



e-MANAGEMENT

e-Government Solutions. Delivered.

Certified SBA 8(a) woman-owned, minority-owned small business

Corporate Headquarters:

1010 Wayne Avenue, Suite 1150
Silver Spring, Maryland 20910
301.565.2988 Telephone
301.565.2995 Facsimile
www.e-mcinc.com

e-Management - Proprietary Information

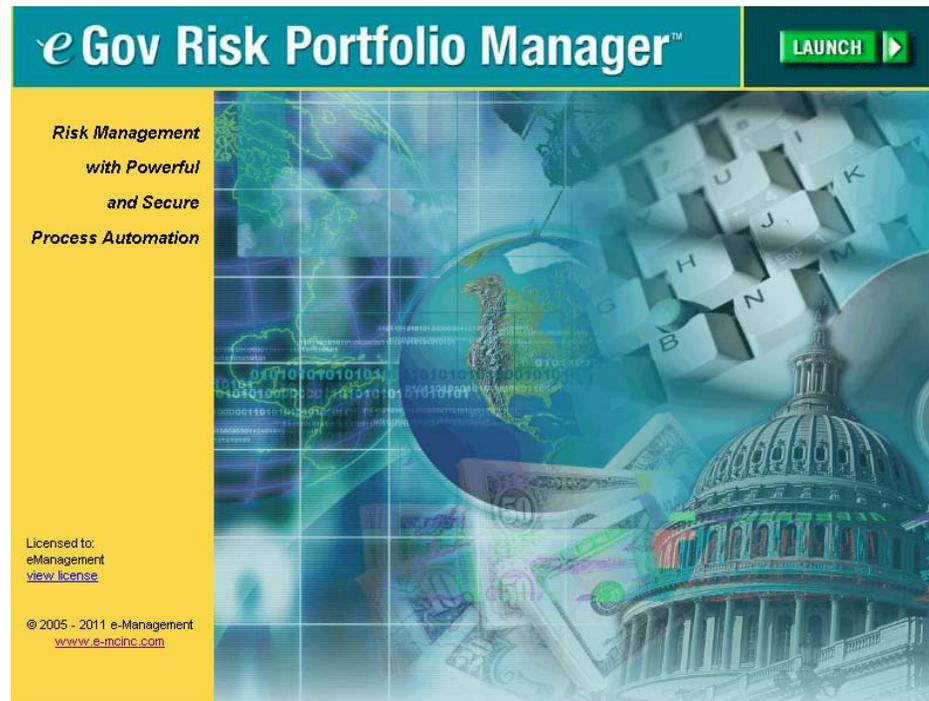
Risk Management:

Overview of e-Gov Risk Portfolio Manager™ (e-Gov RPM™) V4 for Under Secretary of Energy

March 2011

Today's Agenda

