its broader cybersecurity, ERM, risk assessment, and improvement processes. At planned intervals and after significant changes to services, suppliers, or contracts, the organization should assess its reliance on cloud providers and their upstream dependencies. These assessments should consider concentration risk, connectivity and service availability, regulatory obligations, data handling, and access to compliance evidence. Assessing these dependencies separately from enterprise risk processes may prevent leadership from seeing their full operational, financial, and organizational impact.

Findings from supplier assessments, incident reviews, and performance evaluations should inform the organization's broader improvement efforts. Repeated problems involving a cloud provider or dependency may indicate a structural risk rather than an isolated performance issue. The organization should use these findings to adjust its supplier strategy, contractual requirements, architecture, risk responses, and resilience plans.

Example Mitigating Controls

- Administrative Controls
  - **Integrate cloud-related supply chain risks into cybersecurity and enterprise risk management processes.**

    The organization should incorporate risks associated with cloud providers and their upstream dependencies into cybersecurity and enterprise risk management. Where cloud dependencies materially affect resilience, regulatory exposure, or financial risk, the organization should reflect these impacts in ERM analysis and governance.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - GV.SC-03
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Program Management (PM)
  - Supply Chain Risk Management (SR)

GV.SC-04 *Suppliers are known and prioritized by criticality*

Potential Risks and Considerations

The organization should identify and prioritize cloud providers, OT vendors, and other suppliers according to their importance to cloud-supported OT functions. Criticality criteria should consider the functions and data the supplier supports, potential safety and operational impacts, regulatory obligations, concentration risk, and time to replace the supplier or restore the service. The criteria should also reflect the organization's responsibilities and visibility under the applicable service model.

Supplier prioritization should also account for the cloud provider's upstream dependencies. The organization may have limited visibility into these upstream dependencies. A cloud provider's third-party risk management may reduce some risks, and assurance evidence may help the organization evaluate that program. When information is unavailable, the organization should document the uncertainty and consider how an upstream disruption could affect critical OT functions.

Example Mitigating Controls

- Administrative Controls
  - **Maintain an inventory of suppliers for cloud-supported OT systems.**

    Develop and maintain an accurate and current inventory of suppliers and service providers that cloud-supported OT systems rely on, including cloud providers and material upstream dependencies where known.
  - **Evaluate and prioritize cloud-related suppliers using defined criticality criteria.**

    Assess suppliers that cloud-supported OT systems rely on against documented criticality criteria, and prioritize them based on factors such as mission impact, data sensitivity, and potential regulatory or financial exposure.
  - **Include the cloud service model in supplier criticality assessments.**

    Criticality determinations should reflect differences in responsibility and dependency across service models. Consider the degree to which the service relies on cloud provider-managed infrastructure, software, and upstream dependencies.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - GV.SC-04
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Supply Chain Management, Transparency, and Accountability (STA)

- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.9: Inventory of information and other associated assets
  - Control 5.21: Managing information security in the ICT supply chain
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Supply Chain Risk Management (SR)

GV.SC-05 *Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties*

Potential Risks and Considerations

Contracts and other agreements for cloud technologies that support OT systems should include cybersecurity and supply chain risk management requirements based on supplier criticality and potential operational impact. These agreements should define responsibilities, security and availability commitments, verification rights, incident notification, planned service change notices, and response and restoration support. Without clear and prioritized requirements, the organization may have limited ability to hold the supplier accountable, obtain needed evidence, or coordinate timely response and recovery.

Municipal utilities, rural cooperatives, and other smaller energy organizations may have limited ability to negotiate customized contracts or SLAs. In these cases, the organization should assess whether standard cloud provider terms, available assurance reports, shared responsibility documentation, support options, incident notification processes, and compensating controls sufficiently meet its OT security, resilience, and compliance needs. Joint procurement frameworks or industry trade associations may provide additional avenues for smaller organizations to identify, develop, or adopt common contract provisions.

Example Mitigating Controls

- Administrative Controls
  - **Establish contractual requirements to address the cybersecurity and supply chain risks associated with cloud technologies.**

    Contracts for cloud-based products and services that support OT systems should define requirements that enable the organization to manage cybersecurity and supply chain risks associated with provider-managed services and infrastructure. Contractual provisions may include:

    - security and performance requirements
    - rules and protocols for information sharing, incident notification, and escalation

    - timelines for vulnerability disclosure
    - evidence of security practices, including certifications, attestations, or audit reports
    - requirements related to data sovereignty, residency, and regulatory obligations
  - **Use collaborative procurement and sector resources to support cloud contract requirements.**

    Where individual negotiation authority is limited, consider joint procurement frameworks, cooperative purchasing vehicles, industry trade associations, or sector-developed resources to support cloud contract requirements. These mechanisms may help organizations identify common security, resilience, incident notification, evidence access, support, and compliance provisions for cloud technologies that support OT environments.

- Cloud Provider Controls
  - **Notify customers of material changes to subcontractors and suppliers.**

    Notify customers of material changes to the subcontractors and supplier relationships that support contracted services, within the timeframes the agreement defines. Describe changes that affect service delivery, data handling, or cybersecurity responsibilities, and identify any action the customer needs to take. Give advance notice for planned changes and prompt notice when advance notice is not possible.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - EX.CN-01
  - EX.CN-02
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Supply Chain Management, Transparency, and Accountability (STA)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.19: Information security in supplier relationships
  - Control 5.20: Addressing information security within supplier agreements
  - Control 5.21: Managing information security in the ICT supply chain
  - Control 5.31: Legal, statutory, regulatory and contractual requirements
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - System and Services Acquisition (SA)

GV.SC-06 *Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships*

Potential Risks and Considerations

Before entering an agreement, the organization should perform due diligence on each cloud service that may support OT functions. The depth of the review should reflect supplier criticality and the potential impact of service failure or compromise. The organization should assess how the cloud provider manages cybersecurity, manages vulnerabilities, responds to incidents, and addresses supply chain risks. Because the organization generally cannot evaluate provider-managed infrastructure directly, it relies on the assurance artifacts the cloud provider makes available in addition to public authorization listings. The organization's due diligence should address the specific service offering and deployment scope rather than the cloud provider as a whole.

The organization should interpret assurance sources according to their scope, period, and purpose. Assurance artifacts may include System and Organization Controls (SOC) 2® Type II reports [AICPA & CIMA 2026] and International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) 27001 certifications [ISO/IEC 2022].

Due diligence should also evaluate the hosting infrastructure, data flows, service locations, and upstream dependencies that support a cloud service. The organization should determine whether these factors create operational resilience, jurisdictional, data residency, or other compliance constraints. Evaluating these dependencies before commitment can help the organization avoid compliance gaps and costly architectural rework.

Example Mitigating Controls

- Administrative Controls
  - **Integrate cloud-specific due diligence into procurement and supplier evaluation processes.**

    Procurement and supplier evaluation processes should require the organization to evaluate a prospective cloud provider's cybersecurity capabilities, incident response practices, supply chain risk management processes, hosting architecture, jurisdictional considerations, and available assurance evidence before it enters into a formal agreement. When the organization cannot directly evaluate provider-managed infrastructure, it should review available third-party attestations, certifications, audit reports, or other oversight mechanisms to determine whether they provide sufficient visibility for risk-based decision making. Evaluate each artifact's scope, assessment period, control coverage, exceptions, exclusions, and customer responsibilities. When the organization identifies gaps, it should define contractual terms or compensating measures before commitment.

- Cloud Provider Controls
  - **Provide assurance information for customer due diligence.**

    Make current documentation and independent assurance artifacts available to customers. Describe the assessed services, regions, controls, and assessment periods. Identify relevant exclusions, findings, and limits on access or use.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - EX.DD-01
  - EX.DD-02
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.21: Managing information security in the ICT supply chain
  - Control 5.23: Information security for use of cloud services
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Supply Chain Risk Management (SR)

GV.SC-07 *The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship*

Potential Risks and Considerations

The organization should monitor cybersecurity risks from cloud providers and their upstream dependencies throughout each supplier relationship. Cloud adoption places some infrastructure and service operations under cloud provider or subcontractor control, which limits direct inspection. The frequency and depth of monitoring should reflect supplier criticality and the potential impact on OT operations. Monitoring may use tenant logs, cloud provider notifications, service health information, contractual compliance data, assurance artifacts, and relevant authorization statuses. Because these sources differ in scope and timeliness, no single source provides a complete view of supplier risk.

Material changes to a cloud provider or service should trigger reassessment of supplier risk. Relevant changes may include architectural updates, incidents, changes in ownership or service scope, new upstream dependencies, reduced support quality, or changes in reported control effectiveness. The organization should document these changes, reevaluate supplier criticality, update risk responses, and escalate material risks through cybersecurity and enterprise risk management processes.

Example Mitigating Controls

- Administrative Controls
  - **Monitor supplier compliance with cybersecurity requirements and address any deficiencies.**

    Monitor supplier adherence to defined cybersecurity and service requirements throughout the relationship lifecycle. Set an assessment frequency commensurate with supplier criticality. Monitor cloud providers using published assurance artifacts, supplemented by service health information, cloud provider notifications, and tenant telemetry. Establish processes for resolving identified deficiencies or disputes and adjust oversight activities when risk conditions change.
  - **Periodically reassess supplier risk profiles and escalate material changes.**

    Review and update the risk profiles of cloud providers and other critical suppliers based on performance results, incidents, architectural changes, or other relevant factors. Escalate material changes in supplier risk to cybersecurity governance and ERM processes.
  - **Maintain business continuity plans that address supplier disruptions.**

    Business continuity and incident response plans should account for potential disruptions affecting cloud-supported OT systems. These plans should define roles, responsibilities, and coordination procedures with cloud providers and other critical suppliers.
- Cloud Provider Controls
  - **Report material changes in assurance and control effectiveness.**

    Provide current assurance information throughout the service relationship. Notify customers of material changes to assessment scope, certification or authorization status, or control effectiveness that affect contracted services.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - EX.MM-01
  - EX.MM-02
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Supply Chain Management, Transparency, and Accountability (STA)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.19: Information security in supplier relationships
  - Control 5.21: Managing information security in the ICT supply chain

- Control 5.22: Monitoring, review and change management of supplier services
- Control 5.23: Information security for use of cloud services

- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Supply Chain Risk Management (SR)

GV.SC-08 *Relevant suppliers and other third parties are included in incident planning, response, and recovery activities*

Potential Risks and Considerations

Incident response and recovery plans should incorporate the roles established between the organization and relevant cloud providers or other suppliers. Plans should reflect the applicable service model and contractual commitments. They should define which party performs or supports detection, containment, investigation, notification, and recovery. Plans should also identify points of contact, reporting timeframes, escalation paths, and crisis communication responsibilities. Without this coordination, response actions may be delayed or fragmented during incidents affecting critical OT operations.

Business continuity and incident response plans should account for disruptions to cloud services, upstream dependencies, and external connectivity on which OT functions depend. Plans should define fallback procedures, restoration priorities, and the sequence for restoring dependent services. They should distinguish the cloud provider's restoration of a cloud service from the organization's validation that the supported OT function is safe and operationally usable. The organization should update these plans as cloud dependencies and shared responsibilities change.

Exercises should include relevant cloud providers and other critical suppliers when contractual terms and support arrangements allow their participation. Exercises should test notification, escalation, evidence sharing, fallback procedures, service restoration, and operational validation. Where a supplier cannot participate, the organization can simulate coordination using the cloud provider's published response commitments and document any untested assumptions. For critical suppliers, agreements should cover provider participation in post-incident lessons-learned activities where feasible.

Example Mitigating Controls

- Administrative Controls
  - **Establish and formalize coordinated incident response roles and processes for cloud-supported OT environments.**

    Define and formalize incident response roles, responsibilities, reporting timelines, communication protocols, and recovery coordination procedures with cloud providers. Review evidence-sharing and notification terms in advance

and understand what information will be available to support incident investigation and to meet regulatory reporting obligations.

- Cloud Provider Controls
  - **Define the incident coordination and exercise support available to customers.**

    Publish the incident coordination support available under each support offering, including participation in customer response and recovery exercises. State the support tier or separate agreement each form of participation requires. Participate within the agreed scope, share relevant findings, and contribute to post-incident lessons-learned activities where the agreement provides for it. Where participation is unavailable, publish the response commitments customers can use to simulate coordination.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - GV.SC-08
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.19: Information security in supplier relationships
  - Control 5.20: Addressing information security within supplier agreements
  - Control 5.24: Information security incident management planning and preparation
  - Control 5.30: ICT readiness for business continuity
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - System and Services Acquisition (SA)

GV.SC-09 *Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle*

Potential Risks and Considerations

The organization should evaluate supply chain security throughout the lifecycle of cloud technologies that support OT systems. Cloud providers and their upstream dependencies manage the acquisition, development, maintenance, and replacement of underlying infrastructure and managed service components. This limits the organization's direct visibility into component provenance, authenticity, and integrity. The organization should use contractual commitments, cloud provider documentation, supplier responses, and independent assurance evidence to evaluate how the cloud provider manages these risks. Because this evidence often describes processes rather

than individual components, the organization should consider its scope and document any remaining uncertainty in its cybersecurity and enterprise risk management processes.

The organization should monitor how provider-managed lifecycle changes affect cloud-supported OT systems, even when it cannot inspect or approve each change. Relevant changes may include patches, upgrades, maintenance activities, service deprecations, and end-of-support decisions. The organization should review available notices and assurance evidence, assess potential cybersecurity and operational impacts, and update risk documentation or response plans when needed.

Example Mitigating Controls

- Administrative Controls
  - **Integrate supplier provenance, authenticity, and integrity assurance into SCRM processes for cloud-supported OT services.**

    Policies and procedures should require the organization to obtain and review available evidence supporting the authenticity, provenance, and integrity of hardware, software, and firmware used to deliver cloud technologies, as well as the cloud provider's processes for detecting and preventing tampering. This may include attestations, certifications, and other supplier-provided evidence. Where the organization identifies gaps in assurance, it should define follow-up actions through risk management, supplier oversight, contractual requirements, or compensating measures.
  - **Establish processes to review provider-delivered updates, upgrades, and maintenance activities that could affect cloud-supported OT systems.**

    Policies and procedures should require the organization to review relevant cloud provider change information, maintenance notifications, and available assurance evidence to assess the potential cybersecurity and operational impact on cloud-supported OT environments. In environments where a cloud provider deploys changes without prior customer review, the organization should use available notifications and monitoring capabilities to identify, assess, and respond promptly to cybersecurity or operational impacts. For customer-applied updates and maintenance, these processes should verify the authenticity and integrity of updates, restrict maintenance activities to authorized personnel, and check for signs of unauthorized modification.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - GV.SC-09
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Program Management (PM)

- Supply Chain Risk Management (SR)

GV.SC-10 *Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement*

Potential Risks and Considerations

The organization should plan how it will end or transition each cloud supplier relationship that supports OT systems. Before provisioning any service, the organization should define exit triggers, roles, notification periods, transition assistance, timelines, and responsibility for maintaining service continuity. Contracts should support these plans and preserve necessary access during a transition. Without defined and enforceable exit provisions, ending a supplier relationship may disrupt operations or weaken resilience.

Service transition plans should define how cloud-supported OT functions will move to another supplier or return to an organization-managed environment. Plans should identify dependencies involving OT monitoring, engineering support, identity services, and recovery capabilities. The organization should test transition procedures where feasible before any deployment to production.

Exit plans should address the portability and disposition of OT data, logs, configurations, and other records held by the cloud provider. Provider-managed or proprietary formats may make these records difficult to extract or migrate. Contracts should define export formats, access rights, retention, and secure deletion. Before ending the relationship, the organization should verify that exported records are complete, intact, decryptable, and usable. After the transition, it should revoke supplier identities, credentials, connections, and other access that is no longer required.

Example Mitigating Controls

- Administrative Controls
  - **Establish and formalize contractual requirements for terminating cloud services.**

    Contracts with cloud providers should define termination conditions, access revocation requirements, data return, and data destruction timelines.
  - **Maintain and test transition plans for cloud-supported OT systems.**

    Maintain and periodically test procedures for transitioning services to alternate cloud providers or internal environments, and assess the cybersecurity, supply chain, and operational resilience risks associated with termination. Transition planning should account for the continuity of mission-critical OT functions.

- Cloud Provider Controls
  - **Support data return at service termination.**

    Provide documented mechanisms to export customer data and relevant metadata in usable formats during service use and termination. State export formats, retrieval timeframes, volume limits, and costs.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - EX.TR-01
  - EX.TR-02
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Interoperability & Portability (IPY)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.11: Return of assets
  - Control 5.19: Information security in supplier relationships
  - Control 5.20: Addressing information security within supplier agreements
  - Control 5.21: Managing information security in the ICT supply chain
  - Control 5.23: Information security for use of cloud services
  - Control 8.10: Information deletion

3.2 Identify (ID)

The Identify Function comprises three Categories:

- Asset Management (ID.AM)
- Risk Assessment (ID.RA)
- Improvement (ID.IM)

3.2.1 Asset Management (ID.AM)

ID.AM-01 *Inventories of hardware managed by the organization are maintained*

Potential Risks and Considerations

Cloud integration can replace some organization-managed hardware with virtual equivalents. In IaaS environments, virtual machines, virtual storage resources, and virtual networking components perform functions that servers, storage devices, and network equipment perform on premises. The organization should track these virtual resources in its inventories of software, services, and systems (ID.AM-02). When a virtual resource replaces on-premises equipment, update the hardware inventory to reflect the retired or repurposed equipment and link it to the record for the virtual resource.

Cloud integration can also add physical hardware to the OT environment. Examples include edge gateways, cloud connectivity appliances, dedicated interconnect equipment, cellular or satellite modems, and provider-supplied hardware installed on premises. The organization should inventory this hardware with other OT equipment and identify which party manages it.

For cloud provider-hosted resources, cloud providers manage and inventory the physical infrastructure they operate. Customers may have limited visibility into those individual physical components or the practices used to inventory them. Cloud provider assurance evidence, including documentation, attestations, and compliance reports, can provide information about how that infrastructure is managed and secured. For some organizations, this information may be necessary to support compliance with regulatory and reliability obligations.

Example Mitigating Controls

- Administrative Controls
  - **Establish asset classification and tagging standards for cloud resources.**

    Define and enforce tagging and metadata standards that identify asset ownership, system function, criticality, and data sensitivity. Align tagging structures with enterprise asset management or configuration management

processes to support unified inventory practices across on-premises OT hardware and virtualized cloud assets.

- **Define shared responsibility for asset inventory management.**

  Document roles and responsibilities for inventory management across on-premises OT assets, customer-managed cloud resources, and cloud provider-managed infrastructure. Ensure that governance processes address how inventory data supports vulnerability management, incident response, and regulatory reporting.

- Technical Controls
  - **Inventory physical hardware that supports cloud integration.**

    Include edge gateways, connectivity appliances, interconnect equipment, and cloud provider-supplied hardware installed on premises in OT hardware inventories. Record each device's location, function, the connections it provides, firmware version, and the party that manages it. Include hardware that a vendor or cloud provider installs or maintains, even when the organization has limited administrative access. Update records when this hardware is added, replaced, relocated, or removed.
- Cloud Provider Controls
  - **Provide transparency into infrastructure asset management practices.**

    Provide documentation, audit artifacts, and independent attestations that describe hardware inventory management practices. Make relevant information available to support customer risk management and regulatory obligations.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 1: Inventory and Control of Enterprise Assets
- CRI Cloud Profile v2.0 [CRI 2024]
  - ID.AM-01
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Datacenter Security (DCS)
  - Universal Endpoint Management (UEM)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.9: Inventory of information and other associated assets
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Configuration Management (CM)

- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - ID.AM: Asset Management

ID.AM-02 *Inventories of software, services, and systems managed by the organization are maintained*

Potential Risks and Considerations

Software and service inventory processes should cover all resources that support OT workflows, regardless of location or cloud service model. The inventory should include on-premises OT software, IaaS resources and their software components, managed platform services, serverless functions, and SaaS applications. Consider how to account for services that operate across multiple regions or cloud environments and scale with demand. Consider which inventory attributes may be necessary for services, such as the regions in which they operate, their external dependencies, and whether the cloud customer or cloud provider manages each service.

IaaS inventory processes may use practices similar to those used for on-premises systems. The inventory should cover virtualized resources and their operating systems, application components, third-party libraries, open-source packages, custom-developed software, and service integrations. Consider how to monitor these components for changes or unauthorized deployments. Inventory processes may also need to account for short-lived resources that may not remain available long enough to be detected by periodic scans or manual inventory methods. Additionally, different cloud service models may affect how resources can be discovered, tracked, and managed.

Cloud provider-native asset discovery, configuration management, and tagging capabilities can help automate portions of cloud asset inventory. For example, when appropriately configured, these capabilities can automatically update inventories when resources are created, changed, or removed. Traditional OT asset management practices can be combined with cloud provider-native discovery and tagging capabilities and analysis of relevant log records to help maintain accurate inventories.

In SaaS environments, the cloud provider manages the application and may rely on an upstream provider to manage underlying infrastructure. Direct visibility into these components may not be available to customers. If additional visibility is needed, consider assurance artifacts and other information. For example, a software bill of materials (SBOM), when available, may provide information about software components and dependencies.

Example Mitigating Controls

- Administrative Controls
  - **Review cloud provider assurance artifacts for software and service inventory practices.**

    Review third-party examination reports, certifications, and related documentation to understand how the cloud provider inventories and manages provider-operated software and services. Evaluate whether these controls support the organization's operational, security, and regulatory requirements.
- Technical Controls
  - **Maintain an inventory of virtual infrastructure supporting OT systems.**

    Inventory virtual machines, virtual disks, and virtual networks that perform the functions of servers, storage devices, and network equipment. Link these records to hardware inventories where virtual resources replace or extend on-premises equipment. Native cloud inventory services record resources at the control plane, and coverage varies by cloud provider and resource type.
  - **Automate discovery and inventory updates for virtual infrastructure.**

    Use cloud provider discovery, logging, and tagging capabilities, or equivalent third-party tools, to automatically record when virtual infrastructure is provisioned, modified, and decommissioned. Capture both persistent and short-lived resources to maintain accurate records.
  - **Maintain an inventory of customer-managed software, services, and system integrations supporting OT functions.**

    Maintain an accurate and current inventory of operating systems, applications, third-party libraries, open-source components, and SaaS integrations that store, process, or transmit OT data. Use automated discovery and configuration management tools to detect software changes and unauthorized service deployments across on-premises and cloud environments.
  - **Integrate software inventory data with vulnerability and configuration management processes.**

    Ensure that software and service inventories help the organization identify vulnerable components quickly, including cryptographic modules and external service dependencies. Integrate inventory management processes with vulnerability management and patch management processes to support risk-based remediation decisions.
- Cloud Provider Controls
  - **Maintain an inventory of software and service components delivering cloud technologies.**

    Maintain a current inventory of software-defined services, platform components, and service dependencies that directly support customer

workloads. Manage these components through secure development, configuration management, and change control processes. Where detailed component information is confidential, provide sufficient documentation or independent attestation to demonstrate effective inventory and lifecycle management controls.

- **Expose customer resource inventories and lifecycle events.**

  Provide interfaces that let customers enumerate the cloud resources they have provisioned and retrieve the identifiers, configurations, and metadata associated with each one. Make creation, modification, and deletion events available so customers can update inventories automatically, including events for short-lived resources. Document the resource types these interfaces cover and the resources they do not.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 2: Inventory and Control of Software Assets
- CRI Cloud Profile v2.0 [CRI 2024]
  - ID.AM-02
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Datacenter Security (DCS)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.9: Inventory of information and other associated assets
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Configuration Management (CM)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - ID.AM: Asset Management

ID.AM-03 *Representations of the organization's authorized network communication and internal and external network data flows are maintained*

Potential Risks and Considerations

Integration of cloud technologies may require updates to documentation of authorized data flows across physical, virtual, provider-managed, and hybrid environments. Documentation should account for communication paths, trust boundaries, segmentation models, and interconnections. It should also identify expected ports and protocols, remote access pathways, and dependencies that could affect latency, availability, or operational predictability, and establish traffic baselines for expected

communications. Tools for network flow logging, traffic monitoring, and configuration management can supplement existing OT network monitoring solutions.

Network management responsibilities and available controls vary by cloud service model. In software as a service (SaaS), the cloud provider manages the underlying infrastructure. Direct visibility into the underlying infrastructure may be limited or unavailable to customers. Cloud provider documentation or other information sources may be needed to understand data paths, architecture, and the cloud provider's external interfaces. Research and document authorized data exchanges, authentication mechanisms, application programming interface integrations, where operational data is transmitted, stored, or processed, and how the service interfaces with other systems. In infrastructure as a service (IaaS), the customer typically manages virtual networks, routing tables, gateways, and security policies within its cloud tenant. In platform as a service (PaaS), customers do not control the underlying cloud provider network, but many services expose customer-configurable network capabilities, such as routing and ingress and egress control.

Example Mitigating Controls

- Technical Controls
  - **Build cloud-supported OT services into the enterprise architecture.**

    The organization's technology architecture should incorporate cloud-supported OT services in a manner that aligns with the organization's mission. Validate each design against the organization's mission, safety, reliability, cybersecurity, and regulatory requirements. Consider applicable government guidance, consensus standards, sector guidance, and cloud provider documentation when designing cloud-supported OT systems. Examples of government and cloud provider resources that may provide applicable guidance include NLR's CloudZero report [Wallace 2024], Azure's Well-Architected framework [Microsoft 2026], security guidance for manufacturing and energy organizations from Google Cloud Office of the Chief Information Security Officer [Google 2025], and AWS's Well-Architected tools and guidance [AWS 2026a].
  - **Maintain documented representations and baselines of authorized network communications and data flows across service models.**

    For IaaS and for PaaS services that expose customer-accessible network telemetry, capture network-level connection attributes and flow metrics. For other PaaS and SaaS services, document application, application programming interface (API), identity, and cloud provider-exposed telemetry available to the customer.
  - **Implement monitoring to establish and maintain network traffic baselines.**

    Use network flow logs, provider-offered traffic monitoring, and on-premises network monitoring tools to establish and maintain baselines of authorized communication patterns. Apply these capabilities across infrastructure,

platform, and software service models, as appropriate to the organization's level of control and visibility.

- **Validate observed communication patterns against documented baselines.**

  Periodically compare observed network and service communications to documented baselines. Investigate unauthorized, unintended, or anomalous data flows that may affect OT data confidentiality, integrity, or availability. Integrate findings with incident response, vendor risk management, and regulatory reporting processes, as appropriate.

- Cloud Provider Controls
  - **Document service endpoints, data locations, and responsibility boundaries.**

    Publish current documentation of service endpoints, integration paths, and supported authentication mechanisms. Identify the regions and service components where customer data is stored and processed and name the third parties involved in delivering the service. State where responsibility for protecting each path passes between the cloud provider and the customer. Communicate changes that affect customer network diagrams and data flow records.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 12: Network Infrastructure Management
- CRI Cloud Profile v2.0 [CRI 2024]
  - ID.AM-03
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Infrastructure Security (I&S)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 8.20: Network security
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Planning (PL)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - ID.AM: Asset Management

ID.AM-04 *Inventories of services provided by suppliers are maintained*

Potential Risks and Considerations

Cloud integration may include services supplied by the cloud provider that require access to or interaction with OT systems or operational data. These services may include SaaS, PaaS, IaaS, applications, managed security services, remote access tools, analytics platforms, and provider-offered services.

Maintaining an accurate inventory of these services may be difficult because cloud technologies and services can be provisioned, modified, or removed rapidly. Continuous discovery tools may help maintain an accurate inventory of services.

Example Mitigating Controls

- Administrative Controls
  - **Maintain an inventory of external services supporting OT systems.**

    Establish and maintain an inventory of external services that support or interface with OT systems, including SaaS, PaaS, IaaS, and other third-party services. The inventory should identify the service's purpose, data sensitivity, integration points, and service ownership.
  - **Establish governance for onboarding and approving new external services.**

    Define and enforce processes for evaluating and approving new externally provided services before they interact with OT systems or sensitive operational data. Update inventory records when the organization authorizes or materially changes a service. Consider whether a service introduces unique support, access, or recovery dependencies for OT operations.
- Technical Controls
  - **Implement tools to continuously discover external services in use.**

    The organization should use appropriate monitoring and analysis methods to identify externally provided services interacting with OT systems. These methods may include DNS logs, network telemetry, identity and access logs, cloud configuration data, API activity records, and billing or usage reports. Cloud access security broker (CASB) tools can provide additional visibility into unsanctioned SaaS usage and data movement across cloud technologies. The organization should reconcile identified services against the authorized inventory.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 15: Service Provider Management

- CRI Cloud Profile v2.0 [CRI 2024]
  - ID.AM-04
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Supply Chain Management, Transparency, and Accountability (STA)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.9: Inventory of information and other associated assets
  - Control 5.19: Information security in supplier relationships
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - System and Services Acquisition (SA)

ID.AM-05 *Assets are prioritized based on classification, criticality, resources, and impact on the mission*

Potential Risks and Considerations

Integration of cloud technologies may change how assets and services should be classified and prioritized. In addition, integration of cloud technologies, such as centralized data platforms, remote access capabilities, or identity services, may introduce new dependencies. Consider how the loss or misuse of cloud technologies—or the assets they support—may impact important OT functions such as visibility, coordination, engineering support, or remote operations. Additionally, consider how negative impacts could increase in cases where individual cloud technologies support many operational functions or operational functions that are distributed over a broad geographic region.

Example Mitigating Controls

- Administrative Controls
  - **Define and apply prioritization criteria to cloud-supported OT assets.**

    Define criteria for prioritizing OT assets based on mission impact, operational criticality, data sensitivity, and external dependencies. Apply these criteria consistently to on-premises and cloud-supported assets, including externally hosted services that directly support OT functions.
  - **Periodically review asset prioritization as cloud dependencies evolve.**

    Review and update asset prioritization when cloud architectures, service models, or operational dependencies materially change. Reflect changes in OT dependency on cloud-hosted services in updated prioritization records.

- Technical Controls
  - **Use metadata and tagging to support classification and prioritization.**

    Use available cloud resource metadata, such as tags or labels, to associate cloud-supported assets with their mission criticality and operational role. Inventory and configuration management systems should reflect these priority designations.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - ID.AM-05
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Datacenter Security (DCS)
  - Data Security and Privacy Lifecycle Management (DSP)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.9: Inventory of information and other associated assets
  - Control 5.12: Classification of information
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Risk Assessment (RA)

ID.AM-07 *Inventories of data and corresponding metadata for designated data types are maintained*

Potential Risks and Considerations

Cloud integration may result in operational data being stored, processed, or transmitted within cloud environments. Operational data may reside in object storage, managed databases, analytics platforms, SaaS applications, and vendor-managed OT services. Provider-offered discovery and classification tools may help maintain an accurate data inventory, but their coverage depends on the services, data stores, and data formats they support. Some data may be more challenging to inspect, such as binary formats or compressed historian files. Provider-offered tools may need to be supplemented with additional inventory processes or information sources.

Data classification processes should account for how metadata, tags or labels are structured within specific cloud technologies. Some provider-offered tools may assign these attributes at the individual data-object level, while others may apply them more broadly, such as at the database, container, storage bucket, or account level.

Example Mitigating Controls

- Administrative Controls
  - **Extend data inventory and classification policies to cloud-supported OT environments.**

    Update data inventory and classification policies to address designated data types stored, processed, and transmitted in cloud technologies. Policies should define classification criteria, ownership responsibilities, and metadata requirements for cloud-supported OT data, consistent with on-premises practices.
- Technical Controls
  - **Implement data discovery and classification capabilities for cloud environments.**

    Use automated data discovery and classification tools, data security posture management (DSPM) tools, or equivalent third-party solutions to discover designated data types within cloud technologies and apply the appropriate classification labels or metadata. Configure the discovery scope to cover supported data stores that hold OT data, such as object storage, managed databases, and software integrations. Identify the remaining locations, including SaaS applications, logs, and backups, through architecture reviews and record them in the inventory. For unstructured data or proprietary binary operational files—such as historian archives, raw telemetry dumps, or system backups—use architecture reviews, application metadata, and specialized parsing where feasible to apply classification labels and record locations in the data inventory.
  - **Maintain metadata for designated cloud-hosted data.**

    Maintain metadata for designated data types in cloud environments, including data owner, classification level, storage location or region, and integration points with OT systems. Update inventory records when data is created, migrated, or materially changed.
- Cloud Provider Controls
  - **Provide mechanisms to support customer data classification and metadata management.**

    Provide functionality and sufficient granularity for cloud customers to apply classification labels, manage metadata, and configure data location settings for commonly identified data types.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 3: Data Protection

- CRI Cloud Profile v2.0 [CRI 2024]
  - ID.AM-07
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Data Security and Privacy Lifecycle Management (DSP)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.9: Inventory of information and other associated assets
  - Control 5.12: Classification of information
  - Control 5.13: Labelling of information
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Configuration Management (CM)

ID.AM-08 *Systems, hardware, software, services, and data are managed throughout their life cycles*

Potential Risks and Considerations

Lifecycle governance processes for OT assets may need to be adapted to accommodate integration of cloud technologies. Consider how to apply existing requirements for approval, oversight, and documentation to cloud technologies. Where feasible, leverage established lifecycle controls including procurement, security review, and architecture approval processes. New requirements may be necessary, such as requirements related to data ownership, retention, access control, monitoring, service retirement, and secure data destruction. Some requirements may need to be met by the cloud provider.

Cloud environments support rapid provisioning and configuration changes through practices like infrastructure-as-code (IaC). Activities such as provisioning, configuration changes, updates, scaling, and decommissioning may be supported by orchestration tools, APIs, and provider-managed processes. Using automated capabilities effectively can improve consistency and reduce errors in inventories, configuration baselines, data classification settings, and decommissioning records. Over time, inconsistencies and errors may result in unmanaged or residual resources, unintended data exposure, or incomplete retirement of systems supporting OT operations.

Example Mitigating Controls

- Administrative Controls
  - **Extend asset lifecycle management processes to cloud-supported OT systems.**

    Update lifecycle processes to address the OT assets, services, and workloads operating in cloud environments. Lifecycle processes should account for provisioning, configuration changes, scaling, transfer, and decommissioning of cloud-supported assets.
  - **Maintain records of asset movement and decommissioning in cloud environments.**

    Update inventories when cloud-supported OT assets are deployed, modified, transferred, or retired. Maintain records of decommissioning activities to support auditability and data retention requirements.
- Technical Controls
  - **Use provider-offered capabilities to track lifecycle events.**

    Use provider-offered logging, configuration history, and asset inventory to track provisioning, configuration changes, and retirements of cloud-supported OT assets.
  - **Configure cloud technologies to support data retention and secure disposal requirements.**

    Configure cloud technologies supporting OT systems to align with organizational data retention and destruction policies. The organization should document data lifecycle configurations, including retention periods and disposal methods, and periodically review them for conformance with legal and regulatory requirements.
- Cloud Provider Controls
  - **Support data retention and verifiable disposal.**

    Provide mechanisms to implement customer retention requirements. Document customer data disposal processes. Document deletion timeframes, retention exceptions, and limitations, and make completion status or assurance information available.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 1: Inventory and Control of Enterprise Assets
  - 2: Inventory and Control of Software Assets
  - 3: Data Protection

  - 4: Secure Configuration of Enterprise Assets and Software
- CRI Cloud Profile v2.0 [CRI 2024]
  - ID.AM-08
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Data Security and Privacy Lifecycle Management (DSP)
- IEC 62443-4-1:2018 [IEC 2018]
  - Practice 7: Security update management
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.9: Inventory of information and other associated assets
  - Control 8.9: Configuration management
  - Control 8.10: Information deletion
  - Control 8.19: Installation of software on operational systems
  - Control 8.27: Secure system architecture and engineering principles
  - Control 8.32: Change management
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Configuration Management (CM)
  - System and Services Acquisition (SA)
  - System and Information Integrity (SI)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - PR.DS: Data Security
  - PR.IP: Information Protection Processes and Procedures

3.2.2 Risk Assessment (ID.RA)

ID.RA-01 *Vulnerabilities in assets are identified, validated, and recorded*

Potential Risks and Considerations

Integrating cloud technologies into OT environments may introduce the potential for new types of vulnerabilities. Update vulnerability identification and analysis processes to account for potential vulnerabilities in customer-deployed workloads (such as operating systems or software), potential vulnerabilities in customer-managed cloud configurations, and potential vulnerabilities in cloud provider-managed services or underlying infrastructure. Consider how vulnerability analysis processes should

document potential impacts to important OT components or functions such as visibility, data flows, or recovery capabilities.

Example Mitigating Controls

- Administrative Controls
  - **Define vulnerability management responsibilities across service models.**

    For each provider-managed and organization-managed component, clearly delineate vulnerability identification, validation, remediation, and tracking responsibilities across SaaS, PaaS, and IaaS service models.
- Technical Controls
  - **Implement vulnerability identification and tracking for cloud-supported OT assets.**

    Use provider-offered or cloud-compatible vulnerability management tools to identify, validate, and record software vulnerabilities within organization-managed components, including guest operating systems, applications, and containers. Supplement these capabilities with automated configuration management capabilities to help detect misconfigurations, identity over-privileging, and policy drift.
  - **Standardize vulnerability tracking across cloud environments.**

    Normalize and record vulnerability findings in a consistent format to enable comparison, prioritization, and remediation tracking and reporting across all environments supporting OT systems.
- Cloud Provider Controls
  - **Identify vulnerabilities in provider-managed infrastructure.**

    Identify vulnerabilities in infrastructure and platform components and share findings relevant to customer workloads through reports, disclosures, or attestations.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 7: Continuous Vulnerability Management
- CRI Cloud Profile v2.0 [CRI 2024]
  - ID.RA-01
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Threat and Vulnerability Management (TVM)

- IEC 62443-4-1:2018 [IEC 2018]
  - Practice 5: Security verification and validation testing
  - Practice 6: Management of security-related issues
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 8.8: Management of technical vulnerabilities
- MITRE ATT&CK for ICS v19.2 [MITRE 2026]
  - M0916: Vulnerability Scanning
- NIST SP 800-30 Guide for Conducting Risk Assessments [NIST 2012]
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Risk Assessment (RA)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - ID.RA: Risk Assessment

ID.RA-02 *Cyber threat intelligence is received from information sharing forums and sources*

Potential Risks and Considerations

Integration of cloud technologies into OT operations may necessitate changes to threat intelligence gathering and analysis processes. Different sources start with different perspectives and provide different types of information. For example, OT-focused intelligence often emphasizes industrial control system vulnerabilities and operational impacts, while cloud-focused intelligence may emphasize identity abuse, misconfiguration, or multi-tenant risks.

Consider what combination of sources will provide sufficient coverage. Example sources to consider include energy sector information-sharing forums, government advisories, vendor reports, and intelligence offered by cloud providers. Consider how to integrate information from different sources into existing processes for analysis, prioritization, threat hunting, and detection.

Example Mitigating Controls

- Administrative Controls
  - **Establish processes to receive and integrate cyber threat intelligence relevant to cloud-supported OT systems.**

    Define and maintain processes to receive, review, and incorporate cyber threat intelligence from relevant sources, including energy sector information sharing forums, government advisories, vendors, and cloud provider channels. Ensure

that intelligence applicable to cloud-supported OT systems is evaluated for operational impact.

- Technical Controls
  - **Identify and prioritize sources of cyber threat intelligence.**

    Identify and prioritize threat intelligence sources that address threats to IT, OT, and cloud-based assets.
  - **Ingest and correlate cyber threat information across cloud-focused and OT-focused sources.**

    Configure security monitoring capabilities to ingest cyber threat intelligence feeds from multiple sources and correlate indicators relevant to cloud-supported OT systems. Correlation processes should account for differences in format, terminology, and technical focus across OT-oriented and cloud-oriented intelligence sources.
  - **Apply correlated intelligence to detection activities.**

    Integrate relevant threat intelligence into the monitoring, alerting, and threat hunting activities affecting cloud-supported OT systems to help speed detection of malicious activity.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - ID.RA-02
- IEC 62443-4-1:2018 [IEC 2018]
  - Practice 6: Management of security-related issues
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.7: Threat intelligence
- MITRE ATT&CK for ICS v19.2 [MITRE 2026]
  - M0919: Threat Intelligence Program
- NIST SP 800-30 Guide for Conducting Risk Assessments [NIST 2012]
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - System and Information Integrity (SI)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - ID.RA: Risk Assessment
- NIST SP 800-150 Guide to Cyber Threat Information Sharing [Johnson 2016]

ID.RA-03 *Internal and external threats to the organization are identified and recorded*

Potential Risks and Considerations

Integrating cloud technology into OT environments may change the potential impacts of existing threats or introduce new ones. Ensure that processes for identifying and recording threats cover cloud technologies and provider-managed capabilities that support OT functions. Threat actors may target these environments through identity abuse, API exploitation, management interface compromise, or the misuse of cloud provider-managed services. Consider threats that are non-adversarial in nature, such as human error, resource exhaustion, network outages, and cloud service failures. Document potential impacts to OT systems and operational processes and consider how dependencies and technologies that support multiple functions or regions may magnify potential impacts.

Cloud integration may increase the number of internal and external parties that can affect systems supporting OT operations. Threat identification processes should account for employees, third-party vendors, cloud providers, and external threat actors, along with the access paths available to them. These paths may include administrative interfaces, APIs, remote access services, delegated roles, and cloud provider support mechanisms. Centralized identity and access management services concentrate this exposure, so one compromised account or access path may reach multiple cloud services or OT security zones. The organization should leverage existing sources of information such as access and architecture reviews, cloud provider advisories, vendor reports, and sector information sharing to identify these threats.

Example Mitigating Controls

- Administrative Controls
  - **Identify and document internal and external threats affecting cloud-supported OT systems.**

    Update threat identification processes to account for cloud-specific attack vectors, including identity misuse, API exploitation, and provider-managed service compromise. Record identified threats affecting cloud-supported OT systems consistently to support tracking, analysis, and risk evaluation.
- Technical Controls
  - **Identify and monitor potential insider threat activity in cloud-supported OT environments.**

    Establish processes to detect and track malicious and non-malicious insider threat activity. Insiders are trusted individuals who have been granted authorized access. Insiders include internal personnel, contractors, and external service personnel who hold authorized or delegated access.

Monitoring should account for privileged access, federated identities, administrative API usage, and delegated roles.

- **Participate in sector-focused and cloud-focused threat information sharing.**

  Establish bi-directional threat information sharing with relevant energy sector forums, Information Sharing and Analysis Centers (ISACs), government entities, and cloud providers. Incorporate shared indicators into threat identification processes, particularly where cloud-focused and OT-focused threat activity may intersect.

- Cloud Provider Controls
  - **Identify and communicate threats affecting cloud hosting infrastructure.**

    Use internal threat research and external intelligence sources to identify threats targeting cloud infrastructure and shared services. Provide timely notification and relevant indicators to customers when such threats could affect tenant environments supporting OT systems.

  - **Identify and monitor potential insider threat activity within cloud provider operations.**

    Maintain processes to detect and record malicious and non-malicious insider activity that could affect cloud infrastructure or tenant environments, including services supporting OT systems.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - ID.RA-03
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Threat and Vulnerability Management (TVM)
- IEC 62443-4-1:2018 [IEC 2018]
  - Practice 6: Management of security-related issues
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.7: Threat intelligence
- NIST SP 800-30 Guide for Conducting Risk Assessments [NIST 2012]
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Risk Assessment (RA)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - ID.RA: Risk Assessment

- NIST SP 800-150 Guide to Cyber Threat Information Sharing [Johnson 2016]

ID.RA-04 *Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded*

Potential Risks and Considerations

Cloud integration can change the potential impacts and likelihoods of threats exploiting vulnerabilities in OT environments. The organization may need to adjust its existing risk assessment and threat analysis processes to reflect dependencies on provider-managed services, external network connectivity, and shared infrastructure. For latency-sensitive or mission-critical OT processes, a loss of availability, integrity, or predictable timing may cause operational, safety, environmental, or financial consequences comparable to those associated with on-premises OT assets. If risk scenarios omit these cloud-specific dependencies, the organization may underestimate the likelihood of the risk scenario occurring, the likelihood of exploitation where an adversarial path exists, or the resulting operational impact.

Risk scenarios involving cloud-supported OT systems should also account for concentration risk and cascading or systemic effects. These scenarios may include service outages, identity compromises, or misconfigurations that affect multiple workloads, sites, or geographic regions simultaneously. Evaluating shared dependencies and potential propagation paths across interconnected OT and enterprise systems may help estimate impact and likelihood more accurately.

Example Mitigating Controls

- Administrative Controls
  - **Extend risk assessment processes to cloud-supported OT systems.**

    Risk assessment processes should explicitly evaluate the likelihood and potential impact of threats exploiting vulnerabilities in cloud-supported OT environments. Scenarios should consider dependencies on provider-managed services, connectivity, identity platforms, and shared infrastructure. Document risks in a risk register alongside other operational risks. Engage operational, engineering, and business stakeholders to help ensure that estimates are accurate and defensible.
- Technical Controls
  - **Use automated tools to inform risk impact and likelihood evaluation.**

    Use cloud-native security tools, such as cloud security posture management (CSPM) tools, which identify misconfigurations, or cloud workload protection platforms (CWPPs), which identify vulnerabilities. Combine that information with threat intelligence, architectural analysis, incident history, and expert judgment when estimating likelihood.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - ID.RA-04
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Governance, Risk and Compliance (GRC)
  - Threat and Vulnerability Management (TVM)
- IEC 62443-4-1:2018 [IEC 2018]
  - Practice 6: Management of security-related issues
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.7: Threat intelligence
  - Control 8.8: Management of technical vulnerabilities
- NIST SP 800-30 Guide for Conducting Risk Assessments [NIST 2012]
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Risk Assessment (RA)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - ID.RA: Risk Assessment

ID.RA-05 *Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization*

Potential Risks and Considerations

Threat models that incorporate both OT- and cloud-specific attack scenarios can help the organization prioritize risk responses. These models should examine how threats and vulnerabilities interact across on-premises and cloud environments. Relevant scenarios may include compromised identities, API abuse, exploitation of misconfigured services, and supply chain compromise alongside traditional industrial control system threats. Models should consider inherent risk, which does not account for cybersecurity controls, as well as residual risk, which accounts for cybersecurity controls. When estimating inherent risk, evaluate the threat event before considering compensating controls. When estimating residual risk, account for controls and capabilities, such as cloud-based monitoring, managed detection, automated patching, and resilient architectures that may reduce likelihood, exposure, impact, or recovery time.

Consider dependencies when establishing risk response priorities for OT systems. Example dependencies to consider include cloud provider identity and access services, control planes (the administrative interfaces and APIs used to manage cloud resources), cloud service availability, and the cloud provider’s upstream dependencies.

The selected cloud service model determines which dependencies and security responsibilities the organization manages directly. These dependencies can change how threats reach cloud-supported OT systems and how disruptions affect operations.

Cloud capabilities may also improve resilience through geographic redundancy, scalable capacity, managed security services, and cloud-based recovery environments. Risk analysis should evaluate how these factors change the likelihood that threat events result in adverse impacts, the magnitude of those impacts, and the organization's ability to recover.

Example Mitigating Controls

- Administrative Controls
  - **Ensure risk assessment processes are comprehensive.**

    Risk assessment processes should account for cloud provider-managed dependencies, including identity and access services, cloud service control planes, and upstream providers, when evaluating threats and vulnerabilities affecting OT systems. The organization may use threat modeling frameworks to develop risk scenarios that reflect both OT- and cloud-related conditions. Document the resulting likelihood and impact estimates. Consider how to integrate this information with existing processes for assessment and prioritization of operational risks.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - ID.RA-05
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Governance, Risk and Compliance (GRC)
  - Threat and Vulnerability Management (TVM)
- IEC 62443-4-1:2018 [IEC 2018]
  - Practice 6: Management of security-related issues
- NIST SP 800-30 Guide for Conducting Risk Assessments [NIST 2012]
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Risk Assessment (RA)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - ID.RA: Risk Assessment

ID.RA-06 *Risk responses are chosen, prioritized, planned, tracked, and communicated*

Potential Risks and Considerations

Risk responses for cloud-supported OT systems may require coordinated activity by the organization and the cloud provider. Shared responsibility models, contracts, and service capabilities determine each party's role in identifying, reporting, remediating, and verifying risks. The organization should document cloud provider obligations in risk response plans and track whether the cloud provider fulfills them. An executive leader with sufficient authority should be identified and should decide whether residual risk to mission, safety, reliability, and cybersecurity falls within the organization's risk tolerance.

Risk responses implemented in cloud environments could impact OT systems and operations. When a response involves changes to cloud configurations, identity controls, or network architecture, the organization should evaluate proposed changes against OT operational requirements. Security improvements may alter traffic flows, authentication paths, or system configurations. A response action may be technically sound from a cybersecurity perspective but unsuitable for operational functions if it undermines timing, visibility, availability, or real-time processing characteristics.

Example Mitigating Controls

- Administrative Controls
  - **Integrate cloud-supported OT systems into risk response planning and tracking.**

    Risk management processes should account for how the organization selects, prioritizes, plans, and tracks responses to risks affecting cloud-supported OT systems. Risk response decisions should clearly distinguish between customer-managed and provider-managed responsibilities and document who owns remediation actions. Track planned responses through established mechanisms, such as a risk register or plan of action, and communicate them to relevant operational and leadership stakeholders to help ensure alignment with mission-critical OT requirements.
- Technical Controls
  - **Implement technical mechanisms to support a coordinated risk response in cloud-supported OT environments.**

    Use provider-offered configuration management, change management, and workflow tools to implement and track risk response actions affecting cloud-supported OT systems. Where risk responses involve provider-managed components, establish documented coordination procedures and technical interfaces, such as service tickets, escalation paths, or API-based requests, to ensure timely execution and visibility of remediation activities.

- Cloud Provider Controls
  - **Provide a tracked intake path for customer-reported risks.**

    Publish how customers report a risk or defect in a cloud service or its underlying infrastructure, and the severity definitions and response commitments that apply to each support offering. Track each report as a case, record its status, and respond to status requests. State when an issue moves into internal vulnerability management and what information customers receive about it. Identify what exposure remains for the customer.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - ID.RA-06
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Governance, Risk and Compliance (GRC)
  - Threat and Vulnerability Management (TVM)
- IEC 62443-4-1:2018 [IEC 2018]
  - Practice 6: Management of security-related issues
- NIST SP 800-30 Guide for Conducting Risk Assessments [NIST 2012]
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Risk Assessment (RA)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - ID.RA: Risk Assessment

ID.RA-07 *Changes and exceptions are managed, assessed for risk impact, recorded, and tracked*

Potential Risks and Considerations

The organization should update its change management process to address changes to cloud technologies that could affect OT systems and operational processes. This may include changes initiated by the cloud provider, such as routine maintenance, feature updates, or service retirements. Change management processes should evaluate, record, and track potential effects on safety, reliability, cybersecurity, and operations. The organization should also address provider-announced changes that may require the organization to act or confirm continued compatibility with OT requirements.

Example Mitigating Controls

- Administrative Controls
  - **Incorporate cloud technologies and integrations into formal change management processes.**

    Include cloud technologies and integrations that support OT systems in formal change and exception management processes. Before implementation, assess each proposed change and requested exception for potential effects on safety, operations, and security. Identify responsible parties, obtain required approvals, establish a rollback plan when feasible, and track the change or exception through completion.
  - **Establish a process to review and respond to cloud provider service changes.**

    Establish a process to review cloud provider notices about changes such as service updates, deprecations, maintenance events, and end-of-support timelines. Assess each relevant change for potential effects on safety, operations, and security. Assign and document required actions, then track them through completion. The process should also address changes that the cloud provider applies with little or no notice or changes that the organization cannot defer. Define how the organization will detect these changes, assess their effects, apply contingency or recovery measures, and document its response.
- Cloud Provider Controls
  - **Provide advance notification of service changes.**

    Provide advance notice of planned service changes, maintenance events, deprecations, or policy updates that may affect customer tenant environments.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 2: Inventory and Control of Software Assets
- CRI Cloud Profile v2.0 [CRI 2024]
  - ID.RA-07
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Change Control and Configuration Management (CCC)
- IEC 62443-4-1:2018 [IEC 2018]
  - Practice 6: Management of security-related issues
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 8.32: Change management

- NIST SP 800-30 Guide for Conducting Risk Assessments [NIST 2012]
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Configuration Management (CM)

ID.RA-08 *Processes for receiving, analyzing, and responding to vulnerability disclosures are established*

Potential Risks and Considerations

Responsibility for handling vulnerability disclosures differs across cloud service models. The organization should understand and document how responsibilities are delineated with the cloud provider, then build its vulnerability disclosure and response processes around those delineations. In IaaS deployments, the customer generally addresses vulnerabilities in guest operating systems, applications, and OT workloads, while the cloud provider manages vulnerabilities in underlying infrastructure. In PaaS, the cloud provider addresses platform components, while the customer remains responsible for its deployed applications, configurations, and integrations. In SaaS, the cloud provider generally remediates vulnerabilities in the service, while the customer evaluates its configurations, integrations, and potential effects on OT operations. Without clear ownership and coordination, remediation actions may be delayed or inconsistently applied.

Vulnerability disclosure processes should incorporate cloud provider advisories and other cloud provider notifications in addition to traditional software disclosures. These communications may describe infrastructure updates, service changes, configuration guidance, or exposure conditions that affect customer environments. The organization should develop a process to receive disclosures from cloud providers, vendors, or government sources, analyze them for relevance, and document and track them through established remediation processes.

Example Mitigating Controls

- Administrative Controls
  - **Incorporate cloud-related disclosures into vulnerability management processes.**

    Ensure that vulnerability management processes account for disclosures affecting cloud-supported OT systems, including cloud provider advisories, vendor notifications, and government alerts. Prioritize disclosures, assign ownership, and document and track them through remediation or risk acceptance processes.

- **Define shared vulnerability disclosure and notification requirements in contracts.**

  Establish contractual provisions that clarify roles, responsibilities, and notification timelines for vulnerability disclosures affecting provider-managed and customer-managed components. Contracts should define how each party communicates and escalates disclosures.

- Cloud Provider Controls
  - **Maintain and operate a coordinated vulnerability disclosure program.**

    Establish and maintain a public vulnerability disclosure program that enables researchers and others to responsibly report suspected vulnerabilities affecting cloud infrastructure or services. Analyze disclosures through established vulnerability management processes and notify customers when a vulnerability may materially impact customer environments or service resilience.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 7: Continuous Vulnerability Management
- CRI Cloud Profile v2.0 [CRI 2024]
  - ID.RA-08
- IEC 62443-4-1:2018 [IEC 2018]
  - Practice 6: Management of security-related issues
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.24: Information security incident management planning and preparation
  - Control 5.26: Response to information security incidents
  - Control 6.8: Information security event reporting
  - Control 8.8: Management of technical vulnerabilities
- NIST SP 800-30 Guide for Conducting Risk Assessments [NIST 2012]
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Risk Assessment (RA)

ID.RA-09 *The authenticity and integrity of hardware and software are assessed prior to acquisition and use*

Potential Risks and Considerations

Preconfigured cloud resources can accelerate deployment, but the organization should assess their authenticity and integrity before using them to support OT systems. Examples of these resources include virtual machines (VMs), machine images, containers, and software obtained through cloud provider marketplaces or similar sources. The organization should assess publisher reputation and software composition, and verify artifact authenticity and integrity using available provenance information. While marketplace resources may undergo cloud provider or third-party review, resources sourced from outside of formal marketplaces may not receive equivalent review.

Validate each resource's software configuration and behavior before deploying it in an environment that supports OT systems. Images and templates may include unapproved settings, unsupported components, or known vulnerabilities. Controlled testing, integrity verification, and comparison with approved baselines can identify conflicts with security and operational requirements before deployment.

Example Mitigating Controls

- Technical Controls
  - **Validate externally sourced resources before deployment.**

    Before deploying pre-configured resources obtained from cloud provider marketplaces or other sources, verify publisher reputation, software composition, and configuration integrity. These resources include VMs, machine images, containers, and templates. Test resources in controlled environments and compare them against approved baselines to confirm they align with security and operational requirements for OT systems.
- Cloud Provider Controls
  - **Validate the integrity of software components used to host cloud technologies.**

    Implement controls to validate the integrity of software operating within cloud infrastructure and pre-configured service offerings, such as verification against trusted publisher signatures, cryptographic hashes, or secure build processes.
  - **Validate the authenticity and integrity of hardware supporting cloud infrastructure.**

    Maintain supply chain validation and inspection processes to confirm hardware authenticity and detect unauthorized modification of infrastructure components used to deliver cloud technologies.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - EX.DD-04
- IEC 62443-3-3:2013 [IEC 2013]
  - Foundational Requirement 3: System integrity
- IEC 62443-4-1:2018 [IEC 2018]
  - Practice 4: Secure implementation
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.21: Managing information security in the ICT supply chain
  - Control 8.29: Security testing in development and acceptance
- MITRE ATT&CK for ICS v19.2 [MITRE 2026]
  - M0946: Boot Integrity
- NIST SP 800-30 Guide for Conducting Risk Assessments [NIST 2012]
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - System and Information Integrity (SI)
  - Supply Chain Risk Management (SR)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - ID.SC: Supply Chain Risk Management

ID.RA-10 *Critical suppliers are assessed prior to acquisition*

Potential Risks and Considerations

The organization may need to extend or tailor existing due diligence processes to address cloud-specific risks and dependencies. Many of the underlying review activities, such as evaluation of audit reports, security certifications, service commitments, data handling provisions, incident notification terms, or contract clauses related to portability and termination, are consistent with broader supplier risk management practices. However, cloud service models may require additional focus on shared responsibility boundaries, multi-tenant architectures, upstream infrastructure dependencies, and provider-managed change processes. Assessments of critical suppliers should evaluate how the supplier manages its own supply chain (including software development practices, infrastructure dependencies, and vulnerability response processes) to determine whether it aligns with the organization’s operational reliability, cybersecurity, and regulatory requirements.

Before acquisition, the organization should assess critical suppliers that provide cloud-delivered capabilities supporting OT processes. Many suppliers of process control platforms, monitoring solutions, analytics tools, or other OT-supporting technologies rely on cloud infrastructure or deliver cloud-hosted services in their offerings. Supplier assessments should evaluate the security of the product or service, the supplier's cloud architecture and hosting model, and dependencies on cloud providers or other suppliers. When detailed architectural information is unavailable, the organization may rely on available documentation, third-party attestations, and other assurance evidence. Without an assessment that covers both the direct supplier and its cloud dependencies, the organization may underestimate operational, cybersecurity, and data protection risks in cloud-supported OT environments.

Example Mitigating Controls

- Administrative Controls
  - **Assess the cloud dependencies of critical suppliers.**

    Before acquiring a product or service that relies on cloud infrastructure, perform a risk-based assessment of the supplier's cloud architecture, hosting model, and relevant security and resilience controls. Request appropriate documentation, such as audit reports, certifications, or descriptions of service continuity practices. Assess how the supplier manages upstream cloud dependencies, including vulnerability response, service availability, and data protection responsibilities.
  - **Establish contractual requirements for supply chain incident notification.**

    Include contractual provisions requiring suppliers to notify the organization, within defined timeframes, of cybersecurity or operational incidents affecting their services or upstream cloud dependencies. Notification requirements should apply where such incidents impact OT operations or sensitive data. Contracts should define reporting expectations, communication channels, and coordination responsibilities to support timely risk assessment and response.
  - **Periodically reassess critical suppliers and their cloud dependencies.**

    Establish processes to periodically reassess critical suppliers whose products or services support OT functions, including any reliance on cloud infrastructure or upstream service providers. Reassessments should consider material changes in architecture, service models, regulatory requirements, threats, and operational criticality. Update risk determinations and contractual or oversight mechanisms as needed so they continue to align with organizational security, reliability, and compliance objectives.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 15: Service Provider Management

- CRI Cloud Profile v2.0 [CRI 2024]
  - EX.DD-03
- IEC 62443-4-1:2018 [IEC 2018]
  - Practice 2: Specification of security requirements
  - Practice 6: Management of security-related issues
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.19: Information security in supplier relationships
  - Control 5.21: Managing information security in the ICT supply chain
- NIST SP 800-30 Guide for Conducting Risk Assessments [NIST 2012]
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Supply Chain Risk Management (SR)

3.2.3 Improvement (ID.IM)

ID.IM-01 *Improvements are identified from evaluations*

Potential Risks and Considerations

Evaluations of cloud-supported OT systems should account for how each cloud service model divides responsibilities between the organization and the cloud provider. Self-assessments, independent audits, and automated compliance checks should examine controls under the organization's direct control, including resource provisioning, configuration management, identity administration, and scaling. Evaluations should also consider cloud provider-managed controls, such as infrastructure maintenance and managed service updates, using available documentation and assurance evidence. Considering both areas helps the organization identify improvements and determine which party is responsible for implementing them.

Security evaluations should account for cloud-specific design elements alongside traditional OT security considerations. These elements may include identity-based access models, software-defined networking, service integrations, and configuration automation. Evaluations should determine how these elements interact with OT functions and whether controls remain effective as cloud dependencies, cloud provider services, and threats change. The organization should use findings to identify needed changes to configurations, architectures, and controls. If the organization does not address these findings, weaknesses may persist and increase the risk of operational disruption, regulatory consequences, or recurring incidents in environments affecting critical energy operations.

Example Mitigating Controls

- Administrative Controls
  - **Include cloud-supported OT systems within the cybersecurity evaluation scope.**

    Include cloud technologies and architectures that support OT systems within the scope of internal assessments and independent third-party reviews. Evaluations should address both customer-managed configurations and relevant provider-managed controls, consistent with shared responsibility boundaries. Assessments should identify control gaps, architectural weaknesses, and improvement opportunities affecting cloud-supported OT systems.
- Technical Controls
  - **Use continuous monitoring to inform security and resilience improvements.**

    Implement continuous monitoring across on-premises and cloud-supported OT environments to identify trends, recurring weaknesses, configuration drift, and control performance gaps. Continuous monitoring capabilities may operate periodically, on an event-driven basis (such as when configuration changes are made), or on an ongoing basis. Define frequencies and triggers appropriate to the risk and verify how each tool evaluates the environment. Use the results to check adherence to internal standards, regulatory obligations, and architectural baselines, and to drive corrective action.
  - **Integrate cloud security posture review and workload inspection capabilities into evaluation processes.**

    Deploy cloud security posture assessment capabilities to evaluate the control plane for configuration drift, overly permissive access policies, and network rules that depart from approved design. Be aware of OT workload conditions where specific safeguards might be necessary, such as agentless or low-impact workload protection capabilities, pre-deployment image scanning, and control plane guardrails to evaluate compliance without impairing operational stability.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - ID.IM-01
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Audit and Assurance (A&A)

- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.35: Independent review of information security
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Assessment, Authorization, and Monitoring (CA)

ID.IM-02 *Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties*

Potential Risks and Considerations

Cloud providers generally permit customer security testing within defined boundaries to protect platform stability and other tenants. The organization should review cloud provider testing policies, rules of engagement, and notification requirements before initiating penetration tests or other active assessments. Some managed or vendor-provided services may limit or prohibit the direct testing of the underlying infrastructure. In these cases, the organization should rely on available assurance artifacts, third-party assessments, and contractual mechanisms to supplement direct testing activities. Understanding these constraints in advance helps the organization plan and coordinate security assessments in cloud-supported OT environments.

The organization should use security tests and exercises to identify improvements across on-premises and cloud environments. Security tests should evaluate cloud configurations, identity dependencies, remote access paths, and data recovery mechanisms that support OT functions. Incident response, restoration, and business continuity exercises should include cloud-supported OT systems and coordination with cloud providers. Where feasible, the organization should use representative cloud environments to provide responders with practical experience.

The organization should document findings from tests and exercises, assign accountability for remediation, and track corrective actions to completion. The organization should prioritize findings based on their potential impact on cloud-supported OT systems, including findings about unrealistic recovery assumptions, cloud provider coordination gaps, or weak fallback procedures. The organization should also use exercise results to determine whether operators and engineers can use restored capabilities effectively under realistic operating conditions. If the organization does not implement identified improvements, known weaknesses may persist and increase the likelihood or impact of operational disruption affecting OT functions.

Example Mitigating Controls

- Administrative Controls
  - **Include cloud-supported OT services in security testing and exercise programs.**

    Expand the scope of security testing, tabletop exercises, and continuity simulations to include cloud technologies that support OT systems. Use results to identify improvement opportunities related to identity management, connectivity, recovery procedures, third-party coordination, and control effectiveness.
- Technical Controls
  - **Perform authorized testing of customer-managed cloud resources and configurations.**

    Conduct penetration testing, configuration assessments, and validation activities within the boundaries established by the cloud provider to assess the effectiveness of controls protecting cloud-supported OT systems. Where the cloud provider restricts direct testing of managed services, supplement testing activities by reviewing cloud provider assurance artifacts and third-party assessments.
  - **Conduct coordinated incident response and recovery exercises with critical suppliers.**

    Plan and execute joint incident response, restoration, and crisis simulations to validate communication channels, escalation procedures, and recovery workflows. Cloud-provider participation in customer exercises varies by provider, service, support offering, and agreement. Participation may be included in a premium or incident-response service, require a separate engagement, or be unavailable. Document lessons learned, assign remediation actions, and track completion to strengthen future response effectiveness.
- Cloud Provider Controls
  - **Define permitted security testing.**

    Publish service-specific security testing boundaries, prohibited activities, and approval or notification procedures.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 11: Data Recovery
  - 17: Incident Response Management
  - 18: Penetration Testing

- CRI Cloud Profile v2.0 [CRI 2024]
  - ID.IM-02
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Business Continuity Management and Operational Resilience (BCR)
  - Security Incident Management, E-Discovery, and Cloud Forensics (SEF)
  - Threat and Vulnerability Management (TVM)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.24: Information security incident management planning and preparation
- MITRE ATT&CK for ICS v19.2 [MITRE 2026]
  - M0947: Audit
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Assessment, Authorization, and Monitoring (CA)
  - Contingency Planning (CP)
  - Incident Response (IR)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - DE.CM: Security Continuous Monitoring

ID.IM-03 *Improvements are identified from execution of operational processes, procedures, and activities*

Potential Risks and Considerations

The organization can use information from routine operations in cloud-supported OT environments to identify improvements. Cloud platforms often provide activity logs, service performance metrics, usage trends, configuration records, and billing data. The organization can use this information to assess access control effectiveness, resource use, configuration consistency, and service performance. The organization can then refine identity policies, improve network segmentation and recovery strategies, or redesign workloads to reduce single points of failure.

Identifying improvements from routine operations in cloud-supported OT environments may require expertise in cloud architecture, data analysis, and platform governance. The organization should document and review lessons learned from routine operations, service disruptions, configuration drift, or coordination challenges with cloud providers. These lessons should inform updates to procedures and architectural decisions. If the organization does not act on them, inefficient processes, control weaknesses, and

resilience gaps may persist and increase the risk of disruptions or incidents affecting OT functions.

Example Mitigating Controls

- Technical Controls
  - **Analyze operational metrics to identify and track improvement opportunities.**

    Use capabilities offered by the cloud provider or third-party tools to collect and analyze operational and security metrics for cloud-supported OT functions. Evaluate trends in access activity, configuration drift, service performance, logging coverage, and resource utilization to identify improvement opportunities. Document findings and track corrective actions, such as refining access controls, strengthening monitoring and alerting, improving resilience configurations, and optimizing resource use, to support reliable and secure operations.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 17: Incident Response Management
- CRI Cloud Profile v2.0 [CRI 2024]
  - ID.IM-03
- IEC 62443-4-1:2018 [IEC 2018]
  - Practice 1: Security management
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.27: Learning from information security incidents
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Contingency Planning (CP)
  - Incident Response (IR)
  - Program Management (PM)

ID.IM-04 *Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved*

Potential Risks and Considerations

The organization should update incident response and related cybersecurity plans to address cloud technologies that support OT functions. Core response principles, such

as containment, eradication, recovery, and communication, remain consistent across on-premises and cloud environments. However, response procedures may differ when an incident originates in or affects cloud-supported environments. Actions may include isolating cloud resources, revoking credentials or active sessions, restoring workloads from snapshots, redeploying resources from approved templates, or coordinating with a cloud provider on managed services. Plans should address identity layers, control planes, infrastructure components, and application services. They should explain how incidents at each layer may affect OT operations.

Response and recovery plans for cloud-supported OT systems should define responsibilities and identify the services required to restore operations. Restoration workflows, such as redeploying resources through IaC or restoring virtualized workloads from snapshots, may depend on control planes, identity and key management services, code repositories, and network connectivity. If these dependencies are unavailable or compromised, automated recovery may be delayed or blocked. Plans should state which actions the organization can perform and which require cloud provider support. They should also provide protected emergency administrative access that does not rely on the primary identity path, preserve authorized access to required keys and recovery artifacts, and define fallback procedures that minimize control plane dependencies.

Contracts and operational agreements should support response and recovery plans by defining cloud provider notification time frames, escalation paths, evidence preservation and sharing procedures, and recovery commitments. These provisions should cover incidents affecting the organization's cloud tenants, provider-managed services, and underlying infrastructure. Plans should also define post-restoration validation steps and acceptance criteria for OT functionality, data integrity, connectivity, and performance. The organization should communicate plans to relevant stakeholders and update them as architectures, responsibilities, lessons learned, and threats change. Poorly documented, coordinated, or maintained plans can delay containment, prolong recovery, or result in incomplete remediation.

Example Mitigating Controls

- Administrative Controls
  - **Update and maintain incident response and recovery plans for cloud-supported OT environments.**

    Expand incident response, business continuity, and disaster recovery plans to address cloud-hosted workloads and dependencies between OT and cloud environments. Define roles, escalation pathways, containment actions, and restoration procedures across organization and cloud provider responsibility boundaries. Identify and test critical recovery dependencies, including identity and key management services, cloud control planes, network connectivity, backups, and deployment templates. Maintain protected emergency administrative access that does not rely on the primary identity path. Review

and update plans periodically and after exercises, incidents, or significant service and architecture changes.

- **Establish contractual and operational coordination procedures with cloud providers.**

  Define and document coordination mechanisms with cloud providers and other critical suppliers for incident notification, escalation, information sharing, and recovery support. Ensure that plans align with contractual obligations and specify communication channels, timelines, and points of contact for incidents affecting cloud-supported OT operations.

- **Validate cloud-specific response and recovery capabilities through exercises.**

  Periodically test incident response and recovery procedures for cloud-supported OT systems through tabletop exercises, technical simulations, or restoration tests. Validate the organization's ability to isolate affected resources, restore data and configurations, and coordinate with cloud providers. Document findings and incorporate identified improvements into updated plans.

- **Review and update cybersecurity-related plans, procedures, standards, and other documentation to address cloud-supported OT environments.**

  Cloud integration in OT environments may require the organization to holistically review cybersecurity-related plans, procedures, standards, and related documentation beyond incident response and recovery plans. These updates should reflect changes in architecture, responsibilities, dependencies, and operational requirements so governance and technical implementation remain aligned.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 17: Incident Response Management
- CRI Cloud Profile v2.0 [CRI 2024]
  - ID.IM-04
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Business Continuity Management and Operational Resilience (BCR)
  - Security Incident Management, E-Discovery, and Cloud Forensics (SEF)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.24: Information security incident management planning and preparation

  - Control 5.29: Information security during disruption
  - Control 5.30: ICT readiness for business continuity
  - Control 5.37: Documented operating procedures
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Configuration Management (CM)
  - Contingency Planning (CP)
  - Incident Response (IR)
  - Program Management (PM)
  - Supply Chain Risk Management (SR)
- NIST SP 800-61 Rev. 3 Incident Response Recommendations and Considerations for Cybersecurity [Nelson 2025]
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - PR.IP: Information Protection Processes and Procedures

3.3 Protect (PR)

The Protect Function comprises five Categories:

- Identity Management, Authentication, and Access Control (PR.AA)
- Awareness and Training (PR.AT)
- Data Security (PR.DS)
- Platform Security (PR.PS)
- Technology Infrastructure Resilience (PR.IR)

3.3.1 Identity Management, Authentication, and Access Control (PR.AA)

PR.AA-01 *Identities and credentials for authorized users, services, and hardware are managed by the organization*

Potential Risks and Considerations

Integration of cloud technologies within OT environments may require changes to—or entirely new—processes or tools for managing identities and credentials. Cloud architectures may use federated identity models, token-based authentication, and automated provisioning. These capabilities can expand the number and types of identities, including non-human identities such as service accounts, workload identities, or automated access through APIs. The organization should assign a unique, attributable identity to each service, device, or integration. Inventory long-lived credentials and federation trust relationships. For short-lived tokens, govern and monitor attributes such as the issuer, subject, scope, and use rather than attempting to inventory every token.

Cloud control planes can give privileged identities broad authority over identity, networking, storage, and compute services. When identity services are federated across OT and cloud environments, one compromised privileged credential may provide access to several platforms. APIs and automation can increase the scale and speed of unauthorized actions. The organization should identify privileged human and non-human identities, including emergency accounts, federated administrator accounts, and privileged service identities, and manage their credentials throughout their lifecycles.

Virtualized OT assets and cloud-deployed workloads may include default or widely known credentials, just as on-premises assets may. Reusable images and templates can replicate the same credential across many resources. Rapid provisioning may also leave default credentials unchanged if provisioning processes do not require their replacement. The organization should identify and replace default credentials during provisioning and prevent images and templates from distributing shared secrets. If these resources support or connect to OT environments, unmanaged credentials may allow users to gain or maintain access.

Example Mitigating Controls

- Technical Controls
  - **Extend identity lifecycle management processes to include cloud-integrated OT environments.**

    Adapt existing identity and access management processes to include cloud-based user accounts, service accounts, machine identities, and workload identities. Apply provisioning, modification, and deprovisioning processes consistently across OT and cloud systems.
  - **Monitor identity provisioning and privileged activity within cloud tenants.**

    Configure logging and monitoring capabilities to detect new account creation, privilege changes, credential issuance, and anomalous authentication activity. Integrate relevant logs with centralized monitoring platforms, such as a security information and event management (SIEM) platform, to support cross-domain visibility and periodic review of privileged access.
- Cloud Provider Controls
  - **Provide identity and credential lifecycle capabilities.**

    Provide administrative interfaces that create, inventory, modify, and deactivate the user, service, device, and workload identities the service supports. Support unique attribution for each identity and manage the issuance, rotation, and revocation of its credentials. Document how long lifecycle changes take to propagate and identify the credentials and access paths that need a separate action to revoke.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 5: Account Management
- CRI Cloud Profile v2.0 [CRI 2024]
  - PR.AA-01
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Cryptography, Encryption & Key Management (CEK)
  - Identity and Access Management (IAM)
- IEC 62443-3-3:2013 [IEC 2013]
  - Foundational Requirement 1: Identification and authentication control
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.16: Identity management
  - Control 5.17: Authentication information

- MITRE ATT&CK for ICS v19.2 [MITRE 2026]
  - M0918: User Account Management
  - M0926: Privileged Account Management
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Identification and Authentication (IA)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - PR.AC: Identity Management and Access Control

PR.AA-02 *Identities are proofed and bound to credentials based on the context of interactions*

Potential Risks and Considerations

Identity-proofing and credential-binding requirements should reflect the consequences of granting access to an impostor. These requirements should cover employees and third parties whose identities the organization provisions or authorizes in its environments and whose access can affect important systems, data, or processes. These parties may include cloud provider personnel, contractors, vendors, or managed service providers who access the organization's tenant. Cloud providers remain responsible for identity-proofing personnel who administer provider infrastructure. The organization evaluates those practices through contractual requirements and assurance evidence. Potential effects on safety, reliability, and operations should inform the overall identity assurance approach, including selection of identity assurance levels (IALs) to decide how rigorously to proof human identities. The organization should limit instances of shared identities that would weaken the association between an individual and activity recorded in audit logs.

Example Mitigating Controls

- Administrative Controls
  - **Consider standards-based identity assurance levels.**

    NIST SP 800-63A-4 provides identity proofing guidance for federal agencies, credential service providers, and other organizations that use identity proofing services [Temoshok 2025a]. Energy organizations may consider its IAL model as a reference for deciding how rigorously to verify the identity of people who access cloud technologies that support OT environments.
  - **Require unique, attributable identities for third-party access.**

    Issue individual, uniquely attributable identities to third parties who access OT systems or cloud-integrated services. Prohibit credential sharing where feasible and define proofing and credential-binding requirements consistent with the level of access granted.

- Technical Controls
  - **Enforce identity proofing and authenticator binding for accounts.**

    Implement identity proofing and enrollment processes commensurate with the defined assurance requirements and context of use. Bind approved authenticators to unique accounts, and ensure that provisioning, modification, and deprovisioning processes maintain traceability between the identity record, the account, and associated authenticators.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 5: Account Management
- CRI Cloud Profile v2.0 [CRI 2024]
  - PR.AA-02
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Identity and Access Management (IAM)
- IEC 62443-3-3:2013 [IEC 2013]
  - Foundational Requirement 1: Identification and authentication control
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.16: Identity management
  - Control 5.17: Authentication information
- MITRE ATT&CK for ICS v19.2 [MITRE 2026]
  - M0918: User Account Management
  - M0926: Privileged Account Management
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Identification and Authentication (IA)
- NIST SP 800-63A-4 [Temoshok 2025a]
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - PR.AC: Identity Management and Access Control
  - Remote Access

PR.AA-03 *Users, services, and hardware are authenticated*

Potential Risks and Considerations

Authentication practices in OT environments that integrate cloud technologies may differ from legacy OT implementations. Cloud environments may introduce federated identity systems, multifactor authentication (MFA), conditional access policies, and provider-specific authentication architectures. Cloud identity services may provide authentication mechanisms that can be configured as part of authentication processes designed to meet higher authentication assurance levels (AALs). Integrating these mechanisms across multiple cloud providers and legacy OT components may require the organization to coordinate architectures to enforce authentication requirements consistently. The organization should consider phishing-resistant MFA for privileged and remote access where feasible and configure other MFA methods to resist MFA-fatigue attacks.

The organization should set session, access-token, and refresh-token lifetimes based on risk; require reauthentication before privileged, safety-relevant, or other high-impact actions; and revoke sessions and tokens promptly where supported. Where immediate access-token revocation is not supported, use short token lifetimes and available session termination, refresh-token revocation, shared signaling, or other compensating mechanisms.

Identity as a service (IDaaS) solutions centralize authentication across on-premises and cloud environments. These services deliver single sign-on (SSO) and federated identity architectures that can improve visibility and control when the organization properly governs, configures, and monitors them. Centralized authentication services may reduce password sprawl, simplify revocation, and help the organization enforce MFA and session management controls consistently across multiple cloud providers and OT-connected systems. However, they may also create operational dependency on centralized identity services, so the organization should define how it will maintain authorized access during identity service disruption, degraded operations, or recovery. The organization should consider architectural approaches that maintain authentication integrity and operational continuity, particularly in environments that access critical OT functions.

The environment’s authentication design should address non-human entities. These include devices, applications, APIs, service accounts, and cloud technologies that exchange data or perform automated actions in cloud-integrated OT environments. Where appropriate, mutual authentication can help prevent unauthorized system-to-system interactions. Authentication mechanisms should account for operational compatibility, latency sensitivity, emergency access, and restoration needs so that stronger authentication does not unintentionally impair safe and reliable operations.

Example Mitigating Controls

- Technical Controls
  - **Enforce strong authentication mechanisms for access to cloud-integrated OT environments.**

    Where the organization uses passwords, enforce password policies consistent with applicable organizational requirements and current standards. Require MFA for user and administrative access to cloud technologies that support OT environments. Where feasible, implement phishing-resistant authentication mechanisms, such as hardware security keys or device-bound passkeys, for privileged or high-risk access. Where supported, use conditional access policies to enforce context-aware authentication decisions based on user role, device compliance, and network location.
  - **Consider standards-based authentication assurance levels.**

    NIST SP 800-63B-4 defines authentication requirements for federal agencies [Temoshok 2025b]. Energy organizations may consider its AAL model as a reference for deciding how strongly to authenticate users in cloud-supported OT environments.
  - **Apply compensating controls for legacy or constrained OT assets.**

    Where OT systems or virtualized workloads cannot support modern authentication mechanisms directly, require phishing-resistant MFA to a controlled intermediary and prohibit alternative access paths. Record and monitor privileged sessions.
  - **Design and maintain resilient authentication infrastructure.**

    Design and maintain resilient authentication infrastructure that supports OT functions to withstand a cloud or identity provider outage. Consider redundant authentication capabilities across geographic regions or environments. Maintain a locally survivable authentication path for critical OT functions that must remain accessible when centralized identity services are unavailable. Consider emergency access procedures with credentials in offline or separately administered systems, restrict their use to defined conditions, and alert on every use.
- Cloud Provider Controls
  - **Support session revocation and an independent administrative access path.**

    Let customers configure authentication policies, session lifetimes, and reauthentication requirements for the service. Provide a mechanism for session and token revocation. Document, for each access-token type, how quickly revocation takes effect. Provide an emergency administrative access method that works when the customer’s federated identity service is unavailable. Protect it with strong authentication and restricted privileges and record every use.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 6: Access Control Management
- CRI Cloud Profile v2.0 [CRI 2024]
  - PR.AA-03
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Datacenter Security (DCS)
  - Identity and Access Management (IAM)
- IEC 62443-3-3:2013 [IEC 2013]
  - Foundational Requirement 1: Identification and authentication control
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.16: Identity management
  - Control 5.17: Authentication information
  - Control 8.5: Secure authentication
- MITRE ATT&CK for ICS v19.2 [MITRE 2026]
  - M0802: Communication Authenticity
  - M0804: Human User Authentication
  - M0813: Software Process and Device Authentication
  - M0927: Password Policies
  - M0932: Multi-factor Authentication
  - M0936: Account Use Policies
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Identification and Authentication (IA)
- NIST SP 800-63B-4 [Temoshok 2025b]
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - PR.AC: Identity Management and Access Control
  - Remote Access

PR.AA-04 *Identity assertions are protected, conveyed, and verified*

Potential Risks and Considerations

The organization should protect and validate identity assertions used for federated access to cloud-integrated OT environments. An assertion conveys authentication and identity information from an identity provider to the cloud service that relies on it. Implementations should use standards-based federation protocols and authenticated, protected channels. Before granting access, the receiving service should verify the assertion's issuer, signature, intended audience, and validity period. In most cases the cloud service performs this validation, and the organization's role is to configure the trust relationship correctly and keep signing keys current. The organization performs the validation itself for applications it builds and operates in its own tenant. Short validity periods reduce the time available for misuse but do not prevent replay. The receiving service should also enforce replay protection, such as validating a nonce or rejecting an assertion identifier that it has already accepted.

Cloud technologies may be accessed through multiple pathways. Users and systems may use web-based portals, APIs, secure shell (SSH) sessions, or automated service-to-service communications to access cloud services. Depending on the implementation, these pathways may use federated identity assertions, access tokens, certificates, or other credentials. The organization should apply the protection and verification requirements appropriate to each mechanism. Without the consistent enforcement of approved authentication flows and verification mechanisms, the organization risks bypassing federated controls or introducing weak integration points that undermine identity assurance.

Example Mitigating Controls

- Technical Controls
  - **Consider standards-based protection and validation of identity assertions.**

    NIST SP 800-63C-4 defines federation requirements for federal agencies [Temoshok 2025c]. Energy organizations may consider its federation assurance level (FAL) model as a reference for deciding how strongly to protect identity assertions in cloud-supported OT environments.
  - **Enforce approved authentication flows and restrict unsupported access methods.**

    Configure cloud technologies to require approved federation or authentication mechanisms. Disable or restrict alternative access pathways that bypass centralized identity controls. Monitor the cloud environment for unauthorized or misconfigured authentication integrations. Some highly privileged accounts, such as the organization's root administrative account, may authenticate outside the federated path and may not support federation in all cloud provider

architectures. Protect these accounts with phishing-resistant MFA and credential protection. Restrict their use to approved emergency access and administrative tasks that the cloud provider requires them to perform. Do not use them for routine administration, and alert on every use.

- Cloud Provider Controls
  - **Protect and validate federated identity assertions.**

    Protect identity assertions exchanged through federation interfaces. Validate each assertion's issuer, signature, intended audience, and validity period before granting access. Apply replay protection appropriate to the protocol. Provide settings that let customers restrict which identity sources and authentication paths the service trusts. Identify the privileged accounts and interfaces those settings do not reach.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - PR.AA-04
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Identity and Access Management (IAM)
- IEC 62443-3-3:2013 [IEC 2013]
  - Foundational Requirement 1: Identification and authentication control
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.17: Authentication information
  - Control 8.5: Secure authentication
  - Control 8.24: Use of cryptography
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Identification and Authentication (IA)
- NIST SP 800-63C-4 [Temoshok 2025c]
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - PR.AC: Identity Management and Access Control

PR.AA-05 *Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties*

Potential Risks and Considerations

Principles for managing access permissions are consistent across on-premises and cloud-supported OT environments. However, the organization may implement them differently in each environment. In IaaS, the cloud provider's identity and access management framework controls access to cloud control plane functions, such as provisioning virtual machines, modifying virtual networks, or assigning roles and permissions. The organization typically manages separate permissions within guest operating systems and applications. PaaS and SaaS services may enforce authorization through service-level or application-level roles. Resource-based policies and trust relationships across accounts or tenants may grant additional access. The organization should evaluate the combined effect of these authorization layers to enforce least privilege and separation of duties.

Role-based access control (RBAC) and attribute-based access control (ABAC) can support least privilege in cloud-integrated OT environments. These models restrict access based on assigned role or defined attributes, such as identity, requested action, location, time of access, or device posture. However, some legacy OT systems or protocols cannot use modern identity and authorization services. In these cases, the organization may need intermediary controls or compensating mechanisms to maintain equivalent control over OT-relevant access.

Third-party access to cloud-supported OT environments requires coordinated permission management across cloud and OT systems. Third parties, such as vendors or managed service providers, may require privileged or remote access to perform maintenance activities. The organization should clearly define and limit each party's permissions, grant access only for the required period, and review permissions regularly. Weak permission management may create excessive privileges, accounts that remain active after access is no longer needed, or conflicts with separation of duties requirements. These conditions may enable unauthorized access, privilege escalation, or misuse of retained access.

Example Mitigating Controls

- Administrative Controls
  - **Revoke access appropriately following role changes or termination.**

    Promptly revoke or modify access to cloud technologies that support OT environments when personnel change roles or leave the organization. These modifications include disabling accounts, revoking credentials, and updating role assignments to prevent residual or unauthorized access.

- **Conduct periodic entitlement and policy reviews.**

  Regularly review user accounts, role assignments, and access policies across cloud-integrated OT environments, and carefully scrutinize privileged roles. Reviews should validate continued business need, enforce separation of duties, and identify excessive permissions.

- Technical Controls
  - **Enforce RBAC and ABAC for cloud-supported OT systems.**

    Configure cloud identity and access management policies to restrict access to OT-related resources based on defined roles, attributes, and operational responsibilities. Ensure that access assignments align with least privilege and separation of duties principles. Consider using privileged access management (PAM) tools to enforce credential vaulting, session recording, and time-limited access for administrative and privileged accounts that support OT-connected cloud environments.

  - **Use just-in-time access for privileged and third-party access to cloud-supported OT environments.**

    Configure cloud identity and access management (IAM) or PAM tools to grant time-bound, on-demand elevated access rather than standing privileges. Native just-in-time (JIT) capabilities vary by cloud provider and may require premium identity licensing or a third-party solution. Apply JIT patterns for vendor and contractor access to cloud resources that support OT. Require approval workflows and log all JIT access grants.

  - **Implement entitlement visibility and monitoring mechanisms.**

    Deploy cloud infrastructure entitlement management (CIEM) tools or native cloud IAM analysis features that provide visibility into permission assignments, privilege inheritance, and cross-account access. Use these capabilities to detect excessive entitlements, policy misconfigurations, and privilege escalation risks across cloud environments that support OT operations.

- Cloud Provider Controls
  - **Expose effective permissions and support authorization boundaries.**

    Provide authorization controls that restrict access by role, resource, action, and supported contextual attributes. Support least privilege, separation of duties, and time-limited privileged access, either directly or through compatible integrations. Expose role assignments, resource policies, inherited permissions, and cross-account trust settings so customers can review the combined effect. Document policy precedence and the enforcement limits that apply.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 6: Access Control Management
- CRI Cloud Profile v2.0 [CRI 2024]
  - PR.AA-05
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Identity and Access Management (IAM)
- IEC 62443-3-3:2013 [IEC 2013]
  - Foundational Requirement 2: Use control
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.2: Information security roles and responsibilities
  - Control 5.3: Segregation of duties
  - Control 5.15: Access control
  - Control 5.18: Access rights
  - Control 8.2: Privileged access rights
  - Control 8.3: Information access restriction
  - Control 8.18: Use of privileged utility programs
- MITRE ATT&CK for ICS v19.2 [MITRE 2026]
  - M0800: Authorization Enforcement
  - M0801: Access Management
  - M0922: Restrict File and Directory Permissions
  - M0947: Audit
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Access Control (AC)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - PR.AC: Identity Management and Access Control

PR.AA-06 *Physical access to assets is managed, monitored, and enforced commensurate with risk*

Potential Risks and Considerations

Responsibility depends on who operates the facility and the equipment. The organization manages physical access to its OT devices and facilities. The cloud provider manages physical access to its datacenters. The organization generally evaluates the cloud provider's controls through independent audit reports, certifications, and other assurance evidence. This evaluation should determine whether the controls meet the organization's operational risk management needs.

Cloud integration does not transfer the responsibility for physical access to organization-managed field equipment, network infrastructure, or edge devices. Maintenance personnel and third parties, such as vendors or contractors, may require physical access to assets that communicate with cloud services. The organization should establish access restrictions, escort requirements, and monitoring practices based on the criticality of the OT systems these assets support.

Example Mitigating Controls

- Administrative Controls
  - **Review assurance artifacts for the cloud provider's physical security controls.**

    During procurement and contracting, review cloud provider documentation and independent assurance artifacts. For example, consider SOC 2® Type II reports or ISO/IEC 27001 certifications [AICPA & CIMA 2026, ISO/IEC 2022]. Evaluate whether documented controls align with organizational risk management expectations for systems that support OT operations. Address identified gaps through contractual mechanisms or risk acceptance processes.
- Physical Controls
  - **Manage physical access to OT facilities and edge infrastructure.**

    Restrict and monitor physical access to OT devices, field equipment, and edge devices that interface with cloud technologies. Apply controls commensurate with system criticality, including managing visitors, logging access events, and escorting third-party personnel.
- Cloud Provider Controls
  - **Restrict and monitor physical access to provider-managed facilities.**

    Limit physical access to datacenter facilities and infrastructure to personnel with defined roles and business need. Enforce access through layered controls, such as badge systems, surveillance, and access logging, in accordance with contractual commitments and applicable standards. Control visitor access to

sensitive areas of facilities through registration, identity verification, escorting where appropriate, and time-bound access approvals.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - PR.AA-06
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Datacenter Security (DCS)
  - Human Resources (HRS)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 7.1: Physical security perimeters
  - Control 7.2: Physical entry
  - Control 7.3: Securing offices, rooms and facilities
  - Control 7.4: Physical security monitoring
  - Control 7.5: Protecting against physical and environmental threats
  - Control 7.12: Cabling security
- MITRE ATT&CK for ICS v19.2 [MITRE 2026]
  - M0934: Limit Hardware Installation
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Physical and Environmental Protection (PE)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - PR.AC: Identity Management and Access Control
  - DE.CM: Security Continuous Monitoring

3.3.2 Awareness and Training (PR.AT)

PR.AT-01 *Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind*

Potential Risks and Considerations

Cybersecurity awareness programs should address how cloud integration changes risk to OT systems. Relevant personnel should understand shared responsibility, identity

and access management, secure configuration, and the risks associated with internet-accessible services. Traditional cybersecurity principles still apply, but cloud adoption can change system architectures, access paths, and potential attack surfaces.

Awareness training should connect common cloud-related threats and actions to their potential effects on OT operations and safety. Examples include publicly exposed storage resources, excessive permissions, misuse of service accounts, and phishing attempts that target federated accounts. Training should also address risks from third-party integrations and software supply-chain dependencies. Personnel should understand that actions taken through cloud management interfaces can affect OT operations without directly interacting with physical equipment.

Example Mitigating Controls

- Administrative Controls
  - **Incorporate cloud-related topics into general cybersecurity awareness programs.**

    Ensure that cybersecurity awareness training includes foundational concepts related to the cloud technologies that support OT environments, including shared responsibility, identity and access risks, secure configuration expectations, and reporting procedures for suspected cloud-related incidents. Training should emphasize how cloud-integrated systems can affect OT operations and safety, where applicable.
  - **Establish baseline security awareness expectations for third parties.**

    Require contractors and third-party personnel with access to cloud-supported OT environments to complete security awareness training consistent with organizational policies. Contracts should define requirements for acceptable use, credential protection, and incident reporting.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 14: Security Awareness and Skills Training
- CRI Cloud Profile v2.0 [CRI 2024]
  - PR.AT-01
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Human Resources (HRS)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 6.3: Information security awareness, education and training

- MITRE ATT&CK for ICS v19.2 [MITRE 2026]
  - M0917: User Training
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Awareness and Training (AT)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - PR.AT: Awareness and Training

PR.AT-02 *Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind*

Potential Risks and Considerations

Personnel who design, configure, administer, or secure OT systems need training that reflects their assigned cloud responsibilities. Training should address how configuration errors and improper privilege assignments can affect OT operations and safety. It should also account for differences among cloud platforms, hybrid architectures, and service models. In IaaS, personnel may configure virtual compute, identity, and networking controls. In PaaS, they may configure applications, data, identities, integrations, and service-level security settings. In SaaS, training may focus on application configuration, data protection, and the organization's responsibilities under contracts and shared responsibility models. Personnel who use cloud-hosted cybersecurity or operational tools may also need training on tool functions and the handling of OT data.

OT operators need role-specific training when operational processes depend on cloud technologies. Operators may not manage cloud resources directly, but they should understand how connectivity loss, authentication failures, and configuration changes can affect safety, availability, and resilience. This knowledge helps them make informed decisions during planned changes, service disruptions, and cybersecurity incidents involving cloud-supported OT systems.

Example Mitigating Controls

- Administrative Controls
  - **Establish role-based cloud security training requirements for specialized roles.**

    Define training requirements for personnel whose responsibilities include architecting, configuring, administering, or securing cloud-integrated OT environments. Require personnel to complete role-appropriate training before they receive elevated or sensitive access. Training should address secure configuration, identity and access controls, resilience features, and how

changes in the cloud environment affect OT systems. Training programs offered by the cloud provider and role-based certification paths may serve as a baseline for establishing and validating cloud security competency for relevant personnel.

- **Define qualification requirements for third-party personnel with specialized cloud access.**

  Include contractual provisions that specify training, experience, or certification expectations for third-party personnel who administer or maintain cloud technologies that support OT environments. Qualification requirements should align with the level of access granted and the criticality of the systems supported.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 14: Security Awareness and Skills Training
- CRI Cloud Profile v2.0 [CRI 2024]
  - PR.AT-02
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Human Resources (HRS)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 6.3: Information security awareness, education and training
- MITRE ATT&CK for ICS v19.2 [MITRE 2026]
  - M0913: Application Developer Guidance
  - M0917: User Training
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Awareness and Training (AT)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - PR.AT: Awareness and Training

3.3.3 Data Security (PR.DS)

PR.DS-01 *The confidentiality, integrity, and availability of data-at-rest are protected*

Potential Risks and Considerations

Encryption is a key control for protecting the confidentiality of data at rest in cloud environments. Protecting integrity and availability also requires controls such as access restrictions, integrity validation, backups, redundancy, and ensuring that cryptographic keys remain available when data must be accessed or restored. Available key management options vary by cloud provider and service. Common examples include provider-managed keys, customer-managed keys held in the cloud provider's key management service, customer-provided keys supplied with each request, customer-generated key material imported into a cloud provider service, and keys held outside the cloud provider environment. These options differ in who controls the keys, where key material resides, who operates the key management service, and how the cloud service uses the keys. Those differences affect access control, revocation, availability dependencies, and the organization's ability to meet regulatory requirements. Key management approaches should align with organizational policy, regulatory requirements, and operational resilience considerations. For OT workloads, the organization should validate encryption configurations for compatibility with virtualized devices, legacy applications, and performance-sensitive processes.

Where an OT application or legacy component does not support native encryption of stored data, the organization should determine whether encryption can be provided by the underlying storage or platform. Where encryption is not feasible at an appropriate layer, the organization should document the limitation and apply compensating controls, such as strict access controls, network segmentation, and monitoring. While these controls may provide defense in depth, they are not equivalent substitutes for encryption at rest.

Protecting OT data in cloud storage depends on secure configurations and correctly assigned access permissions. A data classification scheme that identifies OT data by its sensitivity and criticality helps the organization apply appropriate access controls and encryption requirements. The organization should manage these controls consistently and validate permissions across object storage, file shares, collaboration platforms, and other cloud storage services. Incorrect settings or excessive permissions may allow unauthorized access, modification, or deletion of sensitive OT data.

Cloud-integrated OT workloads may rely on stored secrets, such as authentication tokens and API keys, to access cloud services and other systems. The organization should store these secrets in approved secrets-management systems, restrict access to them, and securely provide them to workloads when needed. Secrets stored in plaintext configuration files, embedded in code or deployment templates, or exposed through inadequately protected environment variables may enable unauthorized access to cloud resources and connected OT systems.

Development and testing environments may also process OT-related data. Where feasible, the organization should use synthetic, anonymized, or minimized datasets to reduce exposure of OT-related data if these environments are compromised.

Data-at-rest protections should preserve the confidentiality, integrity, and availability of OT data during normal operations, degraded operations, and recovery. The organization should confirm that authorized personnel can access, decrypt, and use protected data within required recovery timelines. Key management, backup, and access control processes should align with recovery objectives.

Example Mitigating Controls

- Technical Controls
  - **Standardize secure storage configurations.**

    Develop and implement configuration templates or policy-as-code (PaC) mechanisms to help define configuration requirements that enforce encryption, least-privilege storage permissions, integrity validation, deletion prevention, and redundancy based on operational data criticality and recovery requirements. Monitor for corruption and unauthorized modification or deletion.
  - **Monitor for storage misconfigurations.**

    Deploy cloud security tools capable of identifying misconfigured storage resources, excessive permissions, or policy drift that affects OT-related data. Integrate findings into remediation workflows.
  - **Apply layered protections where encryption is not supported.**

    Where OT systems or legacy components cannot support encryption of stored data, implement compensating controls such as restricted access controls, network segmentation, or secure gateways to reduce exposure risk.
  - **Protect and manage stored secrets.**

    Use secure secret management mechanisms to store and inject authentication tokens and API keys into workloads. Restrict access to secrets, enable rotation where feasible, and prevent storing secrets in plaintext configuration files or code repositories.
  - **Minimize sensitive data in non-production environments.**

    Use synthetic or anonymized data in development and testing environments where operational data is not required. This practice reduces the exposure of OT data if a compromise occurs.
- Cloud Provider Controls
  - **Provide key management options and disclose key access conditions.**

    Encrypt customer data at rest within the service boundary. Offer documented key management options. For each option, state who holds the key material, who operates the key management service, and who can perform

cryptographic operations. Support controlled access, rotation, and recovery for keys and secrets the service manages. Describe what happens to data access and restoration when a key is revoked, deleted, or unavailable.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 3: Data Protection
- CRI Cloud Profile v2.0 [CRI 2024]
  - PR.DS-01
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Cryptography, Encryption & Key Management (CEK)
  - Data Security and Privacy Lifecycle Management (DSP)
  - Universal Endpoint Management (UEM)
- IEC 62443-3-3:2013 [IEC 2013]
  - Foundational Requirement 3: System integrity
  - Foundational Requirement 4: Data confidentiality
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.12: Classification of information
  - Control 5.15: Access control
  - Control 5.33: Protection of records
  - Control 5.34: Privacy and protection of PII
  - Control 8.24: Use of cryptography
- MITRE ATT&CK for ICS v19.2 [MITRE 2026]
  - M0803: Data Loss Prevention
  - M0922: Restrict File and Directory Permissions
  - M0941: Encrypt Sensitive Information
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - System and Communications Protection (SC)
  - System and Information Integrity (SI)

- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - PR.DS: Data Security
  - PR.PT: Protective Technology

PR.DS-02 *The confidentiality, integrity, and availability of data-in-transit are protected*

Potential Risks and Considerations

Protecting OT data in transit requires appropriate encryption and integrity controls across cloud-integrated communication paths. The organization should identify trust boundaries and protect communications among on-premises OT systems, cloud technologies, third-party providers, and field devices. Hybrid data flows may traverse several network paths, security zones, and service providers. The organization should identify where protections begin and end, where data appears in decrypted form, and how transport security failures could affect OT operations.

Legacy OT protocols and devices may not support modern mechanisms that protect confidentiality, integrity, and message authenticity. Some may also be sensitive to latency, packet inspection, or changes in session handling. When native end-to-end encryption is not feasible, the organization may use secure gateways, encrypted tunnels, network segmentation, and other layered safeguards to reduce exposure. The organization should evaluate the additional trust dependencies and failure points that these measures introduce. It should also confirm that transport protections do not add unacceptable latency, jitter, packet loss, or connection failures. Secure communication should provide redundancy and tested failover when required to meet OT availability needs.

Example Mitigating Controls

- Administrative Controls
  - **Plan secure and resilient transport for OT data.**

    Document OT data flows and trust boundaries across on-premises systems, cloud technologies, third parties, and field devices. For each flow, define confidentiality, integrity, and availability requirements; identify protection termination points, dependencies, and single points of failure; and design appropriate redundancy, failover, and degraded operating modes. Review the architecture when systems or data flows change and validate that it continues to meet OT operational requirements.

- Technical Controls
  - **Define and enforce encryption at network trust boundaries.**

    Configure secure communication mechanisms for data exchanged among cloud technologies, on-premises OT systems, third parties, and field devices. Apply encryption protocols appropriate to the defined trust boundary and ensure the secure configuration of transport mechanisms, including certificate validation, cipher selection, and integrity protection. Clearly document and control the points where encrypted sessions terminate.
  - **Implement secure gateways or tunneling mechanisms between OT and cloud networks.**

    Where OT devices or protocols do not support native encryption, deploy intermediary gateways, secure tunnels, or protocol wrappers to protect communications across untrusted networks.
  - **Manage and monitor the cryptographic material used to protect data-in-transit.**

    Implement processes that manage the certificates and keys used to secure communications. Monitor for expired certificates, weak ciphers, and misconfigured secure channels that could weaken the protection of OT-related data.
- Cloud Provider Controls
  - **Disclose customer-facing encryption termination points.**

    Provide secure transport interfaces for customer connections and protect customer data as it moves between service components. Publish the supported protocols and cipher options and the configuration each one requires. Identify the customer-facing points where an encrypted session terminates, such as load balancers and service endpoints. State the default protection applied to traffic between datacenters and between internal service components.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 3: Data Protection
- CRI Cloud Profile v2.0 [CRI 2024]
  - PR.DS-02
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Cryptography, Encryption & Key Management (CEK)
  - Data Security and Privacy Lifecycle Management (DSP)

- IEC 62443-3-3:2013 [IEC 2013]
  - Foundational Requirement 3: System integrity
  - Foundational Requirement 4: Data confidentiality
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.14: Information transfer
  - Control 8.20: Network security
  - Control 8.21: Security of network services
  - Control 8.24: Use of cryptography
- MITRE ATT&CK for ICS v19.2 [MITRE 2026]
  - M0803: Data Loss Prevention
  - M0808: Encrypt Network Traffic
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - System and Communications Protection (SC)
  - System and Information Integrity (SI)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - PR.DS: Data Security
  - PR.PT: Protective Technology

PR.DS-10 *The confidentiality, integrity, and availability of data-in-use are protected*

Potential Risks and Considerations

Protecting data in use covers OT data while it is being processed by workloads or services. Confidentiality and integrity controls may include workload isolation, memory protection, trusted execution, access control, and integrity validation. Availability of the processing function depends on runtime resilience controls such as capacity planning, redundancy, failover, health monitoring, and locally survivable OT operation.

In IaaS, for example, the cloud provider may manage the hypervisor, while the organization manages guest operating systems and workloads. Cloud provider-managed events, such as host maintenance or hardware retirement, may affect running workloads depending on the service and configuration. Separately, customer-selected interruptible, spot, or preemptible capacity can be stopped, terminated, hibernated, or evicted when the provider reclaims capacity. Do not use interruptible capacity for OT workloads that require continuous availability unless the workload is explicitly designed and tested for interruption.

The sensitivity and operational importance of an OT workload should inform its isolation and tenancy requirements. Greater separation from other tenants or workloads may provide stronger isolation for some use cases. However, it can increase cost or reduce deployment flexibility and scalability. The organization should evaluate these tradeoffs against data sensitivity and OT performance, availability, and resilience requirements.

Confidential computing and Trusted Execution Environments (TEEs) can help protect the confidentiality and integrity of OT data and code within the protected execution environment during processing. They do not, by themselves, protect data before entry or after exit from the TEE, eliminate side-channel risks, or provide availability.

Example Mitigating Controls

- Technical Controls
  - **Configure workload isolation consistent with OT risk requirements.**

    Select and configure isolation options that match the sensitivity and criticality of OT workloads. Some cloud providers offer dedicated or sole-tenant compute options that provide physical separation from other customers at the compute-host level. Storage, networking, control planes, and other service components typically remain shared.
  - **Evaluate hardware-based memory protection features for sensitive OT workloads.**

    Where supported and aligned with operational requirements, consider enabling hardware-based protections, such as confidential computing using TEEs, to protect sensitive OT data while it is being processed.
  - **Configure cloud services to maintain runtime availability.**

    Protect availability through capacity planning, redundancy, failover, and health monitoring. Account for provider quotas when sizing failover capacity. Define how OT processes operate safely when a cloud workload is unavailable.
- Cloud Provider Controls
  - **Describe and assure workload isolation boundaries.**

    Enforce isolation between customer workloads and other tenants in compute environments. Restrict privileged access to customer data during processing and validate the protections built into hypervisors and managed runtimes. Describe the dedicated tenancy and confidential computing options available, the security boundary each one provides, and the compatibility limits that apply. Provide documentation or independent assurance for protections customers cannot inspect.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - PR.DS-10
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Data Security and Privacy Lifecycle Management (DSP)
  - Infrastructure Security (I&S)
- IEC 62443-3-3:2013 [IEC 2013]
  - Foundational Requirement 3: System integrity
  - Foundational Requirement 4: Data confidentiality
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 8.7: Protection against malware
  - Control 8.12: Data leakage prevention
- MITRE ATT&CK for ICS v19.2 [MITRE 2026]
  - M0928: Operating System Configuration
  - M0948: Application Isolation and Sandboxing
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Access Control (AC)
  - System and Communications Protection (SC)
  - System and Information Integrity (SI)

PR.DS-11 *Backups of data are created, protected, maintained, and tested*

Potential Risks and Considerations

Backup strategies for OT data in cloud environments should align with the organization's operational resilience objectives and recovery requirements. Cloud services can automate backups and store or replicate data across regions. Replication can improve availability, but it does not replace separate backups because it may also propagate corruption or deletion. The organization should evaluate cost, restore times, replication lag, and dependencies on network connectivity and cloud provider services. Restoration tests should confirm that personnel can retrieve, validate, decrypt, and use backup data under degraded conditions and within required recovery timelines.

Geographically distributed backups can improve resilience to localized failures and regional disruptions. However, storing backup copies in other regions or jurisdictions may create data residency, regulatory, or contractual considerations. The organization

should identify where backup copies are stored and confirm that those locations meet applicable requirements.

Cloud backup architectures can improve cyber resilience when backup and recovery resources are separated from production systems. Separate administrative domains, restricted connectivity, distinct privileged access controls, and immutable backup controls can reduce the likelihood that an incident affecting production systems also compromises backup data. Isolated recovery environments can provide a controlled location to restore and validate workloads before reconnecting them to OT operations. The organization should regularly test these protections and restoration procedures to confirm that recovery can proceed safely and predictably.

Example Mitigating Controls

- Administrative Controls
  - **Periodically test backup-restoration processes.**

    Conduct periodic restoration tests to validate that personnel can successfully retrieve, decrypt where applicable, and restore backups within defined recovery objectives. Verify data integrity and completeness.
- Technical Controls
  - **Configure and enforce backup policies for OT data and recovery artifacts.**

    Configure backup mechanisms for OT data and the artifacts needed to restore supporting services, such as configurations, identity settings, cryptographic recovery information, software artifacts, logs, and licenses. Align retention, frequency, encryption, geographic location, immutability, and redundancy with OT data criticality and recovery requirements.
  - **Implement logical isolation and immutability for backup resources.**

    Where supported, enable immutability controls, such as write-once, read-many (WORM) storage or retention locks, to reduce the risk of backup compromise during a security incident. Immutability controls vary in strength, and some modes allow privileged identities to shorten retention or remove protection. Select a mode that matches the threat and retention requirement, restrict permissions that can bypass it, and test that protected backups cannot be deleted early. Separate production and recovery environments, including their administrative access. Where appropriate, consider vault-based or logically isolated recovery architectures that limit routine connectivity between the recovery environment and production workloads.
  - **Maintain independent copies of critical OT data where required.**

    For OT data that supports safety, regulatory compliance, or root cause analysis (RCA), maintain independent or offline copies consistent with organizational policy.

- Cloud Provider Controls
  - **Provide immutable retention options and expose backup failures.**

    Provide backup and restoration capabilities for customer data and supported recovery artifacts. Let customers configure schedule, retention, encryption, storage location, and separation from production access. Offer immutable retention for the backup resources the service supports. Document coverage, dependencies, retrieval times, and limitations, and make backup failures visible to customers promptly.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 11: Data Recovery
- CRI Cloud Profile v2.0 [CRI 2024]
  - PR.DS-11
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Business Continuity Management and Operational Resilience (BCR)
- IEC 62443-3-3:2013 [IEC 2013]
  - Foundational Requirement 7: Resource availability
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 8.13: Information backup
- MITRE ATT&CK for ICS v19.2 [MITRE 2026]
  - M0953: Data Backup
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Contingency Planning (CP)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - PR.IP: Information Protection Processes and Procedures

3.3.4 Platform Security (PR.PS)

PR.PS-01 *Configuration management practices are established and applied*

Potential Risks and Considerations

The organization should extend configuration management governance to cloud resources and control planes that support OT environments. On-premises and cloud

technologies may require different procedures and tools, but both should meet consistent approval, documentation, and oversight requirements.

Cloud automation increases the speed and scale of configuration changes affecting resources that support OT processes. Automated provisioning, dynamic scaling, and short-lived resources can improve efficiency, but they can also reproduce configuration errors quickly. Configuration management practices should apply approved security baselines throughout each resource's lifecycle. For example, images or templates that contain default credentials can replicate them across many resources. Baselines should require the organization to remove, disable, or replace these credentials before the resource enters service. Automated checks can verify compliance where feasible. Without consistent enforcement, configuration weaknesses may introduce vulnerabilities or operational instability.

Cloud security tools can help the organization apply and monitor approved configuration baselines at scale. IaC, configuration templates, and policy-based automation can define and deploy configurations at scale. CSPM tools or other related monitoring capabilities can identify deviations in supported cloud resources and services. The organization should integrate these tools with established configuration management processes and account for differences among cloud providers. Effective use also requires personnel who can interpret findings consistently across hybrid and multi-cloud environments.

Example Mitigating Controls

- Technical Controls
  - **Establish hardened configuration baselines for cloud resources that support OT systems.**

    Develop, test, deploy, and maintain hardened baselines that enforce the organization's configuration management policies for cloud resources that support OT systems. Industry-established benchmarks, such as Center for Internet Security (CIS) Benchmarks for cloud technologies, may inform baseline development [CIS 2026]. The organization may implement baselines through configuration templates or IaC mechanisms to deploy secure configurations consistently.
  - **Implement PaC and continuous configuration monitoring.**

    Use PaC frameworks and cloud policy guardrails to validate configuration requirements during deployment and block noncompliant changes. Use CSPM tools or similar mechanisms to continuously assess deployed resources for deviations from approved configuration baselines. These tools identify misconfigurations and configuration drift and produce findings that support timely remediation across cloud environments that support OT workloads. Where the organization enables automated remediation, test it before use so that corrective changes do not disrupt OT operations.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 4: Secure Configuration of Enterprise Assets and Software
- CRI Cloud Profile v2.0 [CRI 2024]
  - PR.PS-01
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Cryptography, Encryption & Key Management (CEK)
  - Change Control and Configuration Management (CCC)
  - Infrastructure Security (I&S)
- IEC 62443-3-3:2013 [IEC 2013]
  - Foundational Requirement 7: Resource availability
- IEC 62443-4-1:2018 [IEC 2018]
  - Practice 4: Secure implementation
  - Practice 7: Security update management
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 8.19: Installation of software on operational systems
  - Control 8.32: Change management
- MITRE ATT&CK for ICS v19.2 [MITRE 2026]
  - M0814: Static Network Configuration
  - M0915: Active Directory Configuration
  - M0924: Restrict Registry Permissions
  - M0928: Operating System Configuration
  - M0947: Audit
  - M0954: Software Configuration
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Configuration Management (CM)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - PR.IP: Information Protection Processes and Procedures

PR.PS-02 *Software is maintained, replaced, and removed commensurate with risk*

Potential Risks and Considerations

Software maintenance processes should cover software that supports OT functions in cloud environments. This includes guest operating systems, applications, container images, and other components deployed on virtual machines or containers. The maintenance method depends on the service model and workload design. The organization may patch systems in place, rebuild and redeploy immutable workloads from updated base images, update application dependencies or runtime versions, or prepare for provider-managed service upgrades. The organization should test customer-controlled updates before deployment. For provider-managed changes, it should review lifecycle notices, assess compatibility, and use testing or scheduling options when available. These activities should follow established OT change management and maintenance practices.

Maintaining software in cloud-supported OT environments may require additional expertise, tooling, and information sources. The organization should monitor advisories and lifecycle notices from cloud providers, operating system vendors, OT equipment manufacturers, and application vendors. It should incorporate relevant information into maintenance and vulnerability management processes so that personnel can prioritize, test, and schedule updates based on operational requirements.

Software maintenance also includes removing software that is no longer needed and replacing unsupported components. Cloud-supported OT environments may retain outdated container images, unused services, or unnecessary software packages. Some OT applications and engineering tools may require unsupported or end-of-life software to maintain compatibility with operational processes. When continued use is necessary, the organization should document the risk, define a replacement or retirement plan, and apply compensating safeguards. These safeguards may include network segmentation, access restrictions, monitoring, and application allowlisting. Unsupported or unnecessary software can increase the attack surface and expose systems supporting OT processes to known vulnerabilities.

Example Mitigating Controls

- Technical Controls
  - **Extend software management processes to cloud environments.**

    Extend existing OT software maintenance processes to include the operating systems, applications, and container images deployed in cloud environments. Establish defined patching cadences, testing procedures, and deployment validation processes so the organization can apply updates without disrupting operational processes. Also establish an expedited, risk-based process to evaluate, test, approve, and deploy urgent patches or other mitigations outside the normal cadence when active exploitation or unacceptable risk requires faster action.

- **Monitor vulnerabilities that affect cloud-hosted OT software components.**

  Use vulnerability management tools and advisory monitoring processes to identify vulnerabilities that affect operating systems, container images, application dependencies, and other software components deployed within cloud-hosted OT workloads. Where available, use container registries with integrated image scanning to detect known vulnerabilities before deployment. Maintaining an SBOM for OT software components can improve visibility into dependencies and support identifying vulnerabilities quickly. Evaluate and remediate vulnerabilities within defined maintenance timeframes.

- **Remove unsupported or unnecessary software from cloud-hosted resources.**

  Identify and remove unauthorized, unused, or unsupported software components deployed within cloud environments that support OT systems. Reducing unnecessary services, outdated images, and unused instances helps minimize the attack surface of the cloud resources that support OT operations.

- **Implement compensating controls for systems that require unsupported software.**

  Where OT systems or engineering tools require unsupported or end-of-life software, implement compensating controls, such as network segmentation, additional access controls, or enhanced monitoring. Implement these controls using cloud networking configurations and security services to reduce exposure while pursuing modernization strategies.

- Cloud Provider Controls
  - **Maintain managed-service software and offer maintenance scheduling options.**

    Maintain the software and runtime components through defined update, testing, and retirement processes. Remediate vulnerabilities according to risk and provide an expedited path for urgent threats. Validate changes before deployment and monitor their effect on service availability. Publish version support and end-of-support timelines. Offer maintenance window and version selection options where the service supports them. State the actions a customer takes before an upgrade.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 2: Inventory and Control of Software Assets
  - 4: Secure Configuration of Enterprise Assets and Software
- CRI Cloud Profile v2.0 [CRI 2024]
  - PR.PS-02

- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Application & Interface Security (AIS)
  - Data Security and Privacy Lifecycle Management (DSP)
  - Threat and Vulnerability Management (TVM)
  - Universal Endpoint Management (UEM)
- IEC 62443-3-3:2013 [IEC 2013]
  - Foundational Requirement 3: System integrity
- IEC 62443-4-1:2018 [IEC 2018]
  - Practice 7: Security update management
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 8.8: Management of technical vulnerabilities
  - Control 8.19: Installation of software on operational systems
  - Control 8.32: Change management
- MITRE ATT&CK for ICS v19.2 [MITRE 2026]
  - M0928: Operating System Configuration
  - M0942: Disable or Remove Feature or Program
  - M0947: Audit
  - M0951: Update Software
  - M0954: Software Configuration
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Configuration Management (CM)
  - Maintenance (MA)
  - System and Information Integrity (SI)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - Flaw Remediation and Patch Management

PR.PS-03 *Hardware is maintained, replaced, and removed commensurate with risk*

Potential Risks and Considerations

Cloud providers manage the lifecycle of physical hardware that supports cloud compute, storage, and networking. For SaaS offerings, the SaaS provider may operate this hardware or depend on an upstream cloud provider. The organization typically cannot

directly inspect or control hardware maintenance, replacement, and disposal. It should evaluate the cloud provider's documentation, contractual commitments, audit reports, and other assurance evidence covering hardware maintenance, vulnerability management, and secure disposal. This evaluation should determine whether cloud provider practices meet the organization's operational resilience and risk management needs.

Cloud provider redundancy does not automatically make cloud-supported OT workloads resilient to underlying hardware events. Hardware failures, vulnerabilities, or maintenance activities could affect service availability. Cloud providers may offer redundant compute, storage, and networking across separate availability zones or regions. The organization should identify relevant areas where a single failure could affect multiple systems and select and configure the redundancy needed to meet OT requirements.

The organization remains responsible for the hardware it owns and operates to connect OT environments to cloud technologies. This includes edge, network, and communications devices. The organization should maintain, replace, and securely dispose of these devices through established lifecycle processes, based on their criticality and operational role. Some hybrid offerings place provider-managed hardware at organization facilities. In these cases, agreements should define responsibility for maintenance, replacement, and disposal. The organization remains responsible for facility security and site conditions.

Example Mitigating Controls

- Technical Controls
  - **Design a resilient architecture for cloud technologies that support OT systems.**

    Deploy cloud workloads that support OT using resilient architecture patterns, such as workload distribution, redundancy across availability zones or regions, or failover capabilities. These practices help reduce the operational impact of hardware failures or infrastructure lifecycle events that affect the underlying cloud platform.
- Cloud Provider Controls
  - **Sanitize or destroy storage media before disposal or reuse.**

    Sanitize or destroy storage media before disposal or before reuse that could expose customer data. Remove retired hardware from service through controlled processes and record its disposition. Apply the same practices to hardware located at customer sites, consistent with the responsibilities the agreement assigns. Provide documentation or independent assurance of these practices.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - PR.PS-03
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.9: Inventory of information and other associated assets
  - Control 5.11: Return of assets
  - Control 7.13: Equipment maintenance
  - Control 7.14: Secure disposal or re-use of equipment
- MITRE ATT&CK for ICS v19.2 [MITRE 2026]
  - M0947: Audit
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Maintenance (MA)
  - System and Services Acquisition (SA)

PR.PS-04 *Log records are generated and made available for continuous monitoring*

Potential Risks and Considerations

Logging visibility in cloud-supported OT environments depends on the service model and the division of responsibilities. Cloud platforms may provide the organization with logs for control plane, network, identity, and application activity within its tenant. Logs for cloud provider infrastructure, physical datacenters, and the internal operation of managed services generally remain under cloud provider control. The cloud provider may share selected logs, service health information, incident notifications, or investigation support.

The organization is generally responsible for configuring the logging available within its cloud tenant. Relevant sources depend on the service model and may include control plane activity, identity events, network flow records, operating system and application events, and service-specific logs. The organization should collect the records needed to monitor and investigate activities affecting cloud-supported OT workloads. Logs, together with service metrics, can also help operations personnel assess availability, performance, and deviations from defined operating thresholds.

Cloud technologies can generate large volumes of logs from APIs, automated operations, and numerous service components. The organization may need centralized aggregation and analytic tools to collect, normalize, and correlate events across cloud and on-premises OT environments. It should define log retention periods based on regulatory, operational, and forensic needs. Native cloud logging services often provide

configurable retention, but the organization may need to export logs to archival storage to meet longer retention or immutability requirements. Without effective aggregation and analysis, important indicators of malicious or abnormal activity may remain undetected.

Example Mitigating Controls

- Administrative Controls
  - **Define logging requirements for cloud environments that support OT systems.**

    Document the logging requirements necessary to support monitoring, incident response, and forensic investigations for cloud technologies that support OT systems. Prioritize the events that matter most to OT operations, because log volume and cost limit what the organization can collect and retain.
- Technical Controls
  - **Extend log collection to cloud technologies that support OT systems.**

    Configure operating systems, applications, and cloud technologies that support OT systems to generate log records and securely transmit them to a centralized logging infrastructure. Include the tenant control plane, the identity provider, and administrative APIs. Capture security-relevant administrative actions, such as identity and access changes, policy changes, network security changes, logging changes, and changes to cloud resources that support OT functions. Consider logging sources that the organization may not currently log, such as API calls that affect OT data, configurations, or commands.
  - **Protect the integrity and availability of log records.**

    Send security-relevant logs to an organization-controlled destination that is administered separately from the source environment. Design this destination to remain available to authorized responders if a source environment is compromised. Store retained log records with immutable storage, such as WORM storage. Set retention periods that meet regulatory requirements and support incident response before locking them. Where supported, use a locked retention mode that tenant administrators cannot shorten or bypass during the retention period. If only a bypass-able mode is available, strictly limit bypass permissions, require independent approval, and alert on any change to retention settings. Use cryptographic digests stored in a separate trusted location to detect modification. When records must also prove their source, use digital signatures or another mechanism that supports verifiable origin attribution.
  - **Restrict and monitor changes to logs.**

    Use preventive policies to restrict actions that disable log collection or export, change log destinations, delete retained records, or shorten required retention. Confirm which principals and resource types these policies reach, because coverage varies by cloud provider. Require independent approval for high-

impact logging changes. Alert on attempted or completed changes. Monitor ingestion, storage, and retention health to detect missing, delayed, or prematurely deleted records.

- **Aggregate OT and cloud telemetry for analysis.**

  Design logging infrastructure to aggregate OT and cloud telemetry so that analysts can monitor and investigate across environments.

- Cloud Provider Controls
  - **Generate customer security audit records and report logging failures.**

    Generate audit records for the identity, administrative, configuration, and data access events that occur in provider-managed services on a customer's behalf. Include the event time, initiating identity, affected resource, action, and outcome. Provide configurable collection and secure export, and make delivery failures and delays visible to customers. Protect these records within provider-managed logging systems and document the events and services that logging does not cover.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 3: Data Protection
  - 8: Audit Log Management
- CRI Cloud Profile v2.0 [CRI 2024]
  - PR.PS-04
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Logging and Monitoring (LOG)
- IEC 62443-3-3:2013 [IEC 2013]
  - Foundational Requirement 2: Use control
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 8.15: Logging
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Audit and Accountability (AU)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - PR.PT: Protective Technology

PR.PS-05 *Installation and execution of unauthorized software are prevented*

Potential Risks and Considerations

Controls that prevent unauthorized software from running should cover cloud-supported OT workloads and their deployment paths. This includes virtual machines, containers, and deployment pipelines. Automated deployment and rapid scaling can reproduce unauthorized software or malicious code across many resources if controls are weak or inconsistent. The organization should adapt its existing configuration management and application control practices to ensure that only approved software and binaries can reach or execute on systems that support OT operations.

Immutable deployment approaches can reduce opportunities to install unauthorized software on running cloud workloads. Under this model, the organization replaces workloads instead of modifying them after deployment. When updates are needed, the organization replaces the running instance with a newly built and validated image rather than patching it in place. These measures can reduce persistence that depends on modifying an individual workload.

Immutable deployment shifts software authorization to the build and deployment process. Build systems, artifact repositories, images, deployment templates, and deployment identities therefore become high-value targets. An attacker who compromises these components can insert malicious code that persists across workload replacements. Immutability also does not stop unauthorized code from executing in memory or from permitted writable storage. The organization should combine immutable deployment with runtime monitoring, artifact integrity protections, tightly controlled deployment privileges, and logging of build, deployment, and control activity.

Example Mitigating Controls

- Technical Controls
  - **Control the execution and deployment of authorized software.**

    For virtual machines and other host-based environments, use application allowlisting where operationally appropriate to restrict execution to approved software, scripts, and binaries. For containerized workloads, restrict deployment to approved images and registries, verify image integrity and provenance, enforce deployment or admission policies, and use appropriate runtime controls to restrict unauthorized execution.
  - **Monitor cloud-hosted OT workloads for unauthorized software execution.**

    Deploy monitoring solutions that can identify when unapproved software executes or when abnormal behavior occurs within cloud-hosted OT systems. Monitoring tools should provide visibility into runtime activity and generate alerts when deviations from approved software baselines occur.

- **Use immutable deployment for cloud-hosted OT workloads.**

  Where operationally feasible, update cloud-hosted OT workloads by deploying new instances from approved images rather than changing running instances in place. Apply this approach to virtual machines, containers, and other compute resources that host OT-related applications. Validate replacement images against approved baselines before deployment. This approach does not by itself prevent changes to a running instance. Monitor running instances for drift from their source images and restrict direct administrative changes.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 2: Inventory and Control of Software Assets
- CRI Cloud Profile v2.0 [CRI 2024]
  - PR.PS-05
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Universal Endpoint Management (UEM)
- IEC 62443-3-3:2013 [IEC 2013]
  - Foundational Requirement 3: System integrity
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 8.19: Installation of software on operational systems
- MITRE ATT&CK for ICS v19.2 [MITRE 2026]
  - M0938: Execution Prevention
  - M0944: Restrict Library Loading
  - M0945: Code Signing
  - M0949: Antivirus/Antimalware
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Configuration Management (CM)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - PR.IP: Information Protection Processes and Procedures
  - PR.MA: Maintenance
  - DE.CM: Security Continuous Monitoring

PR.PS-06 *Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle*

Potential Risks and Considerations

Secure software development practices should cover cloud-hosted development and deployment services used for software that supports OT functions. Code repositories, build services, artifact stores, and deployment platforms may change relevant trust boundaries and access paths. Although the tools and procedures may differ, the organization should continue to protect source code, build artifacts, testing and release processes, and deployment approvals throughout the software development lifecycle. Unauthorized or insufficiently governed changes may affect OT performance, availability, or safety.

Secure development practices should treat IaC templates, provisioning scripts, and pipeline definitions as software. Development, security, and operations (DevSecOps) practices and continuous integration and continuous delivery (CI/CD) pipelines can help automate the building, testing, and delivery of applications and infrastructure. The organization should integrate security testing, configuration validation, and operational readiness checks into CI/CD pipelines. These controls help prevent rapid delivery from bypassing the change management and operational requirements that apply to OT systems.

Software and workload artifacts used to support OT operations may originate from internal development teams, vendors, or third-party repositories. These artifacts may include VM templates, container images, software packages, and libraries. Before use, the organization should verify each artifact's source, integrity, and provenance and assess it for known vulnerabilities or unapproved components. Without appropriate validation and governance, vulnerable or malicious software components may be introduced into systems that support OT processes.

Example Mitigating Controls

- Administrative Controls
  - **Adapt software development lifecycle (SDLC) practices for cloud-supported OT environments.**

    Update existing SDLC practices to address development and deployment of applications and infrastructure that support OT workloads in cloud environments. Development processes should incorporate security testing, artifact validation, and operational readiness checks consistent with OT safety and reliability requirements. Governance processes should also ensure appropriate separation of duties among development, testing, and deployment functions.

- **Measure the performance of secure development practices for cloud-supported OT workloads.**

  Define measures that show whether these practices work as intended. Useful measures include the share of deployments that pass required pipeline gates, the number of gate overrides and the reasons for them, the time to remediate vulnerabilities found in artifacts, and the share of OT-supporting workloads that deploy through the governed pipeline. Review results on a defined schedule, compare them over time, and use the trends to target improvements.

- Technical Controls
  - **Secure the CI/CD pipelines used to deploy OT workloads.**

    Configure CI/CD pipelines that support OT workloads to enforce security controls, such as access restrictions, integrity protection of build artifacts, or validation steps before deployment. Pipeline configurations should support operational approval gates and automated checks to reduce the likelihood of deploying untested or unsafe changes to environments that support OT processes.

  - **Verify the integrity and provenance of software artifacts.**

    Obtain artifacts from approved repositories and verify their integrity and provenance using authenticated release or build information. Where supported, validate signatures or attestations against trusted publisher or builder identities and confirm that they apply to the artifacts being deployed.

  - **Scan software artifacts and infrastructure configurations for vulnerabilities.**

    Implement automated scanning capabilities within development or deployment pipelines to identify known vulnerabilities, insecure configurations, or policy violations in software artifacts and IaC templates before deployment to cloud environments that support OT systems. Use software composition analysis (SCA) tools to identify vulnerable open-source or third-party dependencies in OT software components. Integrate secrets scanning into pipelines to detect hardcoded credentials, API keys, or certificates in source code and configuration files before release.

- Cloud Provider Controls
  - **Protect hosted development and deployment services.**

    For hosted source repositories, build systems, artifact stores, and deployment services, protect customer code, artifacts, credentials, and pipeline configurations from unauthorized access and modification. Provide controls for approval gates, separation of duties, artifact integrity verification, and audit records. Isolate build execution between customers and restrict privileged access to the supporting platform.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 16: Application Software Security
- CRI Cloud Profile v2.0 [CRI 2024]
  - PR.PS-06
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Application & Interface Security (AIS)
  - Data Security and Privacy Lifecycle Management (DSP)
- IEC 62443-4-1:2018 [IEC 2018]
  - Practice 1: Security management
  - Practice 2: Specification of security requirements
  - Practice 3: Secure by design
  - Practice 4: Secure implementation
  - Practice 5: Security verification and validation testing
  - Practice 6: Management of security-related issues
  - Practice 7: Security update management
  - Practice 8: Security guidelines
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 8.25: Secure development life cycle
  - Control 8.26: Application security requirements
  - Control 8.27: Secure system architecture and engineering principles
  - Control 8.28: Secure coding
  - Control 8.29: Security testing in development and acceptance
  - Control 8.30: Outsourced development
  - Control 8.31: Separation of development, test and production environments
- MITRE ATT&CK for ICS v19.2 [MITRE 2026]
  - M0913: Application Developer Guidance
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - System and Services Acquisition (SA)

- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - PR.IP: Information Protection Processes and Procedures
- NIST SP 800-218 [NIST 2022]

3.3.5 Technology Infrastructure Resilience (PR.IR)

PR.IR-01 *Networks and environments are protected from unauthorized logical access and usage*

Potential Risks and Considerations

Where the cloud service exposes customer-managed networking, the organization should extend appropriate network segmentation and trust boundaries into the cloud environment. Virtual private clouds (VPCs), subnets, security groups, routing policies, and cloud firewalls can establish trust boundaries between OT systems, enterprise IT environments, and externally accessible services. Segmentation policies should permit only the communications required for operational processes. Communications between cloud technologies and on-premises OT control networks should be mediated in an industrial demilitarized zone (DMZ). Place gateways, proxies, brokers, and inspection controls within or at the boundaries of that DMZ, and prohibit direct routing between cloud networks and lower-level OT control zones.

Cloud networking can maintain fine-grained segmentation as workloads are created, moved, or scaled. Policies based on workload identities or governed attributes, such as tags and labels, can remain effective when IP addresses change. However, API-driven network changes, incorrect routing rules, and improperly assigned attributes can quickly alter authorized communication paths. The organization should control changes to network policies and attributes and validate policy outcomes after automated changes.

Monitoring should provide visibility into traffic crossing cloud and OT segmentation boundaries. Provider-offered flow logs typically record connection metadata rather than packet contents. Coverage, aggregation intervals, and excluded traffic vary by cloud provider and service. The organization should understand these limitations and combine flow records with firewall, DNS, identity, application, and endpoint logs. Correlating these sources can help the organization identify unauthorized access attempts, policy violations, and abnormal activity affecting OT workloads.

Example Mitigating Controls

- Administrative Controls
  - **Update segmentation and network architecture strategies for cloud-supported OT environments.**

    Revise network segmentation and cybersecurity architecture strategies to address cloud networking constructs and OT operational requirements. Strategies should define trust boundaries between OT systems, IT environments, and externally accessible services. The organization may use multi-account architectures, VPCs, or clearly defined network zones to strengthen logical isolation of OT workloads. Terminate cloud connectivity in a DMZ or intermediary zone.
- Technical Controls
  - **Architect cloud networks to isolate OT workloads.**

    Design cloud networking architecture to isolate OT resources using segmentation mechanisms, such as VPCs, subnets, routing policies, network access control lists (NACLs), or virtual firewall controls. Use these mechanisms to enforce defined trust boundaries and restrict communications to only those required for operational processes. Where feasible, use dedicated network interconnects combined with private endpoints to route communications between OT and cloud environments without traversing the public internet. Private routing reduces exposure but does not by itself provide confidentiality or integrity. Authenticate and encrypt communications between OT and cloud environments on every path, including private ones.
  - **Implement micro-segmentation to limit lateral movement.**

    Apply micro-segmentation controls, such as security groups or equivalent workload-level policies, to restrict communications between systems supporting OT workloads. Segmentation policies should minimize unnecessary east-west traffic and reduce lateral movement within cloud environments.
- Cloud Provider Controls
  - **Enforce network policy as resources change and disclose uncovered paths.**

    Provide network and service access controls that let customers set isolation boundaries and restrict ingress, egress, and communication between workloads. Support private connectivity for the services that offer it. Enforce configured policies as resources are created, moved, or scaled. Document the endpoints, service traffic, and management paths those policies do not cover.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 3: Data Protection
  - 12: Network Infrastructure Management
  - 13: Network Monitoring and Defense
- CRI Cloud Profile v2.0 [CRI 2024]
  - PR.IR-01
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Infrastructure Security (I&S)
- IEC 62443-3-3:2013 [IEC 2013]
  - Foundational Requirement 2: Use control
  - Foundational Requirement 5: Restricted data flow
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 8.7: Protection against malware
  - Control 8.20: Network security
  - Control 8.21: Security of network services
  - Control 8.22: Segregation of networks
  - Control 8.35: CLD - Segregation in virtual computing environments
- MITRE ATT&CK for ICS v19.2 [MITRE 2026]
  - M0802: Communication Authenticity
  - M0807: Network Allowlists
  - M0814: Static Network Configuration
  - M0930: Network Segmentation
  - M0931: Network Intrusion Prevention
  - M0935: Limit Access to Resource Over Network
  - M0937: Filter Network Traffic
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Access Control (AC)
  - System and Communications Protection (SC)

- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - PR.AC: Identity Management and Access Control

PR.IR-02 *The organization's technology assets are protected from environmental threats*

Potential Risks and Considerations

Physical protection of cloud provider-operated infrastructure from environmental hazards is primarily the cloud provider's responsibility. These hazards may include flooding, fire, wind, severe weather, or extreme temperatures. The organization typically cannot inspect the cloud provider's facilities and environmental controls directly. It should evaluate service documentation, independent audits, compliance attestations, and other assurance evidence that addresses datacenter resilience and environmental protections.

Region and availability zone selection should account for the environmental hazards that could affect cloud-supported OT systems. Redundant resources within one availability zone may share exposure to a localized environmental event. Resources distributed across availability zones within one region may still share exposure to regional events or dependencies. The organization should determine whether critical workloads require redundancy across zones or regions based on operational impact, latency, data consistency, recovery, and data residency requirements.

Example Mitigating Controls

- Administrative Controls
  - **Verify the cloud provider's environmental protections.**

    During procurement and contracting, review cloud provider documentation and independent assurance artifacts to confirm that environmental protections support the availability and resilience of cloud technologies used in OT environments. For example, consider SOC 2® Type II reports [AICPA & CIMA 2026]. Repeat this review at defined intervals to confirm the controls remain effective as services and requirements change. Provider-offered service health dashboards and status notifications can help provide timely information about environmental events or infrastructure disruptions.
- Cloud Provider Controls
  - **Implement environmental protection controls for datacenters.**

    Implement controls at datacenters to protect facilities from environmental threats and maintain operational resilience. Examples include fire detection and suppression systems, redundant power and cooling infrastructure, environmental monitoring, flood protection or drainage controls, and other facility safeguards designed to maintain stable operating conditions.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - PR.IR-02
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Datacenter Security (DCS)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 7.5: Protecting against physical and environmental threats
  - Control 7.8: Equipment siting and protection
  - Control 7.12: Cabling security
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Physical and Environmental Protection (PE)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - PR.IP: Information Protection Processes and Procedures

PR.IR-03 *Mechanisms are implemented to achieve resilience requirements in normal and adverse situations*

Potential Risks and Considerations

Resilience requirements for OT systems should drive architecture decisions. The organization should balance latency, redundancy, cost, and complexity while maintaining the continuity of critical processes. Consider what changes to processes and tools will be needed to achieve important objectives such as recovery time objectives (RTOs) and recovery point objectives (RPOs). Load balancing, distribution across multiple regions, and automated failover can reduce the effect of a single failure when properly designed and tested. However, these mechanisms do not replace local, deterministic execution for protection and safety functions that cannot tolerate cloud service delays or disruptions.

Resilience in cloud-supported OT systems depends on both cloud provider capabilities and the organization’s architecture. Cloud providers implement infrastructure and platform availability controls, but the organization has limited visibility into their design and operation. The organization should use SLAs, cloud provider documentation, assurance evidence, and test results to evaluate whether a service can meet OT resilience requirements. It should consider the scope, exclusions, and dependencies of cloud provider commitments rather than treat them as guarantees. Because cloud service and connectivity disruptions remain possible, OT systems should be able to enter degraded operating modes and maintain minimum required functions when those dependencies fail, until they are restored. Without these measures, cloud provider or

connectivity failures may cause service degradation, operational disruption, or reduced performance.

Example Mitigating Controls

- Administrative Controls
  - **Use cloud provider service commitments as inputs to resilience planning.**

    Many generally available cloud services have published SLAs, but coverage and terms vary by provider and service. SLAs may define service performance with metrics such as uptime percentage or error rates. Cloud providers may measure these metrics across a monthly or other service period, so an SLA percentage does not necessarily indicate how long a single outage may last. Service credits are typically the only remedy when a service falls short, and they do not restore an interrupted operational process. Establish RTOs based on operational requirements. Unless the cloud provider explicitly commits to a restoration time, do not rely on provider restoration within the RTO. Evaluate backup and replication characteristics separately against RPO requirements.
- Technical Controls
  - **Design cloud architectures that meet OT resilience requirements.**

    Design cloud architectures that avoid single points of failure and support continuity of operational processes across both cloud and on-premises environments. Examples include deploying workloads across multiple availability zones or regions and implementing redundant compute and storage resources. Where the organization uses automated failover, it should confirm that the failover behavior, including timing and state changes, is acceptable to the supported process. Safety-critical and latency-sensitive functions should retain local execution and defined degraded modes.
  - **Conduct resilience testing.**

    Periodically conduct resilience testing, such as simulated failover exercises or fault injection in non-production environments, to validate that resilience mechanisms perform as designed under realistic failure conditions.
- Cloud Provider Controls
  - **Publish failure boundaries and the configuration each resilience capability needs.**

    Implement redundancy and failure containment within infrastructure and services. Publish the scope within which a failure of each service is contained, and the dependencies that availability zones or regions share. This lets customers tell an independent failure from one that affects several locations at once. Describe how services behave during a failure and during restoration. State the configuration a customer applies to obtain each documented resilience capability. Provide a supported way for customers to test failure behavior in their own environments.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - PR.IR-03
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Business Continuity Management and Operational Resilience (BCR)
  - Datacenter Security (DCS)
- IEC 62443-3-3:2013 [IEC 2013]
  - Foundational Requirement 7: Resource availability
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.29: Information security during disruption
  - Control 5.30: ICT readiness for business continuity
  - Control 7.11: Supporting utilities
  - Control 8.14: Redundancy of information processing facilities
- MITRE ATT&CK for ICS v19.2 [MITRE 2026]
  - M0811: Redundancy of Service
  - M0815: Watchdog Timers
  - M0953: Data Backup
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Contingency Planning (CP)
  - System and Communications Protection (SC)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - PR.PT: Protective Technology

PR.IR-04 *Adequate resource capacity to ensure availability is maintained*

Potential Risks and Considerations

Configure scaling policies and maintain sufficient baseline resources to meet safety, availability, and performance requirements during both normal and adverse operating conditions. Some resources may take time to scale or may not support automatic scaling. Latency-sensitive workloads may therefore require reserved or pre-provisioned capacity. Misconfigured scaling policies or insufficient resource reservations may degrade system performance and disrupt OT processes that depend on timely data processing.

Cloud service quotas and cloud provider capacity constraints can limit the resources available to OT workloads. Limits may apply by service, account, subscription, availability zone, or region. The organization should identify applicable limits and request increases before expected demand. However, a quota increase does not reserve underlying cloud provider capacity. Where supported and appropriate, the organization may use capacity reservations, pre-provisioning, or alternate deployment locations. Continuity and incident response plans should address regional resource shortages and localized infrastructure disruptions.

Capacity monitoring should track resource use and remaining headroom against operational demand and cloud provider limits. Relevant measures may include compute use, storage consumption, network throughput, connection counts, API limits, scaling events, and reservation use. Cloud provider dashboards and alerts can support monitoring, but the organization may need a consolidated view across accounts, regions, or cloud providers. Alert thresholds and regular reviews of resource utilization should provide enough time to add or reserve capacity before shortages affect OT systems.

Example Mitigating Controls

- Administrative Controls
  - **Perform capacity planning for OT workloads.**

    Establish processes to monitor resource utilization and forecast future capacity requirements for OT assets, devices, and workloads hosted in the cloud. Capacity planning should consider expected operational demand, peak usage scenarios, and resilience requirements so the organization maintains sufficient compute, storage, and network resources to support operational continuity.
  - **Plan for unintended demand on cloud capacity.**

    Extend capacity planning to demand the organization does not intend, such as distributed denial of service (DDoS) attacks, resources an attacker creates, and surges in alert and log volume. Account for failover, which concentrates demand into fewer regions. Confirm that spending limits and budget controls cannot stop a workload that supports an operational process.
- Technical Controls
  - **Monitor resource utilization and capacity thresholds.**

    Use cloud provider monitoring tools or integrated observability platforms to track consumption of compute, storage, and network resources that support OT workloads. Configure alerts or automated notifications when resource utilization approaches defined thresholds that could affect system availability or performance.
  - **Configure scalable cloud architectures for OT workloads.**

    Configure dynamic scaling and redundancy mechanisms to support OT system operational requirements. Examples include implementing auto-scaling

policies, reserving capacity where required, and deploying workloads across multiple availability zones or regions to maintain availability during periods of increased demand or localized infrastructure disruption.

- **Identify and manage cloud provider resource limits.**

  Identify the default account or subscription limits that apply to cloud technologies supporting OT workloads. Request limit increases in advance of anticipated need, and review limits periodically as workloads change, so capacity constraints do not delay recovery or degrade performance during peak demand.

- Cloud Provider Controls
  - **Expose service limits and distinguish quota from available capacity.**

    Provide usage metrics, quota information, threshold alerts, and a documented process for requesting limit increases. Describe the scaling and capacity reservation options available, including regional constraints and activation requirements. State clearly that approving a quota increase does not reserve capacity and does not guarantee it. Make request status and allocation failures visible to customers.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - PR.IR-04
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Datacenter Security (DCS)
  - Infrastructure Security (I&S)
- IEC 62443-3-3:2013 [IEC 2013]
  - Foundational Requirement 7: Resource availability
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 7.11: Supporting utilities
  - Control 8.6: Capacity management
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Contingency Planning (CP)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - PR.DS: Data Security

3.4 Detect (DE)

The Detect Function comprises two Categories:

- Continuous Monitoring (DE.CM)
- Adverse Event Analysis (DE.AE)

3.4.1 Continuous Monitoring (DE.CM)

DE.CM-01 *Networks and network services are monitored to find potentially adverse events*

Potential Risks and Considerations

Consider what information and processes will be necessary to achieve adequate visibility into network activity. Types of logs to consider include cloud network flow logs, firewall and network policy enforcement logs, DNS logs, and load-balancer or proxy access logs where available. Additionally, consider correlation with cloud-service and identity audit logs.

Determine the level of detail needed. Provider-offered flow logs generally provide flow- or connection-level metadata rather than packet payloads. Depending on the provider, service, and configuration, flow-log data may be aggregated or sampled, records may be omitted or skipped, delivery or downstream processing may be delayed, and coverage may vary by resource or network path. Where packet inspection is needed but not feasible, consider whether supplementary information may be useful. Examples include firewall and DNS telemetry, proxy and application-access logs, flow-based behavioral analytics, and endpoint or workload network telemetry. Where traffic mirroring or another packet-copy mechanism is feasible and operationally acceptable, packet-capable Intrusion Detection System (IDS) or Network Detection and Response (NDR) capabilities can provide deeper packet-level analysis.

Consider how these sources may be integrated with existing monitoring and detection processes. Cloud telemetry may differ from traditional OT telemetry in format, granularity, aggregation or delivery timing, and volume. Network telemetry may contain ephemeral or dynamically assigned Internet Protocol (IP) addresses and cloud-specific resource or network-interface identifiers, while audit and control-plane logs may provide information about associated workload, service, or user identities. Consider normalizing these records and using timestamps and available cloud metadata to correlate network observations with resource identifiers, workload or service identities, and relevant audit events rather than relying on IP addresses alone. Centralized monitoring and analytics can correlate activity across cloud and on-premises environments. Cloud-provider-generated security findings, alerts, and threat context may help supplement this analysis..

Example Mitigating Controls

- Administrative Controls
  - **Define network telemetry collection requirements for cloud environments.**

    Establish requirements for collecting and retaining network telemetry that supports monitoring OT workloads deployed in cloud environments. These requirements should identify relevant data sources, such as network flow logs, DNS logs, or logs from managed network or security services, and specify retention periods so telemetry supporting OT processes remains available for analysis. Requirements should also cover each significant communication path between cloud technologies and OT processes, including paths carried by managed services.
- Technical Controls
  - **Integrate cloud network telemetry with centralized monitoring platforms.**

    Forward cloud network telemetry, including network flow logs, DNS logs, and other relevant service logs, to centralized monitoring or analytics platforms that support detection and investigation of adverse events across hybrid environments.
  - **Monitor boundaries of networks that support OT workloads.**

    Implement monitoring capabilities for customer-controlled ingress and egress points, connectivity between cloud and on-premises environments, and other network boundaries that support OT operational processes. Monitoring should capture network flows and other telemetry needed to identify unauthorized connections, abnormal traffic patterns, or deviations from expected network behavior. Where feasible, extend monitoring to east-west traffic within the cloud environment to detect lateral movement between the workloads that support OT systems.
- Cloud Provider Controls
  - **Provide network telemetry for customer-controlled network boundaries.**

    Provide flow records for the virtual networks, ingress and egress points, and interconnections the customer controls. Support export of this telemetry to destinations the customer controls.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 13: Network Monitoring and Defense
- CRI Cloud Profile v2.0 [CRI 2024]
  - DE.CM-01

- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Infrastructure Security (I&S)
  - Logging and Monitoring (LOG)
- IEC 62443-3-3:2013 [IEC 2013]
  - Foundational Requirement 6: Timely response to events
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 8.15: Logging
  - Control 8.20: Network security
  - Control 8.21: Security of network services
  - Control 8.35: CLD - Segregation in virtual computing environments
  - Control 8.36: CLD - Detection and prevention of unauthorized use of cloud services
- MITRE ATT&CK for ICS v19.2 [MITRE 2026]
  - M0920: SSL/TLS Inspection
  - M0931: Network Intrusion Prevention
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Assessment, Authorization, and Monitoring (CA)
  - System and Communications Protection (SC)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - DE.CM: Security Continuous Monitoring
  - DE.AE: Anomalies and Events

DE.CM-02 *The physical environment is monitored to find potentially adverse events*

Potential Risks and Considerations

For cloud provider-operated facilities, the organization should determine how it will receive timely information about physical and environmental events that may affect cloud-supported OT functions. Cloud providers generally monitor physical access activity, power, cooling, fire protection, and other facility conditions. The organization typically has limited visibility into the physical and environmental monitoring systems deployed within cloud provider facilities. The organization should use contractual commitments, service documentation, and independent attestations to evaluate the cloud provider's monitoring and reporting practices. It should determine whether the

timing and detail of cloud provider notifications support its incident response and continuity needs.

The organization remains responsible for monitoring the physical environments it controls. These environments may contain edge devices, network equipment, communication infrastructure, and other hardware that connects OT systems to cloud technologies. Monitoring should detect unauthorized access, tampering, power loss, fire, water intrusion, temperature changes, and other conditions that could disrupt connectivity or OT operations. The organization should define how personnel receive and escalate these alerts during normal and degraded operations.

Example Mitigating Controls

- Administrative Controls
  - **Validate the cloud provider's practices for monitoring the physical environment.**

    During procurement and contracting, review cloud provider documentation and independent assurance artifacts that describe the cloud provider's physical access monitoring and environmental monitoring controls. For example, consider SOC 2® Type II reports or ISO/IEC 27001 certifications [AICPA & CIMA 2026, ISO/IEC 2022]. Repeat this review at defined intervals to obtain assurance the controls remain effective as services and requirements change. Evaluate whether these monitoring controls align with organizational risk management expectations for systems that support OT operations. Address gaps through contractual mechanisms or formal risk management processes.
- Physical Controls
  - **Monitor facilities that contain cloud-connected OT assets.**

    Identify where the edge devices, network equipment, and communication paths that connect OT systems to cloud technologies physically reside. Existing physical environment monitoring may cover these assets already when they sit in facilities the organization monitors. Confirm current coverage and extend monitoring where necessary.
- Cloud Provider Controls
  - **Describe physical and environmental monitoring in documentation.**

    Describe how physical access, facility conditions, and environmental events are monitored in service documentation. Make documentation available to customers on a defined refresh cycle so customers can confirm the controls remain effective as services change.
  - **Report facility conditions that affect customer services.**

    Report infrastructure status, environmental events, and facility conditions that affect the availability or performance of customer workloads through service health channels. Identify the affected services, regions, and time window.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - DE.CM-02
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Datacenter Security (DCS)
- IEC 62443-3-3:2013 [IEC 2013]
  - Foundational Requirement 6: Timely response to events
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 7.1: Physical security perimeters
  - Control 7.2: Physical entry
  - Control 7.3: Securing offices, rooms and facilities
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Physical and Environmental Protection (PE)

DE.CM-03 *Personnel activity and technology usage are monitored to find potentially adverse events*

Potential Risks and Considerations

Activity in cloud environments occurs across multiple operational layers: the organization and identity governance layer, the control plane layer, and the workload and application layer. Activities may be generated by human users, non-human principals, and provider-managed platform services or automated system processes.

At the organization and identity governance layer, activity includes identity lifecycle actions, authentication events, privilege changes, organization-level policy changes, and logging and security configuration changes. These actions may not immediately change a specific workload, but they can change who can access environments, what actions are allowed, and which logs are retained. Automated activity can be repetitive and high in volume. The organization should establish expected patterns for automated behavior, including its permitted actions, resources, and operating times, so analysts can identify deviations.

Control plane monitoring should detect changes to the resources and configurations that define cloud-supported OT environments. Relevant activity includes creating or deleting resources, changing network routes or firewall rules, modifying storage, updating access policies, and changing infrastructure automation. Administrative audit logs generally identify the initiating identity, action, time, and affected resource. However, default collection, coverage, and retention vary by cloud provider and service.

Some related data, network, or service events require explicit configuration and may incur additional costs. Before relying on a log source, the organization should generate representative activity and confirm that the expected records are collected, protected, retained, and available for analysis.

At the workload and application layer, monitoring more closely resembles traditional on-premises user activity monitoring. Workload and application monitoring should cover activity within virtual machines, containers, applications, and managed services that support OT functions. Relevant activity may include operating system logons, privileged command execution, configuration changes, application activity, and administrative sessions within hosted systems. Managed services may provide service-specific access and audit logs instead of host-level logs. Because cloud workloads may be short-lived, the organization should export needed logs to centralized monitoring systems before workloads terminate. Logging priorities should reflect mission, safety, and reliability importance; data sensitivity; how much privilege the system holds; internet exposure; the number of dependent systems; and how far a compromise could spread.

Example Mitigating Controls

- Administrative Controls
  - **Define monitoring requirements for activity in cloud environments.**

    Establish organizational requirements for monitoring human and non-human activity across identity services, cloud management interfaces, and workloads that support OT operations. Monitoring requirements should define relevant telemetry sources, logging configurations, and alerting criteria needed to detect anomalous or unauthorized actions that affect cloud resources.
- Technical Controls
  - **Collect and analyze identity and authentication activity.**

    Enable and monitor identity service logs that record authentication events, privileged role use, and identity lifecycle actions associated with cloud environments. Integrate these logs with centralized monitoring platforms to detect unusual access patterns, failed authentication attempts, or unauthorized privilege use. Give particular attention to changes that alter who can reach the environment and how, such as changes to federation and trust configurations, changes to MFA settings, grants of application roles and consent, the issuance of tokens, and creation of keys and secrets. Monitor use of the most privileged accounts, including emergency access accounts, where activity should be rare and expected. Where supported, user and entity behavior analytics (UEBA) capabilities can supplement rule-based alerting by identifying anomalous patterns in identity and activity data that may indicate compromised credentials or insider activity affecting cloud resources that support OT systems.

- **Monitor control plane activity that affects cloud resources.**

  Collect and analyze logs that record the management operations performed against cloud resources, such as creating or modifying compute instances, network configurations, storage resources, or security policies. Also monitor changes to logging configurations and to cross-account access, because both can conceal later activity. Monitoring these events helps identify unauthorized or unexpected architectural changes that could affect OT workloads. Where PAM tools are in use, enable session recording for privileged administrative access to cloud resources that support OT systems, to support audit and post-incident analysis.

- **Monitor workload and application activity within cloud-hosted systems.**

  Collect telemetry from operating systems, applications, and managed services that support OT workloads. Monitoring should include user logins, administrative commands, configuration changes, and service access logs, where available, to detect anomalous or unauthorized activity within hosted systems.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 8: Audit Log Management
  - 13: Network Monitoring and Defense
- CRI Cloud Profile v2.0 [CRI 2024]
  - DE.CM-03
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Logging and Monitoring (LOG)
  - Universal Endpoint Management (UEM)
- IEC 62443-3-3:2013 [IEC 2013]
  - Foundational Requirement 2: Use control
  - Foundational Requirement 6: Timely response to events
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 8.15: Logging
  - Control 8.16: Monitoring activities
  - Control 8.36: CLD - Detection and prevention of unauthorized use of cloud services

- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Access Control (AC)
  - Audit and Accountability (AU)
  - Assessment, Authorization, and Monitoring (CA)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - DE.CM: Security Continuous Monitoring
  - DE.AE: Anomalies and Events

DE.CM-06 *External service provider activities and services are monitored to find potentially adverse events*

Potential Risks and Considerations

The organization should monitor administrative and maintenance activity that external service providers perform in cloud-supported OT environments. These providers may include cloud providers, managed service providers, systems integrators, OT equipment vendors that perform remote maintenance, and managed security service providers.

Monitoring should preserve individual accountability for actions performed by external service providers. When external service provider personnel authenticate through an external identity system, the organization's logs may record the delegated role or federation session without recording the original authentication event. Individual attribution depends on whether the session includes a unique and reliable identity. The organization should determine which authentication and management records it receives for each access method and identify any gaps. Agreements should require unique identities or attributable sessions, prohibit shared credentials where feasible, and provide access to relevant external service provider records during investigations. Actions performed solely within cloud provider-managed infrastructure may not appear in tenant logs and may require cloud provider evidence or investigative support.

Example Mitigating Controls

- Administrative Controls
  - **Establish monitoring and attribution expectations with external service providers.**

    Define what cloud and external service provider activity the organization needs to see, and record those expectations in agreements. Expectations should include unique and attributable cloud and external service provider identities. Review these expectations when a cloud provider changes how its personnel reach the environment.

- Technical Controls
  - **Monitor external service provider activity in cloud environments.**

    Collect and analyze logs associated with external service provider accounts, including managed service providers, systems integrators, OT equipment vendors, and security service providers. Identify the access methods each provider uses, and determine which authentication events and management operations those methods record in the organization's own logs. Integrate the available telemetry sources with centralized monitoring platforms to detect anomalous access patterns, unexpected configuration changes, or unauthorized privileged actions by provider identities.
- Cloud Provider Controls
  - **Provide attributable records of cloud provider personnel access.**

    Record the actions cloud provider personnel take on customer data and customer environments. Make these records available to customers with the time, the affected resource, the action, and the justification for the access. Identify the accessor by attributes, such as employing entity, location, and job function. Where supported, let customers approve an access request before it proceeds. Document the services covered and the attribution and disclosure limits that apply.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 8: Audit Log Management
  - 13: Network Monitoring and Defense
  - 15: Service Provider Management
- CRI Cloud Profile v2.0 [CRI 2024]
  - DE.CM-06
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Logging and Monitoring (LOG)
  - Universal Endpoint Management (UEM)
- IEC 62443-3-3:2013 [IEC 2013]
  - Foundational Requirement 2: Use control
  - Foundational Requirement 6: Timely response to events
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 8.15: Logging
  - Control 8.16: Monitoring activities

  - Control 8.36: CLD - Detection and prevention of unauthorized use of cloud services
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Access Control (AC)
  - Audit and Accountability (AU)
  - Assessment, Authorization, and Monitoring (CA)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - DE.CM: Security Continuous Monitoring
  - DE.AE: Anomalies and Events

DE.CM-09 *Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events*

Potential Risks and Considerations

Monitoring for cloud-supported OT workloads should cover runtime activity involving computing resources, software, and associated data. Virtual machines, containers, and cloud-deployed applications may face many of the same threats as comparable on-premises environments. Monitoring may include process execution, malware detection, file changes, application behavior, and access to or modification of operational data. Available telemetry depends on the cloud service model and configuration.

For managed services and serverless functions, telemetry may include invocation records, application logs, traces, and the cloud provider's management audit logs, for changes to triggers, permissions, and configurations. Changes to CI/CD pipeline definitions or deployment workflows should be collected from the relevant pipeline, repository, and artifact-management system.

Automated deployment supports consistency, but the speed and scale at which the organization can change resources increase the importance of monitoring for deviations from approved baselines. Monitoring should identify unapproved configuration changes, missing patches, or unexpected software. The organization should retain configuration and deployment records so analysts can trace a runtime deviation to the image, template, automation, or action that introduced it.

The organization should also monitor computing hardware it owns or operates to connect OT environments with cloud technologies. This hardware may include edge gateways, protocol translators, communications equipment, and virtualization hosts. Cloud provider logging does not automatically cover these devices. The organization should monitor their operating health, software and firmware state, configuration changes, administrative activity, and handling of OT data. Correlating this information

with cloud telemetry can help identify adverse events that cross the boundary between local and cloud environments.

Example Mitigating Controls

- Administrative Controls
  - **Validate monitoring agents before deploying them to OT workloads.**

    Test agents in a non-production environment to confirm they do not affect the safety, timing, or reliability of the supported process. Confirm that the system vendor supports the agent, because installing one can void support for some OT applications. Install agents during planned maintenance windows and define how the workload behaves if the agent fails. Where an agent is not acceptable, rely on cloud provider telemetry or other passive sources instead.
- Technical Controls
  - **Monitor cloud runtime environments and software for anomalous activity.**

    Use cloud provider or third-party monitoring solutions to collect telemetry from virtual machines, containers, and other runtime environments that support OT systems. Monitoring should detect indicators such as unauthorized software changes, abnormal process activity, credential misuse, and unexpected data access. Apply file integrity monitoring (FIM) to cloud-hosted OT workloads where changes to critical system files and configurations could affect security or operations. Runtime security options for serverless container platforms differ from those for customer-managed nodes. Confirm which native services or agents the platform supports.
  - **Monitor managed and serverless services that support OT workloads.**

    Identify the managed services that move data between cloud technologies and OT processes, such as event buses, message queues, serverless functions, and data pipelines. Customers generally cannot install traditional host-level monitoring agents on the underlying infrastructure of managed and serverless services. Cloud provider management audit logs may record changes to triggers, permissions, and pipeline definitions. Invocation and message-level records usually require the organization to enable logging for each service, and enabling it does not recover earlier activity. Confirm that logging and retention settings keep the events the organization needs. Monitor for invocations from unexpected sources, changes to triggers or endpoint permissions, and repeated delivery failures on services that support OT workloads.
  - **Monitor access to data that supports OT operations.**

    Collect and analyze access logs for the databases, object storage, file services, and APIs that hold or move OT data. Look for large reads and exports, modification or deletion outside expected processes, and changes to encryption settings or keys. Data plane logging for storage services may not be

enabled by default, so confirm that each source records the events the organization expects.

- **Detect deviations from approved system baselines.**

  Monitor cloud resources and runtime environments for configuration changes that deviate from approved baseline images or templates. CSPM tools identify deviations in cloud resource configuration. It is important to consider that CSPMs may not inspect configurations inside guest operating systems or containers.

- **Correlate telemetry across compute, identity, and network activity.**

  Integrate logs and other telemetry from runtime environments, identity systems, and network monitoring sources to identify complex or multi-stage adverse events affecting cloud resources that support OT systems. SIEM platforms and extended detection and response (XDR) tools may support cross-domain correlation across hybrid OT and cloud environments.

- Cloud Provider Controls
  - **Provide telemetry for managed services customers cannot instrument.**

    Provide service telemetry, findings, or alerts for managed and serverless services where customers cannot deploy their own monitoring. Document what the monitoring covers, what configuration it requires, and where customer visibility ends.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 8: Audit Log Management
  - 9: Email and Web Browser Protections
  - 10: Malware Defenses
  - 13: Network Monitoring and Defense
- CRI Cloud Profile v2.0 [CRI 2024]
  - DE.CM-09
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Change Control and Configuration Management (CCC)
  - Logging and Monitoring (LOG)
  - Universal Endpoint Management (UEM)
- IEC 62443-3-3:2013 [IEC 2013]
  - Foundational Requirement 3: System integrity

  - Foundational Requirement 6: Timely response to events
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 8.15: Logging
  - Control 8.16: Monitoring activities
  - Control 8.23: Web filtering
  - Control 8.36: CLD - Detection and prevention of unauthorized use of cloud services
- MITRE ATT&CK for ICS v19.2 [MITRE 2026]
  - M0803: Data Loss Prevention
  - M0921: Restrict Web-Based Content
  - M0947: Audit
  - M0949: Antivirus/Antimalware
  - M0950: Exploit Protection
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Access Control (AC)
  - Audit and Accountability (AU)
  - Assessment, Authorization, and Monitoring (CA)
  - Configuration Management (CM)
  - System and Communications Protection (SC)
  - System and Information Integrity (SI)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - DE.CM: Security Continuous Monitoring
  - DE.AE: Anomalies and Events

3.4.2 Adverse Event Analysis (DE.AE)

DE.AE-02 *Potentially adverse events are analyzed to better understand associated activities*

Potential Risks and Considerations

Analysis procedures for potentially adverse events should account for how visibility is divided between the organization and the cloud provider. The organization can analyze

activity within its tenant environment, while the cloud provider may hold information about managed services and underlying infrastructure. Neither party may have a complete view of the event. Procedures should identify what information each party can provide, when to request cloud provider support, and how to distinguish customer-managed problems from cloud provider-managed service disruptions or infrastructure conditions.

Event analysis should include personnel who understand the affected OT processes. OT operators, engineers, system owners, and safety personnel can provide context that telemetry alone does not provide. Their involvement can help analysts distinguish malicious or unintended activity from authorized maintenance or equipment faults. This context helps the organization understand the event and determine whether further investigation is needed.

Example Mitigating Controls

- Administrative Controls
  - **Define what analysis results should contain.**

    Establish what analysts record when they analyze an adverse event affecting cloud-supported OT systems. Results should identify the affected entities, the sequence of events, and assigned severity and priority. Results should also separate what the telemetry shows from what the analyst inferred, state the analyst's confidence, describe the effect on operational processes, and note where evidence was unavailable.
  - **Use findings from adverse event analysis to improve detection.**

    Periodically review analyzed events to refine detection logic, update monitoring rules, and improve analytical processes. Lessons learned from prior events can help identify malicious activity and operational anomalies affecting cloud resources that support OT systems.
- Technical Controls
  - **Deploy tools to analyze and correlate cloud telemetry.**

    Use SIEM platforms or similar monitoring tools to collect and analyze telemetry from identity systems, runtime environments, network monitoring sources, and control plane activity logs. These tools should correlate events across multiple systems to identify patterns of suspicious or malicious activity.
  - **Integrate cloud provider telemetry sources into event analysis workflows.**

    Configure monitoring platforms to ingest relevant telemetry generated by cloud technologies so that analysts can investigate potentially adverse events using both tenant-level and provider-generated logs, where available.

- Cloud Provider Controls
  - **Support customer determination of where an event originates.**

    Provide information that helps customers distinguish a customer-managed configuration issue from a service disruption or an infrastructure-level condition. Identify the affected services, regions, and time window, and indicate when a determination is preliminary and subject to revision.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 8: Audit Log Management
- CRI Cloud Profile v2.0 [CRI 2024]
  - DE.AE-02
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Logging and Monitoring (LOG)
- IEC 62443-3-3:2013 [IEC 2013]
  - Foundational Requirement 6: Timely response to events
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.25: Assessment and decision on information security events
  - Control 5.28: Collection of evidence
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Audit and Accountability (AU)
  - Assessment, Authorization, and Monitoring (CA)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - DE.CM: Security Continuous Monitoring
  - DE.AE: Anomalies and Events

DE.AE-03 *Information is correlated from multiple sources*

Potential Risks and Considerations

The organization should correlate relevant logs across on-premises OT systems, cloud environments, and cloud provider services. Hybrid and multi-cloud architectures can increase the number and variety of sources, each with different formats and identifiers. Correlation may combine identity activity, cloud management operations, network flow data, workload and application logs, OT system logs, and available cloud provider

service health information. Without effective correlation of these data sources, the organization may fail to recognize patterns of suspicious activity or coordinated attacks affecting the systems that support operational processes.

Correlation processes should account for cloud-specific identifiers, service identities, short-lived resources, and differences in event timing. Dynamically assigned addresses and rapidly changing resources may require correlation with resource identifiers, identity information, tags, and other cloud metadata. The organization should also normalize timestamps and account for clock differences, collection delays, duplicate records, and records received out of order. Because cloud environments can generate high volumes of logs, correlation processes should deduplicate and prioritize events to preserve analyst effectiveness. In OT environments, prioritization should reflect the safety and reliability consequences of a delayed response.

Example Mitigating Controls

- Technical Controls
  - **Centralize and normalize telemetry for correlation.**

    Deploy centralized monitoring or log analysis platforms, such as SIEM or XDR platforms, that can ingest telemetry from multiple sources, including cloud technology logs, on-premises monitoring systems, runtime environment logs, and threat intelligence feeds. These platforms should correlate events across these data sources to identify patterns of suspicious or malicious activity affecting resources that support OT systems. Where normalization is used, preserve source-specific fields and original records needed for investigation, operational context, and regulatory evidence. Do not rely on a common schema alone when provider-specific fields, OT process context, or service-specific semantics are needed to understand an event.
- Cloud Provider Controls
  - **Publish telemetry schemas, identifiers, and delivery behavior.**

    Publish the telemetry schemas, event identifiers, resource identifiers, and timestamp definitions the service uses, and give advance notice of schema changes. Synchronize timestamps to a reliable time source. Document the expected delivery latency for each log source, and state whether a source can deliver an event more than once or out of order.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 8: Audit Log Management
  - 13: Network Monitoring and Defense

- CRI Cloud Profile v2.0 [CRI 2024]
  - DE.AE-03
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Logging and Monitoring (LOG)
- IEC 62443-3-3:2013 [IEC 2013]
  - Foundational Requirement 6: Timely response to events
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 8.15: Logging
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Audit and Accountability (AU)
  - System and Information Integrity (SI)

DE.AE-04 *The estimated impact and scope of adverse events are understood*

Potential Risks and Considerations

The organization should use up-to-date information about its dependencies and interconnections to estimate the scope of adverse events across hybrid and multi-cloud environments. This information should include relationships among cloud resources, network connections, identity services, provider-managed components, data flows, and the OT processes they support. The analysis should also consider how an event might spread through shared services or interconnected systems. Cloud providers may not expose all internal dependencies of managed services, so analysts should document known dependencies, their assumptions, and remaining visibility gaps.

The organization should use impact analysis to translate affected cloud resources and services into potential consequences for OT operations. Analysts should determine whether cloud resources and services support monitoring, alarming, historian access, engineering support, remote operations, field communications, or backup and recovery. They should consider the criticality of the affected functions, how long the disruption is likely to last, the number of sites involved, and the availability of local or manual alternatives. A compromised identity, a shared network path, a misconfigured policy, or a cloud provider service disruption can affect multiple workloads, sites, or OT functions. Understanding the potential reach helps the organization estimate the operational impact and prioritize response actions.

Example Mitigating Controls

- Administrative Controls
  - **Maintain an inventory of cloud dependencies that support operational processes.**

    Maintain an inventory of cloud technologies, resources, and integrations that support OT systems. Understanding these dependencies helps the organization determine how disruptions that affect specific cloud resources may influence connected systems or downstream operations.
  - **Incorporate cloud-specific logs into impact assessments.**

    Document how analysts should use cloud-specific logs when estimating the impact and scope of adverse events. In addition to logs that record human and non-human activity, consider other sources of information to help identify operational disruptions and abnormal system behavior. Examples include cloud dashboards, cloud provider service health information, or resource utilization data. Additionally, consider both general and account-specific health notifications.
- Technical Controls
  - **Deploy tools to support impact and scope analysis.**

    Use cloud provider or third-party monitoring and analysis tools to determine which resources, identities, and data an adverse event involves. Relevant sources include management activity logs, resource configuration change history, network flow records, data access logs, and workload performance metrics. Correlate these findings with OT operational data to determine which monitoring, analysis, or control functions the event affects. Assess the potential effects on physical processes, employee and public safety, the environment, reliability, and the integrity of operational data. Consider also whether the event forces manual or degraded operations and whether it triggers obligations such as customer notification or regulatory reporting.
  - **Maintain dependency mapping for cloud-supported OT resources.**

    Use cloud provider and third-party asset inventory tools to automate discovery of cloud resources. Map these resources to the OT systems and processes they support. Dependency mappings help analysts understand affected resources, related services, and downstream OT functions during adverse event analysis.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - DE.AE-04

- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Security Incident Management, E-Discovery, and Cloud Forensics (SEF)
- IEC 62443-3-3:2013 [IEC 2013]
  - Foundational Requirement 6: Timely response to events
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.25: Assessment and decision on information security events
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Audit and Accountability (AU)
  - Incident Response (IR)
  - System and Information Integrity (SI)

DE.AE-06 *Information on adverse events is provided to authorized staff and tools*

Potential Risks and Considerations

Distributing information about potentially adverse events promptly helps ensure that appropriate personnel and systems can respond effectively. Cloud integration may expand which parties need adverse event information beyond OT operators who traditionally receive it. For example, security operations personnel who manage shared resources and cloud providers that operate the underlying infrastructure may also need visibility into events. Each recipient should receive enough context to act effectively, but sensitive details about OT architecture and processes should remain limited to recipients who need them. The organization should also route relevant event information to authorized tools so it can correlate, track, escalate, and act on alerts consistently. These tools include security orchestration, automation, and response (SOAR) platforms; SIEM platforms; case management and ticketing systems; and OT monitoring platforms.

The organization should define how alerts and analysis results reach the people and teams responsible for responding to events affecting cloud-supported OT systems. Procedures should identify the required recipients, approved communication channels, acknowledgement requirements, and actions to take when a delivery fails. They should also define what the cloud provider must report and who receives those reports. The organization should maintain at least one out-of-band channel that does not depend on the cloud services that an event may affect.

Example Mitigating Controls

- Administrative Controls
  - **Define roles authorized to receive adverse event information.**

    Identify personnel and operational roles that require access to information about adverse events, such as security operations personnel, incident responders, and OT operators. Establish policies and access controls so the organization distributes adverse event information only to authorized individuals and teams.
  - **Establish requirements for sharing adverse event information promptly.**

    Define procedures and contractual expectations for sharing information about adverse events with relevant internal teams and external partners, including cloud providers. These procedures should support timely communication of events that may affect cloud resources or OT systems.
- Technical Controls
  - **Distribute adverse event information to responsible personnel and response tools.**

    Configure monitoring tools to aggregate and distribute adverse event information across security operations, incident response, and OT operations. Centralizing this information helps ensure that relevant personnel and automated response tools have what they need to investigate and respond to events. Where SOAR platforms are deployed, configure playbooks to automatically route adverse event information to appropriate teams and systems based on event type, severity, and the OT systems potentially affected.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - DE.AE-06
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Logging and Monitoring (LOG)
- IEC 62443-3-3:2013 [IEC 2013]
  - Foundational Requirement 6: Timely response to events
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.25: Assessment and decision on information security events
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Audit and Accountability (AU)

- Incident Response (IR)
- System and Information Integrity (SI)

DE.AE-07 *Cyber threat intelligence and other contextual information are integrated into the analysis*

Potential Risks and Considerations

Event analysis for cloud-supported OT systems should incorporate both cloud-focused and OT-focused cyber threat intelligence sources. Relevant sources may include cloud provider threat research and advisories, Cybersecurity and Infrastructure Security Agency (CISA) Industrial Control Systems (ICS) advisories, ISAC alerts and advisories, OT vendor notifications, and commercial and open-source threat intelligence. Vulnerability disclosures and cloud provider-generated alerts can provide additional context. Together, these sources may help analysts identify indicators of compromise (IOCs), adversary tactics, techniques, and procedures (TTPs), and emerging threats that a source focused only on cloud or OT might not capture.

The organization should evaluate and contextualize threat intelligence before applying it to event analysis. Analysts should determine whether the intelligence applies to the cloud services, OT assets, software versions, and integrations in use. They should correlate relevant intelligence with internal logs and consider asset criticality, known vulnerabilities, system dependencies, current process conditions, approved changes, and potential operational impacts. This context helps analysts determine whether observed activity could affect safe and reliable operations and prevents irrelevant indicators from distracting from higher-priority events.

Example Mitigating Controls

- Technical Controls
  - **Integrate threat intelligence into event analysis platforms.**

    Configure monitoring and analysis platforms to incorporate external threat intelligence for additional context. Integrating these data sources with telemetry from cloud technologies, runtime environments, and identity systems can help analysts identify IOCs and better understand emerging threats that affect OT systems. Consider the use of structured intelligence formats and exchange protocols, such as Structured Threat Information eXpression (STIX) and Trusted Automated Exchange of Intelligence Information (TAXII), to ingest and share threat indicators with ISACs and trusted partners. Configure platforms to record where each indicator came from and how much confidence it carries, to expire or remove indicators that are no longer valid, and to reconcile duplicate or conflicting entries from different sources. Tune matching so that indicators with little relevance to the environment do not generate alerts that analysts cannot act on. Where supported, configure platforms to automatically enrich

detected IOCs with threat intelligence context at detection time to reduce analyst effort and accelerate response.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - DE.AE-07
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.7: Threat intelligence
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Program Management (PM)
  - Risk Assessment (RA)

DE.AE-08 *Incidents are declared when adverse events meet the defined incident criteria*

Potential Risks and Considerations

The organization should update its incident declaration criteria to address adverse events in cloud-supported OT environments. Existing criteria, such as confirmed unauthorized access or loss of view of a process, may remain applicable. Additional criteria may address unauthorized changes to identity federation, unauthorized creation or modification of cloud resources, or exposure of cloud storage containing operational data. Criteria should address observed and potential effects on OT safety, reliability, visibility, remote access, recovery, data integrity, or regulatory obligations. When the cause remains unclear, procedures should allow the organization to manage an event as both a service disruption and a potential cybersecurity incident until analysis resolves the question. This approach can help the organization avoid over-escalating routine service issues while declaring and addressing cloud-related events with operational consequences quickly.

Incident declaration and notification procedures should account for differences between the cloud provider and the organization in the information each can see and the criteria each uses. Contracts and response plans should define which events each party reports to the other, the required timeframes, designated contacts, communication channels, and information to provide. In some cases, each party may have visibility into different aspects of an event, and they may need to coordinate their analysis before determining whether incident criteria have been met. However, either party may make a provisional incident declaration as soon as its own criteria are met and continue coordinated analysis afterward. Procedures should map each applicable legal, regulatory, and contractual reporting obligation to its specific triggering condition, deadline, decision authority, and reporting party. Unclear declaration criteria or authority

can delay response and increase or prolong the impact of disruptions affecting OT systems.

The organization should periodically test its incident declaration criteria and supporting communication procedures. Exercises should evaluate whether alerts reach the correct decision-makers, whether personnel apply criteria consistently, and whether coordination with the cloud provider, where supported and appropriate, contributes to timely decisions. Reviews should identify events that the criteria missed, events personnel escalated unnecessarily, and delays caused by unclear authority or incomplete information. The organization should update its criteria and procedures based on these findings.

Example Mitigating Controls

- Administrative Controls
  - **Define incident declaration criteria for cloud-supported OT systems.**

    Establish and maintain criteria that define when a potentially adverse event affecting cloud resources that support OT systems becomes a cybersecurity incident. Include cloud-specific triggers for triage and incident assessment, such as a cloud provider-declared service event, loss of monitoring visibility, or unexpected control plane activity. Declare an incident when analysis determines that the event meets the organization's cybersecurity incident criteria, applicable reporting triggers, or defined operational-impact thresholds.
- Technical Controls
  - **Implement automated workflows for incident declaration and escalation.**

    Deploy monitoring or incident management capabilities, such as SOAR platforms, that can evaluate adverse events against predefined criteria and initiate response actions. These capabilities may integrate with provider-offered alerting, ticket creation, and escalation to authorized personnel responsible for responding to incidents affecting cloud resources that support OT systems. A named individual should approve any automated action that could disrupt an OT process. The organization may pre-authorize a narrow set of actions, provided it defines how each one fails safely and how responders reverse it.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 17: Incident Response Management
- CRI Cloud Profile v2.0 [CRI 2024]
  - DE.AE-08
- IEC 62443-3-3:2013 [IEC 2013]
  - Foundational Requirement 6: Timely response to events

- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.25: Assessment and decision on information security events
  - Control 5.26: Response to information security incidents
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Incident Response (IR)

3.5 Respond (RS)

The Respond Function comprises four Categories:

- Incident Management (RS.MA)
- Incident Analysis (RS.AN)
- Incident Response Reporting and Communication (RS.CO)
- Incident Mitigation (RS.MI)

3.5.1 Incident Management (RS.MA)

RS.MA-01 *The incident response plan is executed in coordination with relevant third parties once an incident is declared*

Potential Risks and Considerations

During an incident affecting cloud-supported OT systems, the organization should activate a response structure that coordinates internal personnel and relevant third parties. While core incident response principles remain consistent, coordination procedures should account for shared responsibility boundaries, differences in visibility between the organization and the cloud provider, and cloud provider-managed service components. OT operators, engineers, and system owners should participate when response actions could affect operational processes. The organization should clearly define who has the authority to approve actions that carry operational consequences, including transitioning to degraded or local operating modes, isolating affected functions, and authorizing the return of OT systems to service.

The evidence available to incident responders depends on the service model, configuration, and provider capabilities. Evidence may include logs, configuration records, snapshots, memory, packet captures, resource metadata, and provider-held information. Some log sources require explicit configuration, and enabling them after an incident does not provide earlier records. Incident response plans should ensure that personnel have the knowledge, tooling, and access required to retrieve and analyze these records without delay. Before an incident, the organization should configure and test logging, analysis tools, access rights, and evidence preservation. For cloud

provider-managed evidence, procedures should identify the request process, available records, applicable retention periods, and expected delivery time.

The organization should use established cloud provider support and escalation pathways when executing its incident response plan. Cloud provider severity classifications may not reflect the safety, reliability, or operational consequences of an incident for the organization. The organization should map incident priorities to the cloud provider's published support levels and compare its requirements, such as safety thresholds, availability requirements, and recovery time expectations, against what the cloud provider commits to deliver. The organization should document where the two diverge and define internal procedures that cover the difference. Incident leads, escalation contacts, and handoff procedures should help the organization coordinate timely actions across organizational and cloud provider boundaries. Without structured coordination and defined roles, response efforts may be delayed, inconsistent, or fragmented. These effects increase the likelihood that incidents will disrupt OT operations or hinder effective incident containment and recovery.

Example Mitigating Controls

- Administrative Controls
  - **Define incident response roles, responsibilities, and escalation paths for cloud-supported OT systems.**

    Establish and document roles, responsibilities, escalation thresholds, and response time expectations for incidents that affect cloud-supported OT systems. Use operational-level agreements to define handoffs between internal IT, OT, and cloud teams, including coordination procedures, recovery responsibilities, and out-of-band communication channels. Inventory the notification timelines and evidence sharing commitments in the cloud provider's standard service agreement. Document the gaps between cloud provider commitments and OT response requirements.
- Technical Controls
  - **Implement automated incident detection and notification mechanisms.**

    Deploy automated monitoring and alerting capabilities across cloud-supported OT environments to detect deviations in configurations, identity use, connectivity, or service performance that may indicate a security incident. Integrate cloud provider-originated notifications and tenant-generated alerts into centralized response workflows.
- Cloud Provider Controls
  - **Provide mechanisms to support timely incident notification and coordination.**

    Maintain technical capabilities to notify customers of security or operational incidents that affect their tenant environments or relevant provider-managed services. Provide secure communication channels and status tracking

mechanisms to support coordinated investigation, containment, and recovery activities.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - RS.MA-01
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Security Incident Management, E-Discovery, and Cloud Forensics (SEF)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.26: Response to information security incidents
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Incident Response (IR)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - RS.RP: Response Planning
  - RS.CO: Response Communications
  - RS.AN: Response Analysis
  - RS.MI: Response Mitigation

RS.MA-02 *Incident reports are triaged and validated*

Potential Risks and Considerations

Triage criteria for incident reports in cloud-supported OT environments should reflect potential operational consequences. Events involving cloud-hosted applications, identity services, data integrations, or remote access may affect process visibility, field communications, control systems, or operator interfaces. Triage should consider the available technical indicators, the OT functions involved, and credible effects on safety, reliability, or operational continuity. An incident with potentially significant OT consequences may warrant prioritization and escalation by the organization before its cause and full scope are confirmed.

Validation procedures should define the evidence needed to assess incident reports involving cloud-supported OT systems. Responders may need tenant logs, application logs, identity activity, OT system data, change records, and information held by the cloud provider. Procedures should help responders determine what occurred, distinguish confirmed cybersecurity incidents from false positives, and determine whether the report meets the organization’s incident criteria. When needed evidence

resides with the cloud provider, responders should use established request and escalation processes and document any remaining gaps or uncertainty.

Example Mitigating Controls

- Administrative Controls
  - **Establish coordinated validation processes with cloud providers.**

    Define how the organization incorporates cloud-originated alerts, cloud provider notifications, and tenant-level telemetry into OT incident validation processes. Ensure that service agreements and operational procedures specify notification timelines, available data sources, and points of contact to support timely validation of incidents that affect cloud-supported OT systems.
  - **Align internal roles and escalation pathways for incident validation.**

    Define and document how IT, OT, and cloud administration teams collaborate during triage and validation activities. Clearly establish escalation thresholds and decision authority to prevent delays in classifying and prioritizing incidents.
- Technical Controls
  - **Centralize collection and analysis of OT and cloud incident data.**

    Implement capabilities to aggregate relevant OT system alerts, cloud telemetry, and cloud provider notifications to support timely correlation and validation of reported incidents. Apply standardized severity criteria to classify and prioritize incidents consistently. Establish processes for managing false-positive alerts to prevent high alert volumes from obscuring genuine incidents, particularly during periods of operational change or cloud platform updates that may temporarily increase alert noise.
- Cloud Provider Controls
  - **Support incident validation activities for customer environments.**

    Consistent with contractual commitments, provide timely access to relevant incident-related information and coordinate with customers to clarify the scope, severity, and impact of reported events that affect tenant environments.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - RS.MA-02
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Security Incident Management, E-Discovery, and Cloud Forensics (SEF)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.26: Response to information security incidents

- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Incident Response (IR)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - RS.RP: Response Planning
  - RS.CO: Response Communications
  - RS.AN: Response Analysis
  - RS.MI: Response Mitigation

RS.MA-03 *Incidents are categorized and prioritized*

Potential Risks and Considerations

Incident categorization for cloud-supported OT systems should account for both cybersecurity significance and potential operational consequences. An incident involving a cloud-hosted application, identity system, remote access pathway, or data platform may have downstream effects on operator interfaces, engineering support, or communications with field devices. The organization should consider actual and potential effects on safety, reliability, physical processes, mission objectives, and regulatory compliance, in addition to confidentiality, integrity, and availability.

Incident prioritization criteria should be consistent across cloud, IT, and OT response processes. These criteria should consider the affected functions, the number of sites or systems involved, the potential for the incident to spread, available fallback capabilities, and the urgency of operational action. An incident affecting a cloud-based business system may still warrant high priority if that system supports OT identity, monitoring, communications, or recovery. Aligning severity levels and escalation thresholds helps ensure that incidents with safety, reliability, or mission consequences receive appropriate attention and resources.

Example Mitigating Controls

- Administrative Controls
  - **Review and align incident categorization and prioritization criteria across OT, IT, and cloud environments.**

    Review and update incident categories, severity levels, and prioritization criteria so they reflect the potential effect of cybersecurity events on cloud-supported OT systems. Ensure that these criteria account for both the cybersecurity characteristics of the event and its potential operational consequences, including safety, reliability, regulatory conformance, and service continuity considerations, regardless of whether the event originates in a cloud, IT, or OT domain.

- Technical Controls
  - **Automate preliminary incident categorization using predefined criteria.**

    Configure monitoring and incident management tools to apply predefined classification and severity rules that account for the potential effects on cloud-supported OT systems. Review and validate automated categorizations before making final prioritization, escalation, and response decisions.
  - **Centralize incident tracking with impact-based prioritization.**

    Implement an integrated incident tracking capability that consolidates cloud, IT, and OT alerts and assigns priorities based on defined impact criteria. SOAR platforms can support this function by integrating with provider-offered alerting services, OT monitoring systems, and ticketing platforms to provide a unified incident view with automated priority assignment.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - RS.MA-03
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Security Incident Management, E-Discovery, and Cloud Forensics (SEF)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.26: Response to information security incidents
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Incident Response (IR)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - RS.RP: Response Planning
  - RS.CO: Response Communications
  - RS.AN: Response Analysis
  - RS.MI: Response Mitigation

RS.MA-04 *Incidents are escalated or elevated as needed*

Potential Risks and Considerations

Incident escalation processes in cloud-supported OT environments should involve personnel and external stakeholders needed to manage the incident. Predefined escalation triggers should reflect actual or potential effects on safety, reliability,

regulatory obligations, or service continuity. OT teams and cloud providers may use different severity levels, response models, and terminology.

Example Mitigating Controls

- Administrative Controls
  - **Establish documented escalation criteria and decision authority for incidents affecting OT.**

    Define clear escalation triggers for incidents that may affect cloud-supported OT systems, including potential effects on safety, reliability, regulatory obligations, and service continuity. Identify decision-makers, escalation pathways, and external coordination points for elevating incidents internally and with cloud providers. Ensure that these criteria align with contractual notification timelines and coordination expectations.
  - **Establish and test procedures for escalating incidents to cloud providers.**

    Define how the organization escalates incidents to the cloud provider, including how the organization's severity levels map to the cloud provider's support case severities, designated points of contact, and handoff procedures. Periodically review and test these procedures using tabletop exercises to confirm that internal responders understand escalation thresholds and communication channels.
- Technical Controls
  - **Implement automated notification and case-routing capabilities to support incident escalation.**

    Use incident management and monitoring platforms, including SOAR platforms where deployed, to route, notify, and elevate incidents based on predefined escalation triggers for cloud-supported OT environments. Ensure that automated workflows notify designated internal stakeholders, leadership, and external contacts, as appropriate, when incidents meet established escalation thresholds.
- Cloud Provider Controls
  - **Operate documented incident escalation channels.**

    Publish the escalation procedures, severity definitions, contact methods, and response commitments that apply to each support offering. Accept operational impact information from authorized customer contacts and weigh it when evaluating an escalation request. Route escalated incidents to personnel who can coordinate the response, and report case status. Provide an alternate contact method for use when the primary channel is unavailable.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - RS.MA-04
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Security Incident Management, E-Discovery, and Cloud Forensics (SEF)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.26: Response to information security incidents
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Incident Response (IR)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - RS.RP: Response Planning
  - RS.CO: Response Communications
  - RS.AN: Response Analysis
  - RS.MI: Response Mitigation

RS.MA-05 *The criteria for initiating incident recovery are applied*

Potential Risks and Considerations

Recovery should only begin when defined technical and operational criteria show that restoration can proceed safely. These criteria should determine whether containment has sufficiently reduced the threat, eradication has progressed far enough, and the remaining risk is acceptable. Recovery may begin while containment or eradication continues if the organization can control that risk. For cloud-supported OT environments, the organization should confirm the integrity of data and recovery artifacts, the availability of required identity and network services, and the monitoring needed to detect renewed malicious activity.

Example Mitigating Controls

- Administrative Controls
  - **Define recovery criteria for cloud-supported OT systems.**

    Establish and document criteria for initiating recovery activities for incidents that affect cloud-supported OT systems. Criteria should reflect system or asset criticality tiers and include thresholds based on operational impact, data integrity validation, service availability, and dependency status across

on-premises and cloud components. Incorporate these criteria into incident response and continuity plans.

- **Align recovery planning across OT and cloud-service dependencies.**

  Develop recovery plans that account for dependencies between OT systems and cloud technologies, including identity services, data platforms, and application components. Define sequencing and coordination requirements to ensure that restoration actions are consistent with operational priorities and documented service expectations. Where the organization uses IaC, recovery plans should include procedures for redeploying infrastructure and configuration from known-good IaC templates. Service-specific recovery mechanisms may be needed to restore data, secrets, keys, certificates, or identity objects where the service supports recovery. For cryptographic keys and key material, document recovery limits in advance. Deleted, purged, destroyed, or unavailable keys may make dependent data or backups unrecoverable.

- Technical Controls
  - **Implement monitoring and validation mechanisms to support recovery decision making.**

    Deploy tools and processes that monitor restoration progress across OT and cloud environments and validate that predefined recovery criteria have been met before restoration proceeds or full operational status resumes. Make recovery status visible to relevant stakeholders to support informed decision making and escalation when recovery objectives are not met.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - RS.MA-05
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Security Incident Management, E-Discovery, and Cloud Forensics (SEF)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.26: Response to information security incidents
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Incident Response (IR)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - RS.RP: Response Planning
  - RS.AN: Response Analysis
  - RS.IM: Response Improvement

3.5.2 Incident Analysis (RS.AN)

RS.AN-03 *Analysis is performed to establish what has taken place during an incident and the root cause of the incident*

Potential Risks and Considerations

RCA for incidents affecting cloud-supported OT systems should examine events across cloud, IT, OT, and physical processes. Distributed telemetry and software-defined architectures can make it difficult to reconstruct the sequence and effect of an incident. Analysis should correlate identity, control plane, network, workload, application, and OT process data. For customer-managed resources, the organization generally collects available evidence within its tenant. For provider-managed services, the organization may depend on provider-exposed telemetry, exported records, and cloud provider investigative support.

Effective RCA depends on forensic readiness established before an incident. The organization should identify required data sources, provide appropriate access, assign forensic roles, and establish procedures for log retention and evidence handling. For architectures that span multiple geographic regions, service models, or cloud providers, planning should address how the organization aggregates and normalizes data to support timely analysis.

Available forensic evidence varies by cloud resource type. Short-lived resources may require the organization to preserve evidence before resources are stopped, replaced, or terminated. For provider-managed and serverless components, available evidence may include service-native logs, traces, audit records, and configuration history.

Example Mitigating Controls

- Administrative Controls
  - **Establish cloud evidence handling and arrange cloud provider investigative support in advance.**

    Document chain-of-custody procedures for cloud-acquired evidence to support legal proceedings and regulatory compliance. Consider whether additional support from the cloud provider or a third party is needed to support evidence collection and analysis. Some cloud providers offer investigative support through higher support tiers or professional services.
- Technical Controls
  - **Implement cross-domain incident analysis capabilities.**

    Deploy tools and architectures that support aggregation, normalization, and correlation of telemetry from OT systems and cloud environments. Enable investigators to analyze events across identity, network, application, and control system layers to reconstruct the sequence of events and determine the

scope of the incident and its root causes. Investigations may require sources the detection pipeline does not routinely collect or normalize, such as provider-supplied logs obtained on request, archived or cold-storage data, resource snapshots, and configuration history. Retrieval from archival storage tiers may take significantly longer than retrieval from active storage. Confirm expected retrieval times when planning investigative procedures.

- **Establish investigation readiness through pre-authorized access and evidence logging.**

  Predefine and provision the role-based access needed for authorized personnel to investigate incidents across OT and cloud environments. Enable and retain relevant audit logs, configuration records, and event data, and make them retrievable in a way that supports timely analysis, separation of duties, and evidence integrity.

- Cloud Provider Controls
  - **Document the evidence available to customers for each service model.**

    Publish which telemetry, log sources, and configuration records customers can retrieve for each service model, including what is available for managed and serverless components. Identify the default retention period, the retention options customers can configure, and the sources that require a support request. State the limits of the evidence available to customers so they can plan investigations around them.

  - **Describe investigative support offerings and their scope in advance.**

    Describe the investigative support available to customers, including what a standard support case covers and what requires a paid subscription or professional services engagement. Document what access is needed to conduct this work and how the investigation information will be provided to the customer.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - RS.AN-03
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Security Incident Management, E-Discovery, and Cloud Forensics (SEF)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.26: Response to information security incidents
  - Control 5.28: Collection of evidence
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Incident Response (IR)

- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - RS.AN: Response Analysis

RS.AN-06 *Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved*

Potential Risks and Considerations

The organization should define and enforce requirements for recording the actions taken by both the organization and the cloud provider during incident response and investigation activities affecting cloud-supported OT environments. Case management or ticketing systems should capture actions performed across on-premises and cloud environments, including changes made through cloud management interfaces, APIs, identity systems, and configuration tools. Records should identify who performed the action, what was changed or accessed, when it occurred, the tool or access path used, and the authorization or approval associated with the action. To support timeline reconstruction and evidentiary integrity, the organization should preserve original timestamps, protect records from unauthorized modification, and retain them according to organizational, legal, and regulatory requirements.

Example Mitigating Controls

- Administrative Controls
  - **Establish documentation requirements for incident investigations.**

    Define requirements for documenting actions taken during incident response and investigation activities across OT and cloud environments. Ensure that responders record actions performed through cloud management interfaces, APIs, administrative consoles, and OT systems.
  - **Define expectations for third-party incident documentation and information sharing.**

    Evaluate and document the incident notification and information sharing commitments in the cloud provider's standard customer agreement. These commitments generally cover notification of incidents affecting customer data and may not extend to delivering incident records or preserving cloud provider-side evidence. Record the resulting evidence gap in the incident record so the investigation reflects what was available. For other third parties, such as integrators, vendors, and managed service providers, establish contractual provisions that address retention expectations, communication channels, and requirements for preserving the integrity and provenance of supplied information.

- Technical Controls
  - **Preserve the integrity of investigation records and responder activity logs.**

    Implement mechanisms that protect investigative documentation, responder activity records, and cloud audit trails from unauthorized modification or deletion. Enable and protect provider-offered audit trail services for environments that support OT systems, so records include API calls and management operations with timestamps and identity attribution. Use access restrictions and immutable or WORM storage to prevent unauthorized modification or deletion of retained records. Use digital signatures or comparisons with separately protected cryptographic digests to detect alteration.
- Cloud Provider Controls
  - **Provide records of cloud provider actions taken during incidents.**

    Record cloud provider personnel access to customer data and customer environments during incident investigation and response. Include the accessor attributes, time, affected resource, action, and justification. Make the support case history available to the customer. Before an incident, state which records customers can obtain and how long each is retained. Identify the actions these records do not capture, so customers can document the resulting evidence gap.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - RS.AN-06
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Security Incident Management, E-Discovery, and Cloud Forensics (SEF)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.26: Response to information security incidents
  - Control 5.28: Collection of evidence
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Incident Response (IR)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - RS.AN: Response Analysis

RS.AN-07 *Incident data and metadata are collected, and their integrity and provenance are preserved*

Potential Risks and Considerations

Incident collection plans for cloud-supported OT environments should include relevant data and metadata from OT, cloud, and external sources. These sources include tenant logs, control plane activity, API calls, identity records, cloud provider service health events, and other cloud provider or third-party telemetry. Where available, cloud provider APIs or event streams can support timely collection of service health events.

The organization should preserve the integrity and provenance of incident data. At collection, responders should preserve the original record and source metadata, sign the evidence, and store verification information separate from evidence. Verification information should be protected similarly to collected evidence to ensure it can be used to validate the integrity and provenance of evidence. The organization may also need to account for applicable regulatory and legal retention requirements for incident records.

Example Mitigating Controls

- Administrative Controls
  - **Establish evidence handling requirements for incident data and metadata.**

    Define requirements for collecting, labeling, retaining, and preserving incident data and metadata from OT and cloud environments. Limit collection, modification, and retrieval of incident data to authorized personnel. Require practices that preserve timestamps, source attribution, chain of custody, and other provenance information throughout collection, transfer, storage, and use.
- Technical Controls
  - **Implement integrated incident data and metadata collection capabilities.**

    Deploy tools to collect, correlate, and preserve incident data and metadata from OT and cloud environments. Require both time synchronization and normalized time handling. Synchronize each clock to an authoritative time source. Preserve original timestamps and source attributes, and apply retention settings aligned with investigative, legal, regulatory, and operational requirements. Where available, use cloud provider evidence preservation features. These include object immutability with retention policies and legal hold on the storage containing exported logs and evidence.
  - **Use protected storage mechanisms for incident evidence.**

    Store collected incident data and metadata in secure locations that prevent unauthorized alteration or deletion. Apply immutability controls, access restrictions, monitoring, and, where applicable, legal hold capabilities to preserve evidentiary integrity and meet legal or regulatory retention obligations.

- Cloud Provider Controls
  - **Provide evidence export and preservation capabilities.**

    Provide mechanisms that let customers export telemetry, logs, and configuration records to storage the customer controls. Provide immutability capabilities on that storage, such as retention policies and legal hold, and document which services support them. Preserve original timestamps and source attribution in exported records.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - RS.AN-07
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Security Incident Management, E-Discovery, and Cloud Forensics (SEF)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.26: Response to information security incidents
  - Control 5.28: Collection of evidence
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Incident Response (IR)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - RS.AN: Response Analysis

RS.AN-08 *An incident's magnitude is estimated and validated*

Potential Risks and Considerations

The organization should estimate and validate incident magnitude based on both technical scope and potential operational consequences. The assessment should identify affected assets, services, identities, control plane activity, data flows, and downstream OT processes across on-premises and cloud environments. Magnitude does not depend solely on the number of affected cloud resources. It also depends on whether those resources support critical operational processes, shared services, or connectivity paths that OT functions rely on.

Example Mitigating Controls

- Administrative Controls
  - **Incorporate cloud-supported OT dependencies into estimation criteria for determining the magnitude of incidents.**

    Update processes for estimating incident magnitude to account for cloud resources, services, identities, and connectivity paths that support OT functions. These processes should evaluate the extent of affected assets and services, the operational significance of those assets and services, and potential safety, reliability, regulatory, environmental, and service continuity impacts.
- Technical Controls
  - **Implement cross-domain analysis capabilities to support incident magnitude estimates.**

    Use monitoring and analysis tools that aggregate telemetry from OT systems, cloud workloads, identity services, and network components to help estimate the scope of affected assets, services, and functions across environments. Apply automated analyses where appropriate to support initial estimates while requiring human validation to confirm operational significance and overall incident magnitude.

Informative References

- CRI Cloud Profile v2.0 [CRI 2024]
  - RS.AN-08
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Security Incident Management, E-Discovery, and Cloud Forensics (SEF)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.26: Response to information security incidents
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Incident Response (IR)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - RS.AN: Response Analysis

3.5.3 Incident Response Reporting and Communication (RS.CO)

RS.CO-02 *Internal and external stakeholders are notified of incidents*

Potential Risks and Considerations

Incident notifications for cloud-supported OT environments should give stakeholders timely and accurate information that supports both cybersecurity response and operational decision making. Notifications should describe the affected cloud and OT functions, known or potential impacts, interim measures, and expected time of the next update. Standard templates can support consistency while allowing the organization to tailor content to each audience.

Incident notification procedures should account for applicable legal, regulatory, and contractual obligations. Entities subject to the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards should map reporting requirements and timelines in the applicable version of CIP-008 to their internal incident categories and workflows [NERC 2019]. Covered pipeline owners and operators should similarly account for applicable TSA security directive cybersecurity incident reporting requirements [TSA 2026]. Applicability may depend on the entity, its registration or designation, the affected systems, and how cloud technologies support those systems. Before an incident occurs, the organization should identify each reporting trigger, deadline, decision authority, recipient, and responsible reporting party.

Example Mitigating Controls

- Administrative Controls
  - **Define requirements for notifying internal and external stakeholders of incidents.**

    Define which internal and external stakeholders the organization must notify for incidents affecting cloud-supported OT environments and specify the conditions that trigger notification. Establish required content, approval authorities, and timelines so that notifications support operational decision making and satisfy contractual, regulatory, and legal obligations.
- Technical Controls
  - **Implement secure and auditable mechanisms for incident notifications.**

    Use incident tracking and communication platforms that support controlled distribution of incident notifications to authorized stakeholders, including out-of-band communication channels that remain available if primary cloud or IT systems are compromised or degraded. Maintain pre-drafted notification templates for common incident scenarios involving cloud-supported OT systems to support timely and consistent communication during incident response. Ensure that notification mechanisms maintain records of timing,

recipients, content, and delivery status to support regulatory compliance and post-incident review.

- Cloud Provider Controls
  - **Provide notification content sufficient to support customer reporting obligations.**

    Include in incident notifications the information customers need for their own regulatory and contractual reporting, including the affected services, the time window, and the current understanding of scope. Indicate when a determination is preliminary.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 17: Incident Response Management
- CRI Cloud Profile v2.0 [CRI 2024]
  - RS.CO-02
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Security Incident Management, E-Discovery, and Cloud Forensics (SEF)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.5: Contact with authorities
  - Control 5.6: Contact with special interest groups
  - Control 5.26: Response to information security incidents
- MITRE ATT&CK for ICS v19.2 [MITRE 2026]
  - M0810: Out-of-Band Communications Channel
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Incident Response (IR)
  - Supply Chain Risk Management (SR)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - RS.CO: Response Communications

RS.CO-03 *Information is shared with designated internal and external stakeholders*

Potential Risks and Considerations

During incident response, the organization should share relevant information with designated stakeholders under predefined agreements, response plans, and handling

procedures. Information sharing should balance transparency with the need to protect sensitive operational, architectural, and security information. The organization may apply sharing labels, such as those defined in the traffic light protocol (TLP), to indicate "sharing boundaries to be applied by the recipients" [FIRST 2022].

The organization should tailor incident information to each recipient's role and information needs. Senior leadership may require concise updates on operational impact and risk, while technical teams may require detailed indicators, system data, and remediation actions. Legal, compliance, and other support functions may need information related to regulatory or contractual matters. When authorized, sharing information with ISACs, cloud providers, trusted peers, equipment manufacturers, and software vendors can support coordinated response and broader situational awareness. Without clearly defined content requirements and secure distribution practices, the organization risks unauthorized disclosure of sensitive OT information, inconsistent coordination with suppliers, or misinterpretation of incident status by internal or external stakeholders.

Example Mitigating Controls

- Administrative Controls
  - **Define information-sharing requirements for OT and cloud-related incidents.**

    Define and document how the organization shares incident information internally and externally when cloud technologies support OT environments. Specify authorized recipients, required content, approval authorities, handling restrictions, and secure communication channels. Ensure that these requirements align with obligations under regulatory requirements, contracts, and information-sharing agreements.
- Technical Controls
  - **Implement secure and auditable information sharing mechanisms.**

    Use communication and incident management platforms that support controlled distribution of incident information derived from OT and cloud systems. Configure these systems to enforce role-based access, protect sensitive operational data, and maintain audit records of shared information to support accountability and post-incident review.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 17: Incident Response Management
- CRI Cloud Profile v2.0 [CRI 2024]
  - RS.CO-03

- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Security Incident Management, E-Discovery, and Cloud Forensics (SEF)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.6: Contact with special interest groups
  - Control 5.26: Response to information security incidents
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Incident Response (IR)
  - Supply Chain Risk Management (SR)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - RS.CO: Response Communications

3.5.4 Incident Mitigation (RS.MI)

RS.MI-01 *Incidents are contained*

Potential Risks and Considerations

Containment strategies for cloud-supported OT environments should limit incident spread without creating unacceptable safety and reliability effects. The appropriate action depends on the operational role of the affected cloud technology and its dependencies. An analytics or monitoring service may require different treatment than an identity, remote access, or data exchange service. Before isolating a resource or severing a connection, the organization should assess the critical functions and visibility it would lose, the fallback capabilities available, and how operators would continue working.

Containment capabilities vary by service model and shared responsibility. In IaaS environments, the organization can typically isolate workloads, change network and access policies, revoke credentials, and restrict data flows. In PaaS environments, containment options depend on the controls exposed by the platform and may include application, configuration, identity, secret, and network changes. In SaaS environments, containment actions are generally more limited and may focus on accounts, integrations, and cloud provider-supported isolation actions. The organization should document the actions it can perform, the conditions for using them, and the cloud provider request and escalation process for actions only the cloud provider can perform.

Identity-based containment should address both human and non-human identities. Actions may include disabling accounts, invalidating sessions, forcing reauthentication, and rotating credentials. Disabling an identity at the enterprise identity provider can prevent new authentication, but it may not invalidate existing access tokens or sessions. These tokens and sessions may remain usable until they are revoked, denied by policy,

or expire. The organization should understand how to revoke or block those credentials and assess the operational effect before disabling service accounts, workload identities, or other non-human identities that support OT functions.

Example Mitigating Controls

- Administrative Controls
  - **Define containment procedures that account for OT operational impact.**

    Establish containment procedures for incidents affecting cloud-supported OT environments, including who authorizes containment actions and how the organization evaluates operational impact before acting. Procedures should identify which cloud technologies support monitoring, alerting, or control functions that operators depend on, so containment actions do not disrupt those functions.
- Technical Controls
  - **Implement logical and network segmentation to limit incident propagation.**

    Apply segmentation strategies across OT and cloud-integrated environments to isolate affected systems and restrict unauthorized communication. Use logical isolation mechanisms, access control policies, and network rule updates to contain incidents while preserving critical operations. Verify whether each mechanism blocks only new connections or also interrupts established connections.
  - **Deploy and configure containment capabilities across OT and cloud domains.**

    Use security technologies and enforcement mechanisms that enable both automated and manual containment actions, such as credential revocation, workload quarantine, policy enforcement, and traffic restriction. Configure containment tools to support rapid action while requiring authorization and validation to prevent unintended operational impact.
- Cloud Provider Controls
  - **Notify customers of protective actions and provide isolation mechanisms.**

    When an emergency action is needed to protect the platform or customers, take it and notify affected customers promptly. In the notice, identify the affected resources, the action taken, its expected effect, and any action the customer needs to take. Provide mechanisms that let customers restrict access to, or isolate, their own resources and service connections.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 17: Incident Response Management
- CRI Cloud Profile v2.0 [CRI 2024]
  - RS.MI-01
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Security Incident Management, E-Discovery, and Cloud Forensics (SEF)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.26: Response to information security incidents
  - Control 8.8: Management of technical vulnerabilities
  - Control 8.32: Change management
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Incident Response (IR)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - RS.MI: Response Mitigation
  - RS.IM: Response Improvement

RS.MI-02 *Incidents are eradicated*

Potential Risks and Considerations

Eradication in cloud-supported OT environments should remove malicious artifacts, persistence mechanisms, and exploited weaknesses across on-premises and cloud systems. Actions may include removing malicious code, rotating compromised credentials, correcting misconfigurations, patching vulnerabilities, and closing unauthorized access paths.

Eradication should include validating artifacts and recovery sources that could reintroduce compromise. Before reuse, the organization should verify the integrity of images, templates, snapshots, and backups. For provider-managed services, the organization may have limited visibility into remediation of underlying components. Contracts and response procedures should define how the cloud provider communicates affected components, remediation actions, completion status, and any remaining risk.

Example Mitigating Controls

- Administrative Controls
  - **Define eradication and recovery handoff procedures.**

    Define eradication procedures and designate who may authorize eradication actions, declare eradication complete, and approve the transition to recovery. Define the sequence for preserving required evidence before rebuilding or terminating resources, approving remediation actions, verifying eradication, documenting residual risk, and transferring responsibility to recovery personnel. Define who may approve an exception when immediate action is necessary to protect safety or essential operations.
- Technical Controls
  - **Implement cross-domain remediation capabilities.**

    Deploy security technologies and enforcement mechanisms across OT and cloud environments to support remediation actions, such as removing malicious code, revoking compromised credentials, patching vulnerabilities, correcting misconfigurations, and validating system integrity. For cloud-hosted workloads, rebuilding resources from known-good baseline images may be faster and more reliable than attempting to clean a potentially compromised running instance. Capture any important forensic evidence before rebuilding or terminating a resource to protect important disk and memory state.
  - **Review and remediate identity and access configurations following incidents.**

    Evaluate user accounts, service accounts, privileged roles, and access policies across OT and cloud identity systems to identify and correct compromised credentials or excessive privileges. Confirm that access controls match approved baselines before concluding eradication activities.
  - **Conduct post-remediation threat hunting to increase confidence in eradication.**

    Following eradication activities, conduct targeted threat hunting to identify evidence of residual compromise and increase confidence that persistence mechanisms and exploited weaknesses have been removed.
- Cloud Provider Controls
  - **Confirm remediation of cloud infrastructure components.**

    Where a vulnerability or compromise affects cloud infrastructure components, inform affected customers when remediation is complete and identify the services and regions involved. Where remediation requires customer action, state what the customer must do and by when.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 17: Incident Response Management
- CRI Cloud Profile v2.0 [CRI 2024]
  - RS.MI-02
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Security Incident Management, E-Discovery, and Cloud Forensics (SEF)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.26: Response to information security incidents
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Incident Response (IR)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - RS.MI: Response Mitigation
  - RS.IM: Response Improvement

3.6 Recover (RC)

The Recover Function comprises two Categories:

- Incident Recovery Plan Execution (RC.RP)
- Incident Recovery Communication (RC.CO)

3.6.1 Incident Recovery Plan Execution (RC.RP)

RC.RP-01 *The recovery portion of the incident response plan is executed once initiated from the incident response process*

Potential Risks and Considerations

Recovery of cloud-supported OT should follow a defined sequence that accounts for dependencies across on-premises OT and cloud technologies. Before restoring dependent OT functions, the organization should ensure that required identity, connectivity, configuration, and data services are available and operating as expected. The organization should stage recovery activities and maintain local capabilities, degraded operating modes, or manual procedures until it validates cloud-supported functions.

Recovery execution should follow defined roles, decision authorities, and communication pathways among OT operators, cloud administrators, cloud providers, vendors, and other stakeholders. For architectures spanning multiple regions or cloud providers, these parties should coordinate restoration steps and operational handoffs. Without structured sequencing and defined coordination mechanisms, organizations risk delayed recovery, partial restoration of functionality, or reintroduced instability in OT environments.

Example Mitigating Controls

- Administrative Controls
  - **Define contractual and operational recovery coordination for cloud-supported OT environments.**

    Determine what the cloud provider commits to for recovery, including availability service-level terms, support response times, and incident notification and escalation terms. Many public cloud providers do not commit to restoring service by a defined time. Verify whether SLAs or agreements have recovery time commitments and document where no commitment exists. For customer-managed workloads and data, the organization should plan for its restoration responsibilities. For provider-managed components, restoration responsibilities and dependencies should be defined according to the service model and agreement. Define coordination, communication pathways, and dependency sequencing in internal recovery procedures.

- Technical Controls
  - **Implement recovery orchestration capabilities.**

    Deploy tools and processes that support sequenced restoration of OT systems and associated cloud technologies. Align recovery actions with predefined dependencies, authorization workflows, and validation checkpoints before returning systems to operational status. Maintain runbooks with step-by-step procedures for common failure scenarios in cloud-supported OT environments so that personnel can execute coordinated recovery consistently. Use provider-offered automation services to execute sequenced restoration steps. Automated recovery should preserve the same dependencies, approval gates, and operational validation as manual recovery.
  - **Validate recovery states across OT and cloud components.**

    Use monitoring and configuration validation mechanisms to confirm that restored systems meet approved baselines and operational readiness criteria before resuming full production operations.
- Cloud Provider Controls
  - **Document recovery commitments and capabilities.**

    Document commitments for service availability, support response times, and incident notification. Make this information available to customers. Describe recovery capabilities customers can configure and use, and disclose prerequisites, limitations, and customer responsibilities.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 17: Incident Response Management
- CRI Cloud Profile v2.0 [CRI 2024]
  - RC.RP-01
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Security Incident Management, E-Discovery, and Cloud Forensics (SEF)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.26: Response to information security incidents
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Contingency Planning (CP)
  - Incident Response (IR)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - RC.RP: Recovery Planning

RC.RP-02 *Recovery actions are selected, scoped, prioritized, and performed*

Potential Risks and Considerations

Recovery actions should be selected and prioritized by the OT functions they restore, not by where the supporting components are hosted. The organization should scope and prioritize actions based on operational criticality, safety, and defined recovery objectives.

Recovery plans should define when and how to transition to alternate operational states. These states may include redundant cloud deployments, failing over to on-premises backup systems, operating in degraded modes, or following manual control procedures. For each transition, the plans should define the triggers, approval authority, personnel, access privileges, connectivity, and backup resources needed. Capacity in an alternate region is not guaranteed at failover time. Plans that rely on region failover should account for pre-provisioned or reserved capacity, per-region service quota increases, and identity, network, and key management dependencies created in advance. Without clearly defined triggers, approval authorities, and execution resources, the organization may restore less critical services before essential functions or prolong operational disruption.

Example Mitigating Controls

- Administrative Controls
  - **Define and align recovery priorities across OT and cloud environments.**

    Establish and document a hierarchy of recovery priorities that spans on-premises OT systems and integrated cloud technologies. Ensure that RTOs, RPOs, and restoration sequencing reflect operational criticality, safety considerations, regulatory requirements, and service continuity needs. Where cloud technologies support OT functions, establish recovery objectives based on operational requirements and determine which restoration activities are the responsibility of the organization, the cloud provider, or an upstream provider.
  - **Establish centralized recovery coordination and decision authority.**

    Define a recovery governance structure that designates decision-makers, communication channels, status reporting expectations, and authority to approve transitions to alternate operational states during recovery execution. Ensure that internal OT, IT, and cloud teams operate under a unified recovery plan to prevent conflicting actions and to support dynamic reprioritization as conditions change.

- Technical Controls
  - **Implement recovery orchestration capabilities that align with defined priorities.**

    Deploy tools and processes that support coordinated restoration of OT and cloud components based on established recovery priorities. Validate dependencies, backup availability and integrity, required connectivity, and restoration sequencing before returning critical functions to service. Require human oversight to confirm that automated recovery actions align with approved prioritization guidelines and operational readiness criteria, and that they support safe restoration of OT functions.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 11: Data Recovery
  - 17: Incident Response Management
- CRI Cloud Profile v2.0 [CRI 2024]
  - RC.RP-02
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Security Incident Management, E-Discovery, and Cloud Forensics (SEF)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.26: Response to information security incidents
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Contingency Planning (CP)
  - Incident Response (IR)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - RC.RP: Recovery Planning

RC.RP-03 *The integrity of backups and other restoration assets is verified before using them for restoration*

Potential Risks and Considerations

The organization should verify the integrity of restoration assets before using them to recover OT environments. Backups, images, snapshots, configurations, and other restoration assets should be complete, authentic, usable, and free from detected corruption or malicious modification. These expectations apply whether the organization stores or restores these assets on-premises, in the cloud, or across environments.

Verification should address both technical integrity and operational usability. Technical checks may include comparing cryptographic hashes or signatures with trusted references, reviewing versions and configuration baselines, and checking for IOCs. Where possible, the organization should restore and test assets in an isolated environment that represents the recovery target. These activities can help prevent reintroducing vulnerabilities or untested configurations into OT environments.

Example Mitigating Controls

- Administrative Controls
  - **Define integrity verification requirements for backups and other restoration assets.**

    Establish requirements for verifying the integrity and authenticity of OT backups and other restoration assets before using them for restoration, regardless of where the organization stores the assets or where it restores them. Define approved validation methods, required evidence, documentation expectations, and approval authorities for restoration use. Where restoration assets are stored in cloud environments, ensure that storage and versioning practices preserve the information needed to support integrity validation.
- Technical Controls
  - **Implement automated integrity validation mechanisms for restoration assets.**

    Deploy tools and processes that verify the integrity of backups and restoration artifacts before using them. When the organization stores backups as accessible objects or files, verification can include hash comparison, version validation, and configuration baseline comparison. Direct inspection of cloud provider-managed recovery points depends on the backup service and resource type. Integrity assurance for these recovery points depends on cloud provider integrity checks and restore job status reporting, plus restoration and validation testing appropriate to the workload. Validation testing can confirm that restored OT applications start, configurations match approved baselines, and operational data is complete and consistent. Record and review verification results before restoration activities proceed.
  - **Perform periodic backup validation and restoration testing.**

    Conduct regular validation exercises to confirm that backups are complete, retrievable, and capable of supporting OT operations. Include restoration testing across target environments that each method supports, to verify operational readiness and functional suitability before an actual recovery event. Restore targets vary by backup service, workload, and architecture. Consider what changes to tools and processes will be necessary to manage backups of both cloud assets and on-premises assets. As part of validation exercises, verify that encryption keys used to protect backup data are available and

functional, as inaccessible keys can prevent restoration even when backup data is intact.

- Cloud Provider Controls
  - **Provide verification capabilities for managed recovery points.**

    Support restore testing to verify that managed recovery points can be restored, and report the results of backup and restore jobs. Identify the recovery point, time of verification, result, and any errors detected. Provide available information about the integrity and completeness of the recovery point. Document the scope and limitations of the verification so customers can assess the recovery point before using it for restoration.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 17: Incident Response Management
- CRI Cloud Profile v2.0 [CRI 2024]
  - RC.RP-03
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Security Incident Management, E-Discovery, and Cloud Forensics (SEF)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.26: Response to information security incidents
  - Control 8.13: Information backup
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Contingency Planning (CP)
  - Incident Response (IR)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - RC.RP: Recovery Planning

RC.RP-04 *Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms*

Potential Risks and Considerations

Post-incident operating norms for cloud-supported OT environments should reflect critical mission needs and the cybersecurity risk that remains during recovery. These norms may include degraded or manual operation, restricted functionality, temporary access limits, increased monitoring, or compensating controls. The organization should

document the approved operating conditions, remaining risk, decision authority, and criteria for revising or ending the interim conditions.

A cloud provider can restore its own service while dependent OT functions are unready for operation. Published service levels may describe availability over a measurement period. They generally do not commit the cloud provider to a specific restoration time, unless the agreement explicitly includes a recovery or restoration time commitment. The organization restores the resources it manages and validates data, integrations, connectivity, and OT functions. Until the organization completes this validation, post-incident operating norms should define how affected operations continue safely and reliably.

Example Mitigating Controls

- Administrative Controls
  - **Establish post-incident operational norms.**

    Define the operating conditions, limitations, compensating measures, and monitoring requirements that will apply during and after restoration. Base these decisions on critical mission functions and cybersecurity risk. Identify the authority responsible for approving interim operating conditions or changes to post-incident operating norms.
- Technical Controls
  - **Verify restoration to an approved operational state.**

    Use monitoring, configuration management, and performance analysis tools to verify that OT systems and integrated cloud technologies are operating within approved parameters following recovery. Use CSPM tools, cloud provider-native configuration monitoring, or equivalent capabilities to verify that security control baselines are reestablished across customer-managed cloud resources. Identify and address deviations from baseline configurations, expected control states, or performance thresholds before declaring full operational status.
  - **Apply heightened monitoring after recovery.**

    Following recovery declaration, maintain a defined period of enhanced monitoring to detect residual threats, recurring compromises, or operational instability before returning to standard monitoring thresholds and procedures.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 17: Incident Response Management
- CRI Cloud Profile v2.0 [CRI 2024]
  - RC.RP-04

- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Security Incident Management, E-Discovery, and Cloud Forensics (SEF)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.26: Response to information security incidents
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Contingency Planning (CP)
  - Incident Response (IR)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - RC.RP: Recovery Planning

RC.RP-05 *The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed*

Potential Risks and Considerations

The organization should verify the security, configuration, and performance of a restored cloud-supported OT system before returning it to service. Rapid re-provisioning does not replace this validation. The organization should check restored assets for known IOCs and persistence mechanisms. A clean scan does not prove that no compromise remains. The organization should also confirm that:

- Root causes and exploited paths are remediated
- Affected credentials and keys have been rotated or revoked
- Restored artifacts come from trusted baselines
- Configuration and integrity checks pass
- Heightened monitoring is operating.

Performance testing should confirm that restored systems meet latency, throughput, and response time requirements.

Example Mitigating Controls

- Administrative Controls
  - **Define validation requirements and decision authority for restoring assets to service.**

    Establish conditions that restored OT systems and integrated cloud components must meet before they are returned to normal operations. These conditions should address integrity validation, alignment with configuration

baselines, functional readiness, and documentation of validation results. Identify who holds the authority to approve return to service.

- Technical Controls
  - **Implement automated integrity and configuration validation mechanisms.**

    Deploy tools that perform integrity checks on restored data, system images, configurations, and application components. Validate that restored assets match approved baselines and that the organization has addressed vulnerabilities, unauthorized changes, or misconfigurations associated with the incident.
  - **Use representative test or staging environments to validate restored systems before production deployment.**

    Maintain controlled test or staging environments that reflect production OT and cloud-integrated environments. Use these environments to validate restoration actions, configuration states, and system functionality before reintroducing assets into operational environments.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 17: Incident Response Management
- CRI Cloud Profile v2.0 [CRI 2024]
  - RC.RP-05
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Security Incident Management, E-Discovery, and Cloud Forensics (SEF)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.26: Response to information security incidents
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Contingency Planning (CP)
  - Incident Response (IR)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - RC.RP: Recovery Planning

RC.RP-06 *The end of incident recovery is declared based on criteria, and incident-related documentation is completed*

Potential Risks and Considerations

The designated recovery authority should declare incident recovery complete only when predefined technical and operational criteria are met. Evidence should show that restored OT functions have reached the approved post-incident operating state, dependent cloud services are stable, and configuration baselines have been restored. Any remaining deviations, risks, or corrective actions should be formally accepted, assigned, and tracked. Cloud provider service status can support this decision but does not replace the organization's validation.

Before declaring recovery complete, the organization should complete the incident record. Documentation should capture the incident scope, response and recovery actions, key decisions, supporting evidence, validation activities, and lessons learned. Personnel responsible for OT operations, cybersecurity, and cloud administration should contribute information relevant to their roles. Lessons learned should inform updates to recovery plans, architectural decisions, and cybersecurity risk management practices. Inadequate documentation may hinder future incident analysis, weaken improvement efforts, or create compliance gaps.

Example Mitigating Controls

- Administrative Controls
  - **Define authority for declaring the end of recovery.**

    Define the authority that formally declares recovery complete. Require the authority to confirm that return-to-service decisions are complete, that the organization has addressed remaining interim conditions, and that it has completed incident documentation. Identify which stakeholders must concur, such as OT operations, cybersecurity, and cloud administration leads.
  - **Integrate cloud considerations into recovery documentation and after-action requirements.**

    Ensure that recovery documentation captures the activities affecting both OT systems and integrated cloud technologies. Require incident reports, RCA, validation results, and lessons learned. Incorporate improvements into response plans, recovery procedures, and risk management practices.
- Technical Controls
  - **Use incident tracking systems to manage recovery milestones and closure validation.**

    Deploy systems that track recovery actions, validation checkpoints, approval workflows, and documentation status across OT and cloud-supported

environments. Configure these systems so the organization cannot declare closure until it satisfies predefined criteria and documentation requirements.

- **Maintain auditable records of recovery validation and closure decisions.**

  Implement mechanisms to record validation results, stakeholder approvals, corrective action status, and formal recovery closure decisions. Retain records in accordance with regulatory and organizational requirements.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 17: Incident Response Management
- CRI Cloud Profile v2.0 [CRI 2024]
  - RC.RP-06
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Security Incident Management, E-Discovery, and Cloud Forensics (SEF)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.26: Response to information security incidents
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Contingency Planning (CP)
  - Incident Response (IR)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - RC.RP: Recovery Planning

3.6.2 Incident Recovery Communication (RC.CO)

RC.CO-03 *Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders*

Potential Risks and Considerations

Recovery communications should give designated stakeholders timely and accurate information about restoration progress and operational readiness across OT systems and cloud technologies. Updates should identify which functions have been restored and validated, which remain degraded, and which constraints remain. Information for operators and system owners should state whether transition from manual or degraded operation has been authorized and identify the fallback approach if a restored function becomes unstable. Cloud provider service status can inform these updates but does not replace the organization’s assessment of end-to-end operational readiness.

Recovery communication processes should define approval authorities, recipients, communication channels, update frequency, and required content. The organization should coordinate messages with cloud providers or other third parties while meeting applicable regulatory, contractual, and information-handling requirements. Pre-approved templates for common recovery milestones can reduce communication delays and errors under the time pressure of an active incident. Without structured and tested communication processes, the organization may face delays, stakeholder confusion, or noncompliance with regulatory requirements.

Example Mitigating Controls

- Administrative Controls
  - **Define recovery communication requirements for cloud-supported OT environments.**

    Define requirements for providing recovery status updates to designated stakeholders. Specify the approval authorities, required content, recipients, secure communication channels, and timing expectations. Ensure that these requirements align with regulatory, contractual, and information-sharing obligations.
  - **Incorporate cloud-service dependencies into recovery communication planning.**

    Ensure that recovery communication planning addresses the status of OT systems and supporting cloud technologies. Define how the organization incorporates service status information from cloud providers and other suppliers into its recovery updates. Identify which status sources the organization will use and how current each one is.
- Technical Controls
  - **Implement secure and auditable notification mechanisms for communicating recovery status.**

    Use communication and incident management platforms that support controlled distribution of recovery updates to authorized stakeholders, including out-of-band communication channels that remain available if primary cloud or IT systems are compromised or degraded. Configure systems to provide timely notifications of validated recovery milestones and remaining operational constraints while maintaining role-based access controls and records of distributed communications.
- Cloud Provider Controls
  - **Provide recovery status information.**

    Provide recovery and service restoration status information. Identify the affected services, affected regions, and current state of affected services. Provide this information programmatically as well as through a console and state the applicable handling restrictions.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 17: Incident Response Management
- CRI Cloud Profile v2.0 [CRI 2024]
  - RC.CO-03
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Security Incident Management, E-Discovery, and Cloud Forensics (SEF)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.5: Contact with authorities
  - Control 5.26: Response to information security incidents
- MITRE ATT&CK for ICS v19.2 [MITRE 2026]
  - M0810: Out-of-Band Communications Channel
- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Contingency Planning (CP)
  - Incident Response (IR)
  - Supply Chain Risk Management (SR)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - RC.CO: Recovery Communications

RC.CO-04 *Public updates on incident recovery are shared using approved methods and messaging*

Potential Risks and Considerations

Public updates on recovering from incidents affecting cloud-supported OT environments should use approved communication processes and designated spokespersons. The organization remains responsible for the accuracy, timing, and content of its statements, even when recovery activities involve cloud providers or other third parties. Public statements should distinguish confirmed facts from estimates or unknowns and provide the information needed to understand service impacts, recovery progress, remaining constraints, and any protective actions. They should not disclose sensitive details about OT architecture, cloud dependencies, vulnerabilities, or recovery methods that could increase risk. Without structured approval processes and coordinated messaging, the organization may issue inconsistent or incomplete statements that may create confusion, erode public trust, or expose sensitive operational information.

Example Mitigating Controls

- Administrative Controls
  - **Define governance and approval requirements for public recovery communication.**

    Define requirements for issuing public updates related to incident recovery, including approval authorities, required content, communication channels, and applicable regulatory or contractual considerations. Where recovery involves cloud providers or other third parties, define coordination expectations that support consistent and accurate messaging. Governance requirements should address applicable disclosure obligations and restrictions, including limits on information that may be publicly disclosed during or after incidents that affect energy infrastructure.
  - **Develop and maintain approved public messaging guidance and templates.**

    Create and periodically update public communication guidance and templates for incident scenarios involving cloud-supported OT environments. Guidance and templates support clearly communicating recovery status, service impacts, and restoration progress while protecting sensitive operational and security information.
- Technical Controls
  - **Implement controlled and auditable public communication mechanisms.**

    Use approved communication platforms that enforce role-based authorization, content review workflows, and record retention for public updates. Ensure that all public statements related to recovery are traceable to documented approvals and align with established messaging protocols.

Informative References

- CIS Critical Security Controls v8.1 [CIS 2024]
  - 17: Incident Response Management
- CRI Cloud Profile v2.0 [CRI 2024]
  - RC.CO-04
- CSA Cloud Controls Matrix v4.1 [CSA 2026]
  - Security Incident Management, E-Discovery, and Cloud Forensics (SEF)
- ISO/IEC 27017:2026 [ISO/IEC 2026]
  - Control 5.6: Contact with special interest groups
  - Control 5.26: Response to information security incidents

- NIST SP 800-53 Rev. 5 [NIST 2025]
  - Contingency Planning (CP)
  - Incident Response (IR)
  - Supply Chain Risk Management (SR)
- NIST SP 800-82 Rev. 3 [Stouffer 2023]
  - RC.CO: Recovery Communications

APPENDIX A: FUTURE CONSIDERATIONS

Cloud technology and operational technology (OT) are both mature technology domains, but they evolve at different rates. OT environments prioritize safety, reliability, and asset life. As a result, OT environments, particularly in the energy sector [Christopher 2024], often change more slowly than enterprise IT environments. Cloud technology evolves more rapidly and can speed adoption of emerging capabilities, such as artificial intelligence (AI), advanced analytics, automation, and edge computing.

This difference in pace does not make cloud technology unsuitable for OT use cases. However, it does mean that organizations should account for future change when they plan for cloud integration. Architecture decisions, security controls, contracts, governance processes, and operational procedures should support secure adoption today while allowing the organization to adapt as technology, threats, and business needs evolve. The following technology and architecture trends may influence current planning, and organizations should monitor them over time to help keep security and resilience controls aligned with changing conditions.

- ***Quantum Computing*** As quantum computing advances, organizations may need to adopt quantum-resistant technologies to protect cryptographic systems and their supporting technologies. This transition could affect cloud-supported OT environments, particularly capabilities that rely on cryptography, such as remote access, device identity, firmware signing, secure data exchange, and the protection of long-lived sensitive information. NIST finalized its initial post-quantum cryptography standards in 2024 [NIST 2024b, 2024c, 2024d], and major cloud providers have begun publishing adoption timelines. In draft guidance, NIST's proposed transition timeline would begin deprecating 112-bit-strength quantum-vulnerable public-key algorithms after 2030 and disallow quantum-vulnerable public-key algorithms after 2035 [Moody 2024]. Other organizations often use these dates as planning reference points. Many OT assets have long service lives, limited maintenance windows, and constrained compute resources. These factors can make a cryptographic transition difficult, especially when OT assets depend on vendor-qualified firmware, older protocols, fixed certificate formats, or devices that cannot support the larger key sizes, larger signature sizes, or additional compute overhead that post-quantum algorithms may require. Early planning can help organizations avoid rushed changes later.
- ***AI-Assisted Operational Decision Support and Control*** Cloud-enabled analytics, AI, automation, digital twins, and simulation environments may increasingly support or influence OT operational decisions. Examples include grid balancing, pipeline pressure monitoring, alarm prioritization, outage management, and predictive maintenance. These environments can test operating strategies, validate models, train operators, and shape automated recommendations, even

when they do not directly control field assets. These capabilities increasingly include agentic AI systems, which can plan and execute multi-step tasks with limited human intervention. As these recommendations or automated actions become more closely tied to operational decisions, they can affect safety, reliability, and operator situational awareness. Planning should address factors such as decision authority, operator override, fail-safe behavior, data quality, AI explainability, and accountability for functions that influence OT operations. The NIST AI Risk Management Framework provides guidance for governing and managing AI-specific risks [Tabassi 2023].

- ***Alternative and Non-Terrestrial Connectivity*** Organizations may use alternative connectivity services, including Low Earth orbit (LEO) satellite services, private wireless networks, microwave links, or carrier-managed wireless services, to support primary, secondary, or emergency connectivity for remote OT assets. These OT assets may include substations, pipeline facilities, field sensors, generation sites, and emergency operations. Compared with traditional wired terrestrial communications, these connectivity services may have different latency, availability, failover, and restoration characteristics. Planning should account for provider dependencies, communications resilience, routing and failover behavior, encryption and key management, remote device and terminal management, and supply chain risk for provider-managed components and services. This consideration may be most relevant for remote assets, restoration scenarios, and areas with limited terrestrial service.
- ***Automated Cloud Management and Orchestration*** Automated cloud management tools, increasingly enhanced by AI, may change how organizations manage identity, configuration, monitoring, detection, response, and policy enforcement. These tools may reduce manual work and speed routine tasks, but they may also make changes faster than existing OT governance processes can review them. Automated changes, whether made directly by management tools or deployed through continuous integration and continuous delivery (CI/CD) pipelines, can affect historian systems, remote access paths, engineering workflows, and data flows to control centers. Planning should define guardrails, approval thresholds, rollback procedures, change windows, and validation steps for automated actions that may affect OT functions.
- ***Edge-Cloud Convergence*** Cloud-native software may move closer to field assets and OT networks. Examples include containerized analytics, protocol brokers, device management agents, local applications, and edge gateways. These workloads may sit near controllers, protection relays, sensors, actuators, and other operational assets. A compromised or misconfigured edge workload may affect data quality, operator awareness, remote access, or control enablement. Planning should focus on data flows, workload identity, trust boundaries, local survivability,

segmentation, and safety constraints rather than relying only on the distinction between “on-premises” and “cloud” services.

- ***Zero Trust Architecture Adoption*** Zero trust principles are increasingly being adapted for use in OT environments. The limitations of perimeter-based security models and the expansion of remote access, cloud integration, and third-party connectivity in operational environments drive this shift. These principles reduce the reliance on implicit network-based trust by requiring explicit authentication and authorization and by using identity, device, resource, and contextual information to make and reevaluate access decisions. For cloud-connected OT environments, this verification affects how organizations design remote access, engineering workstation connectivity, historian access, and inter-zone communications. As cloud providers mature capabilities that can support zero trust architectures, organizations should evaluate how those capabilities can be incorporated into architectures that integrate cloud with OT while preserving required segmentation, safety, latency, and availability controls. Planning should address identity and access management for OT users and devices, network segmentation, policy enforcement points, and how zero trust controls interact with existing OT security zones defined under frameworks such as IEC 62443 [ISA/IEC 2026].

These considerations do not require organizations to predict every future architecture. They support a more durable planning approach. Organizations can improve their long-term resilience by identifying assumptions, tracking dependencies, assigning ownership for emerging risks, and reviewing controls as cloud-supported OT use cases mature. As vendor capabilities, cloud provider offerings, and regulatory expectations evolve, this approach helps organizations adopt cloud capabilities while preserving the safety, reliability, and resilience priorities of OT environments.

APPENDIX B: GLOSSARY

Term	Definition
agentic artificial intelligence	Artificial intelligence systems capable of planning and executing multi-step tasks towards a goal with limited human intervention.
application programming interface (API)	A system access point or library function that has a well-defined syntax and is accessible from application programs or user code to provide well-defined functionality. Definition from the NIST glossary
cloud access security broker (CASB)	A security tool that can be placed in between users and cloud services to manage traffic and enforce rules related to visibility, asset discovery, data privacy, regulatory compliance, data protection, and threat detection. In addition to being placed in between users and cloud services, modern CASBs can also operate through API integrations, analysis of traffic logs/cloud discovery, reverse/forward proxy paths, or combinations. Microsoft Defender for Cloud Apps, for example, uses app connectors, Cloud Discovery and proxy access. Definition adapted from Microsoft
cloud infrastructure entitlement management (CIEM)	Provides visibility into who or what has access to specific resources. It analyzes permissions, helps identify excessive or unused access, and supports remediation. CIEM also helps organizations to monitor and manage permissions across multiple cloud environments, including Azure, AWS, and GCP. Definition adapted from Microsoft
cloud workload protection platform (CWPP)	A platform that provides a series of protections across cloud environments in an organization connected to physical servers, serverless functions, VMs, and containers. CWPPs can help automate detection and remediation of threats, vulnerabilities, and errors within any of the above infrastructures, supporting the workloads that interact with cloud environments. Definition adapted from Microsoft
container	A method for packaging and securely running an application within an application virtualization environment. Also known as an application container or a server application container. Definition from NIST SP 800-190

Term	Definition
cybersecurity architecture	A structured view of cybersecurity capabilities and their alignment with the organization's enterprise architecture.
data residency	The physical or geographic location where an organization stores and processes its data. Definition from Oracle
data security posture management (DSPM)	A cybersecurity technology that identifies sensitive data across multiple cloud environments and services, assessing its vulnerability to security threats and risk of regulatory non-compliance. Definition from IBM
data sovereignty	The legal and regulatory requirements that apply to data based on the jurisdictions with authority over the data, the organization, or the service provider. Definition from Oracle
DevSecOps	DevSecOps, which is short for development, security and operations, is an application development practice that can help automate the integration of security and security practices at every phase of the software development lifecycle, from initial design through integration, testing, delivery and deployment. Definition from IBM
extended detection and response (XDR)	A platform that delivers security incident detection and automated response capabilities for security infrastructure. XDR integrates threat intelligence and telemetry data from multiple sources with security analytics to provide contextualization and correlation of security alerts. Definition from Gartner
hosting infrastructure	The hardware, software, networking, storage, and other infrastructure used to host a cloud service. The infrastructure may be operated by the cloud service provider or by one or more upstream infrastructure providers. Definition adapted from AWS
identity and access management (IAM)	Broadly refers to the administration of human and non-human identities and their access to on-premises systems, cloud environments, and cloud-hosted applications. Definition adapted from the NIST glossary

Term	Definition
industrial control system	General term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems, and other control system configurations that are often found in the industrial sectors and critical infrastructures, such as programmable logic controllers. An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy). Definition from NIST SP 800-82r3
information technology	A discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. In the context of this publication, the definition includes interconnected or interdependent business and technology systems and the environment in which they operate. Definition from the Electricity Subsector Cybersecurity Risk Management Process
infrastructure-as-a-service (IaaS)	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls). Definition from the NIST glossary
machine image	A machine image is like a bootable blueprint for a virtual machine. The image typically contains the static state of the chosen operating system, apps, and system configuration, in a ready-to-load format. Definition adapted from AWS
on-premises	Hardware and software deployed in organization-controlled facilities.
operational data	Data used or generated by an industrial process. Examples include configuration parameters, event logs, equipment telemetry, system alerts, historian data, and predictive maintenance data.

Term	Definition
operational technology	A broad range of programmable systems and devices that interact with the physical environment or manage devices that interact with the physical environment. These systems and devices detect or cause a direct change through the monitoring and control of devices, processes, and events. Examples include industrial control systems, building automation systems, transportation systems, physical access control systems, physical environment monitoring systems, and physical environment measurement systems. Definition from NIST SP 800-82r3
platform-as-a-service (PaaS)	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. Definition from the NIST glossary
policy-as-code (PaC)	Policy-as-code is the practice of defining decision logic programmatically. With this approach, policies for security, compliance, audits and monitoring are defined using a general purpose, domain-specific, or markup programming language. Definition from Splunk
privileged access management (PAM)	Strategies and tools to protect privileged identities by securing administrative credentials, limiting privileged access to approved users, granting elevated permissions only when needed, automating credential-related tasks, and monitoring privileged activity for security and compliance purposes. Definition from Fortinet
provider-offered	Capabilities directly integrated by cloud providers into their cloud technology offerings.
recovery point objective (RPO)	The point in time to which data must be recovered after an outage. Definition from the NIST glossary
recovery time objective (RTO)	The overall length of time an information system's components can be in the recovery phase before negatively impacting the organization's mission or mission/business processes. Definition from the NIST glossary

Term	Definition
security orchestration, automation, and response (SOAR)	A SOAR solution combines incident response, orchestration and automation, and threat intelligence management capabilities in a single platform. SOAR tools are also used to document and implement processes (such as playbooks, workflows, procedures or processes); support security incident management; and apply machine-based assistance to human security analysts and operators. Definition adapted from Gartner
serverless	A method of abstracting servers away from the user. Operational management falls to the cloud service provider, including handling physical machines and VM provisioning. Scaling and resource provisioning for computing, storage, or networking can be performed manually or configured to automatically adjust based on application demand. Definition adapted from Cloud Native Glossary
service-level agreement (SLA)	A document addressing important commitments between a customer and provider. Examples include technical performance promises, how disputes are to be handled, and any remedies for performance failures. Definition adapted from NIST SP 800-146
shared responsibility model	A delineation of who is responsible for what in regard to a cloud environment. This responsibility matrix varies depending on the cloud provider, service model, and deployment model. Definition adapted from CSA
software-as-a-service (SaaS)	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. Definition from the NIST glossary

Term	Definition
software bill of materials (SBOM)	A formal record containing the details and supply chain relationships of various components used in building software. Software developers and vendors often create products by assembling existing open source and commercial software components. The SBOM enumerates these components in a product. Definition from the NIST glossary
tenant	One or more cloud service users sharing access to a set of physical and virtual resources. Definition from ISO/IEC 22123-1:2023
Trusted Execution Environment (TEE)	A segregated area or enclave, such as an area of memory and CPU, that is protected from the rest of the environment. Definition adapted from Microsoft
user and entity behavior analytics (UEBA)	A type of security software that uses behavioral analytics, machine learning algorithms and automation to identify abnormal and potentially dangerous behavior of users and other entities, including hosts, applications, IP addresses, accounts or services. Definition adapted from IBM
virtual machine	The emulation of a physical computer running its own operating system and apps with virtualized resources. Definition adapted from Azure
virtual private cloud (VPC)	A logically isolated virtual network within a cloud environment. Definition from VMware
zero trust	A collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. Definition from the NIST glossary

APPENDIX C: LIST OF ABBREVIATIONS

AC	Access Control
A&A	Audit and Assurance
AAL	authentication assurance level
ABAC	attribute-based access control
AI	artificial intelligence
AIS	Application & Interface Security
API	application programming interface
AT	Awareness and Training
AU	Audit and Accountability
AWS	Amazon Web Services
BCR	Business Continuity Management and Operational Resilience
CA	Assessment, Authorization, and Monitoring
CASB	cloud access security broker
CCC	Change Control and Configuration Management
CEK	Cryptography, Encryption & Key Management
CESER	DOE Office of Cybersecurity, Energy Security, and Emergency Response
CI/CD	continuous integration and continuous delivery
CIEM	cloud infrastructure entitlement management
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
CM	Configuration Management
CP	Contingency Planning
CRI	Cyber Risk Institute
CSA	Cloud Security Alliance

CSF	NIST Cybersecurity Framework
CSPM	cloud security posture management
CWPP	cloud workload protection platform
DCS	Datacenter Security
DDoS	distributed denial of service
DevSecOps	development, security, and operations
DMZ	demilitarized zone
DNS	domain name system
DOE	United States Department of Energy
DSP	Data Security and Privacy Lifecycle Management
DSPM	data security posture management
ERM	enterprise risk management
ESD	Emergency Shutdown
FAL	federation assurance level
FIM	file integrity monitoring
GCP	Google Cloud Platform
GRC	Governance, Risk and Compliance
HRS	Human Resources
IA	Identification and Authentication
IaaS	infrastructure-as-a-service
IaC	infrastructure-as-code
IAL	identity assurance level
IAM	identity and access management
ICS	industrial control system
IDaaS	identity-as-a-service

IdP	identity provider
IEC	International Electrotechnical Commission
IOC	indicator of compromise
IP	internet protocol
IPY	Interoperability & Portability
IR	Incident Response
ISA	International Society of Automation
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
IT	information technology
I&S	Infrastructure Security
JIT	just-in-time
KPI	key performance indicator
KRI	key risk indicator
LEO	Low Earth orbit
LOG	Logging and Monitoring
MA	Maintenance
MFA	multifactor authentication
MP	Media Protection
NACL	network access control list
NDR	Network Detection and Response
NERC CIP	North American Electric Reliability Corporation Critical Infrastructure Protection
NIST	National Institute of Standards and Technology
NLR	National Laboratory of the Rockies

OCSF	Open Cybersecurity Schema Framework
OT	operational technology
PaaS	platform-as-a-service
PaC	policy-as-code
PAM	privileged access management
PE	Physical and Environmental Protection
PL	Planning
PM	Program Management
PS	Personnel Security
PT	Personally Identifiable Information Processing and Transparency
RA	Risk Assessment
RBAC	role-based access control
RCA	root cause analysis
RPO	recovery point objective
RTO	recovery time objective
SA	System and Services Acquisition
SaaS	software-as-a-service
SBOM	software bill of materials
SC	System and Communication Protection
SCA	software composition analysis
SCADA	supervisory control and data acquisition
SCRM	supply chain risk management
SCuBA	Secure Cloud Business Applications
SDLC	software development lifecycle
SEF	Security Incident Management, E-Discovery, and Cloud Forensics

SI	System and Information Integrity
SIEM	security information and event management
SLA	service-level agreement
SME	subject matter expert
SOAR	security orchestration, automation, and response
SOC	System and Organization Controls
SR	Supply Chain Risk Management
SSH	secure shell
SSO	single sign-on
STA	Supply Chain Management, Transparency, and Accountability
STIX	Structured Threat Information eXpression
TAXII	Trusted Automated Exchange of Intelligence Information
TEE	Trusted Execution Environment
TLP	traffic light protocol
TSA	Transportation Security Administration
TTP	tactics, techniques, and procedures
TVM	Threat and Vulnerability Management
UEBA	user and entity behavior analytics
UEM	Universal Endpoint Management
VM	virtual machine
VPC	virtual private cloud
WORM	write-once, read-many
XDR	extended detection and response

APPENDIX D: REFERENCES

[AICPA & CIMA 2026]
American Institute of CPAs® (AICPA) and Chartered Institute of Management Accountants® (CIMA). System and Organization Controls: SOC Suite of Services. *AICPA & CIMA Website*. June 30, 2026 [accessed]. https://www.aicpa-cima.com/resources/landing/system-and-organization-controls-soc-suite-of-services

[AWS 2026a]
Amazon Web Services (AWS). AWS Well-Architected. *AWS Website*. June 30, 2026 [accessed]. https://aws.amazon.com/architecture/well-architected/

[CESER 2026]
United States Department of Energy (DOE). *CESER Strategic Plan Fiscal Years 2026 to 2030*. DOE Office of Cybersecurity, Energy Security, and Emergency Response. February 2026. https://www.energy.gov/documents/ceser-strategic-plan2026-2030

[Christopher 2024]
Christopher, J. D. *SANS 2024 State of ICS/OT Cybersecurity*. SANS Institute. October 2024. https://sansorg.egnyte.com/dl/oq4USL3qoA

[CIS 2024]
Center for Internet Security (CIS). *CIS Critical Security Controls Version 8.1*. Center for Internet Security. June 2024. https://www.cisecurity.org/controls/v8-1

[CIS 2026]
Center for Internet Security (CIS). *CIS Benchmarks*. Center for Internet Security. September 28, 2026 [accessed]. https://www.cisecurity.org/cis-benchmarks

[CISA 2026]
Cybersecurity and Infrastructure Security Agency (CISA). Secure Cloud Business Applications (SCuBA) Project. *CISA Website*. June 30, 2026 [accessed]. https://www.cisa.gov/resources-tools/services/secure-cloud-business-applications-scuba-project

[CRI 2024]
Cyber Risk Institute (CRI). *The Cloud Profile v2.0*. Cyber Risk Institute. July 17, 2024. https://cyberriskinstitute.org/cloud-profile/

[CSA 2026]
Cloud Security Alliance® (CSA). CSA Cloud Controls Matrix v4.1. CSA Website. January 27, 2026. https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4-1

[FIRST 2022]
Forum of Incident Response and Security Teams, Inc. (FIRST). *TRAFFIC LIGHT PROTOCOL (TLP) FIRST Standards Definitions and Usage Guidance — Version 2.0*. August 2022. https://www.first.org/tlp/docs/tlp-letter.pdf

[Google 2025]
Google Office of the CISO. *Security Guidance for Cloud-Enabled Hybrid Operational Technology Networks*. Google. 2025. https://services.google.com/fh/files/misc/ot_security_blueprint_ociso2025.pdf

[IEC 2013]
International Electrotechnical Commission (IEC). Industrial Communication Networks—Network and System Security—Part 3-3: System Security Requirements and Security Levels. IEC 62443-3-3. August 7, 2013. https://webstore.iec.ch/en/publication/7033

[IEC 2018]
International Electrotechnical Commission (IEC). *Security for Industrial Automation and Control Systems—Part 4-1: Secure Product Development Lifecycle Requirements*. IEC 62443-4-1. January 15, 2018. https://webstore.iec.ch/en/publication/33615

[ISO/IEC 2022]
International Organization for Standardization and International Electrotechnical Commission (ISO/IEC). Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements. ISO/IEC 27001:2022. ISO. 2022. https://www.iso.org/standard/27001

[ISO/IEC 2026]
International Organization for Standardization and International Electrotechnical Commission (ISO/IEC). *Information security, cybersecurity and privacy protection — Information security controls based on ISO/IEC 27002 for cloud services*. ISO/IEC 27017:2026. ISO. July 2026. https://www.iso.org/standard/27017

[ISA/IEC 2026]
International Society of Automation and International Electrotechnical Commission (ISA/IEC). ISA/IEC 62443 Series of Standards. *ISA Website*. June 30, 2026 [accessed]. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

[Johnson 2016]
Johnson, C. et al. *Guide to Cyber Threat Information Sharing*. NIST SP 800-150. October 2016. https://csrc.nist.gov/pubs/sp/800/150/final

[Microsoft 2026]
Microsoft Corporation. Azure Well-Architected Framework. *Microsoft Learn Website*. June 30, 2026 [accessed]. https://learn.microsoft.com/en-us/azure/well-architected/

[MITRE 2026]
The MITRE Corporation. MITRE ATT&CK® for ICS Version 19.2. *MITRE ATT&CK® Website*. August 6, 2026. https://attack.mitre.org/matrices/ics/

[NIST 2012]
National Institute of Standards and Technology (NIST). *Guide for Conducting Risk Assessments*. NIST SP 800-30 Rev. 1. September 2012. https://csrc.nist.gov/pubs/sp/800/30/r1/final

[NIST 2022]
National Institute of Standards and Technology (NIST). *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities*. NIST SP 800-218. February 2022. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf

[NIST 2024a]
National Institute of Standards and Technology (NIST). *The NIST Cybersecurity Framework (CSF) 2.0*. NIST CSWP 29. NIST. February 26, 2024. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[NIST 2024b]
National Institute of Standards and Technology (NIST). *Module-Lattice-Based Key-Encapsulation Mechanism Standard*. FIPS 203. August 13, 2024. https://csrc.nist.gov/pubs/fips/203/final

[NIST 2024c]
National Institute of Standards and Technology (NIST). *Module-Lattice-Based Digital Signature Standard. FIPS 204*. August 13, 2024. https://csrc.nist.gov/pubs/fips/204/final

[NIST 2024d]
National Institute of Standards and Technology (NIST). *Stateless Hash-Based Digital Signature Standard. FIPS 205*. August 13, 2024. https://csrc.nist.gov/pubs/fips/205/final

[NIST 2025]
National Institute of Standards and Technology (NIST). *Security and Privacy Controls for Information Systems and Organizations*. NIST SP 800-53 Rev. 5, Release 5.2.0. August 27, 2025. https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_A_5_2_0/home

[Nelson 2025]
Nelson, A. et al. *Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile*. NIST SP 800-61 Rev. 3. April 2025. https://csrc.nist.gov/pubs/sp/800/61/r3/final

[NERC 2019]
North American Electric Reliability Corporation. *CIP-008-6 - Cyber Security — Incident Reporting and Response Planning.* February 7, 2019 [adopted by NERC Board of Trustees]. https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-008-6.pdf

[Moody 2024]
Moody, D. et al. *Transition to Post-Quantum Cryptography Standards*. NIST IR 8547 ipd. National Institute of Standards and Technology. November 2024. https://doi.org/10.6028/NIST.IR.8547.ipd

[Stouffer 2023]
Stouffer, K. et al. *Guide to Operational Technology (OT) Security*. NIST SP 800-82 Rev. 3. September 2023. https://csrc.nist.gov/pubs/sp/800/82/r3/final

[Tabassi 2023]
Tabassi, E. *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. NIST AI 100-1. January 2023. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

[Temoshok 2025a]
Temoshok, D. et al. *Digital Identity Guidelines: Identity Proofing and Enrollment*. NIST SP 800-63A-4. July 2025. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63A-4.pdf

[Temoshok 2025b]
Temoshok, D. et al. *Digital Identity Guidelines: Authentication and Authenticator Management*. NIST SP 800-63B-4. July 2025. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63B-4.pdf

[Temoshok 2025c]
Temoshok, D. et al. *Digital Identity Guidelines: Federation and Assertions*. NIST SP 800-63C-4. July 2025. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63C-4.pdf

[TSA 2026]
Transportation Security Administration. *Security Directive (SD) Pipeline-2021-01 Series: Enhancing Pipeline Cybersecurity*. January 9, 2026. https://www.tsa.gov/sites/default/files/signed_security-directive-pipeline-2021-01g-and-transmittal-memo_508c.pdf

[Wallace 2024]
Wallace, A. et al. *CloudZero Phase 2 Technical Report*. NREL/TP-5R00-88566. National Laboratory of the Rockies (NLR). May 2024.
https://research-hub.nlr.gov/en/publications/cloudzero-phase-2-technical-report/

APPENDIX E: BIBLIOGRAPHY

This section contains additional sources related to cloud integration in OT environments. These sources are not directly referenced in the Profile but may provide useful context for readers. The sources were reviewed as part of the literature review conducted before the Profile was developed.

[AGA 2020]
American Gas Association (AGA). *Cloud Service Considerations for Migrating Industrial Control Systems*. AGA. October 2020. https://www.aga.org/wp-content/uploads/2023/10/ICS-Cloud-Considerations.pdf

[Alghofaili 2021]
Alghofaili, Y. et al. Secure Cloud Infrastructure: A Survey on Issues, Current Solutions, and Open Challenges. *Applied Sciences*. Volume 11. Issue 19. September 27, 2021. Page 9005. https://doi.org/10.3390/app11199005

[AWS 2021a]
Amazon Web Services (AWS). *Security Best Practices for Manufacturing OT*. AWS. May 20, 2021. https://d1.awsstatic.com/whitepapers/security-bp-for-manufacturing-ot.pdf

[AWS 2021b]
Amazon Web Services (AWS). *AWS User Guide to Support Compliance with North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards*. AWS. November 2021. https://d1.awsstatic.com/whitepapers/Security/aws-support-compliance-nerc-cip-standards.pdf

[AWS 2024]
Amazon Web Services (AWS). *Security Pillar-AWS Well-Architected Framework*. AWS. November 6, 2024. https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/welcome.html

[AWS 2026b]
Amazon Web Services (AWS). AWS Security Maturity Model v2. *AWS Maturity Model Website*. June 30, 2026 [accessed]. https://maturitymodel.security.aws.dev/en/

[Bella 2022]
Bella, H. K. & Vasundra, S. A Study of Security Threats and Attacks in Cloud Computing. Pages 658-666. In *2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT)*. February 25, 2022. https://doi.org/10.1109/ICSSIT53264.2022.9716317

[CISA 2023]
Cybersecurity and Infrastructure Security Agency (CISA). *Secure Cloud Business Applications (SCuBA): Technical Reference Architecture*. CISA. September 2024 [accessed]. https://www.cisa.gov/resources-tools/services/technical-reference-architecture-tra

[CISA 2024]
Cybersecurity and Infrastructure Security Agency (CISA). *Secure Cloud Business Applications (SCuBA) Hybrid Identity Solutions Guidance*. CISA. March 2024. https://www.cisa.gov/sites/default/files/2024-03/Final-02262024-CSSO-SCUBA-508c.pdf

[Currie 2023]
Currie, R. et al. Data Privacy for the Grid: Toward a Data Privacy Standard for Inverter-Based and Distributed Energy Resources. *IEEE Power and Energy Magazine*. Volume 21. Issue 5. September/October 2023. Pages 48–57. https://doi.org/10.1109/MPE.2023.3288595

[Darwish 2024]
Darwish, D. *Emerging Trends in Cloud Computing Analytics, Scalability, and Service Models*. IGI Global. January 2024. https://www.igi-global.com/book/emerging-trends-cloud-computing-analytics/325078

[Doshi 2020]
Doshi, R. & Kute, V. A Review Paper on Security Concerns in Cloud Computing and Proposed Security Models. Pages 1-4. In *2020 International Conference on Emerging Trends in Information Technology and Engineering (Ic-ETITE)*. April 27, 2020. https://ieeexplore.ieee.org/document/9077910

[Dsouza 2021]
Dsouza, R. Ten Security Golden Rules for Industrial IoT Solutions [blog post]. *The Internet of Things on AWS – Official Blog*. September 7, 2021. https://aws.amazon.com/blogs/iot/ten-security-golden-rules-for-industrial-iot-solutions/

[Gunduz 2020]
Gunduz, M. & Das, R. Cyber-Security on Smart Grid: Threats and Potential Solutions. Computer Networks. Volume 169. March Issue. March 14, 2020. Page 107094. https://www.sciencedirect.com/science/article/pii/S1389128619311235

[Jelacic 2017]
Jelacic, B. et al. STRIDE to a Secure Smart Grid in a Hybrid Cloud. *Computer Security*. Volume 10683. December 22, 2017. Pages 77-90. https://link.springer.com/chapter/10.1007/978-3-319-72817-9_6

[Jelacic 2020]
Jelacic, B. et al. Security Risk Assessment-Based Cloud Migration Methodology for Smart Grid OT Services. *Acta Polytechnica Hungarica*. Volume 17. Issue 5. January 2020. Pages 113–34. https://doi.org/10.12700/APH.17.5.2020.5.6

[Kumar 2023]
Kumar, S. et al. Comprehensive Analysis of Cloud Security: Issues & Challenges. Pages 622-627. In *2023 6th International Conference on Contemporary Computing and Informatics (IC3I)*. September 14, 2023. https://doi.org/10.1109/IC3I59117.2023.10398097

[Lambropoulos 2021]
Lambropoulos, G. et al. A Review on Cloud Computing Services, Concerns, and Security Risk Awareness in the Context of Digital Transformation. Pages 1-6. In *2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)*. October 18, 2021. https://ieeexplore.ieee.org/document/9566267

[Luna 2015]
Luna, J. et al. Leveraging the Potential of Cloud Security Service-Level Agreements through Standards. *IEEE Cloud Computing*. Volume 2. Issue 3. July 15, 2015. Pages 32–40. https://doi.org/10.1109/MCC.2015.52

[Mell 2011]
Mell, P. & Grance, T. The NIST Definition of Cloud Computing. NIST SP 800-145. NIST. September 2011. https://csrc.nist.gov/pubs/sp/800/145/final

[NERC 2023]
North American Electric Reliability Corporation (NERC). *BES Operations in the Cloud*. NERC. September 2023.
https://www.nerc.com/globalassets/our-work/white-papers/sites_whitepaper_bes_ops_in_cloud.pdf

[NSA 2020]
National Security Agency (NSA). *Mitigating Cloud Vulnerabilities*. NSA. January 22, 2020.
https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF

[OCD 2021]
OWL Cyber Defense (OCD). Best Practices for OT-to-Cloud Connectivity [blog post]. *Owl Cyber Defense Website*. August 9, 2021.
https://owlcyberdefense.com/blog/best-practices-for-ot-to-cloud-connectivity/

[Pendleton 2024]
Pendleton, J. et al. Cloud Reassurance: A Framework to Enhance Resilience and Trust. Carnegie Endowment for International Peace. January 18, 2024.
https://carnegieendowment.org/research/2024/01/cloud-reassurance-a-framework-to-enhance-resilience-and-trust

[Pericherla 2023]
Pericherla, S. S. Cloud Computing Threats, Vulnerabilities and Countermeasures: A State-of-the-Art. The ISC International Journal of Information Security. Volume 15. Issue 1. January 1, 2023. Pages 1–58. https://doi.org/10.22042/isecure.2022.312328.718

[Singh 2023]
Singh, V. & Kaushik, V. Navigating the Landscape of Security Threat Analysis in Cloud Computing Environments. In *Security and Risk Analysis for Intelligent Cloud Computing*. Kumar, A. et al. [editors] CRC Press. Page 25. 2023. https://doi.org/10.1201/9781003329947

[Tunc 2017]
Tunc, C. et al. Cloud Security Automation Framework. Pages 307-312. In *IEEE 2nd International Workshops on Foundations and Applications of Self* Systems (FAS*W)*. October 12, 2017. https://ieeexplore.ieee.org/document/8064140

[Wali 2022]
Wali, A. Analysis of Security Challenges in Cloud-Based SCADA Systems: A Survey. *TechRxiv* [preprint]. July 14, 2022. https://doi.org/10.36227/techrxiv.20291835.v1

APPENDIX F: ACKNOWLEDGEMENTS

The Energy Sector Cloud Cybersecurity Profile was developed through a collaborative effort between public- and private-sector organizations and was sponsored by the United States Department of Energy (DOE). The DOE thanks the organizations and individuals who provided their expert knowledge, evaluations, and recommendations in support of this effort.

Program Lead

Fowad Muneer
Office of Cybersecurity, Energy Security, and Emergency Response (CESER)
United States Department of Energy

Energy Industry Contributors

David Batz, Edison Electric Institute
Chris Butler, Duke Energy
Paul Carroll, American Public Power Association
Richard Condello, American Public Power Association
Jay Cribb, Southern Company
Kimberly Denbow, American Gas Association
Mike Deniset, TC Energy
Bobby Ellis, Columbia Power and Water Systems
Lew Folkerth, ReliabilityFirst
Brian Foster, Southern California Edison
Mike Fu, TC Energy
Kegan Gerard, Southern California Edison
Chris Goddard, Duke Energy
T.J. Gore, CenterPoint Energy
Martin Heavey, Eversource Energy
Chandler Holgate, American Gas Association
Liz Holland, Duke Energy
Jonathan Homer, CPS Energy
Frank Honkus, Electricity Information Sharing and Analysis Center
Thomas Jacobus, Southern California Edison
Monica Jain, Southern California Edison
Melanie Jocelyn, Southern California Edison
Johnny Mann, CPS Energy
Carter Manucy, National Rural Electric Cooperative Association
Kristine Martz, Edison Electric Institute
George McCauley, CPS Energy
Robby McCutcheon, Kerrville Public Utility Board
Adrian McNamara, American Public Power Association
Robert Mims, Southern Company
Jonathan Mora, Duke Energy
Anil Nair, CPS Energy
Ryan Newlon, National Rural Electric Cooperative Association
Colton Patrick, Omaha Public Power District
Laura Ritter, Duke Energy
Mike Sanders, Southern Company
Moin Shaikh, Long Island Power Authority
Jason Shea, Southern California Edison
William Souza, Duke Energy
Michael Tetto, Eversource Energy
Anil Thomas, CenterPoint Energy
K. Malaika Walton, GridWise Alliance
Karen Wayland, GridWise Alliance

Vendor and Service Provider Contributors

Emily Beam, Cyber Risk Institute
Sheila Casserly, Schneider Electric
Chris Cornillie, Google Cloud
Nikola Dalcekovic, Schneider Electric
Denyette DePierro, Amazon Web Services
Vinod D'Souza, Google Cloud
Patricia Ephraim Eke, Microsoft
Mikhail Falkovich, Microsoft
Aly Farooqui, IBM
Paul Forney, Schneider Electric
John Goodman, Cyber Risk Institute
Sri Gourisetti, Google Cloud
Hanna Grene, Microsoft
Lindsey Hale, Amazon Web Services
Hila Hanif, Amazon Web Services
Kristine Harper, Amazon Web Services
Mike Hoover, IPKeys Cyber Partners
Bilal Khursheed, Microsoft
David Kliemann, IBM
Matt Linton, Google Cloud
Pat Lo, Microsoft
Josh Magri, Cyber Risk Institute
Brianne Miller, Microsoft
Samara Moore, Amazon Web Services
Thomas Nicholson, Amazon Web Services
David Nickles, Amazon Web Services
Nick Panos, Google Cloud
Alex Perry, Google Cloud
Maggy Powell, Amazon Web Services
Eileen Sciarra, Cloud Security Alliance
Jordana Siegel, Amazon Web Services
Chris Sistrunk, Mandiant
Raiford Smith, Google Cloud
Soo Stahl, Microsoft
Craig Sundstrom, Amazon Web Services

Government Contributors

James Briones, DOE
Fowad Muneer, DOE

Program Team

Zackery Adams, Idaho National Laboratory
Sivasathya Pradha Balamurugan, The National Laboratory of the Rockies
Brian Benestelli, Axio
Robert Biestman, The National Laboratory of the Rockies
Rich Caralli, Axio
Tim Coleman, The National Laboratory of the Rockies
Zoe Dormuth, The National Laboratory of the Rockies
Cory Faust, Axio
Tricia Flinn, Software Engineering Institute
John Fry, Axio
Cliff Glantz, Pacific Northwest National Laboratory
Adarsh Hasandka, The National Laboratory of the Rockies
Jordan Henry, The National Laboratory of the Rockies
Dan Kambic, Software Engineering Institute
Lindsay Kishter, Nexight Group
Daniel Komnick, Software Engineering Institute
Maurice Martin, The National Laboratory of the Rockies
Julia Morgan, Idaho National Laboratory
Shaun O'Leary, Pacific Northwest National Laboratory
Jennifer Peters, Nexight Group
Jordan Peterson, The National Laboratory of the Rockies
Alexander Petrilli, Software Engineering Institute
David Rager, The National Laboratory of the Rockies
Emma Stewart, Idaho National Laboratory
Anthony Wallace, The National Laboratory of the Rockies
David White, Axio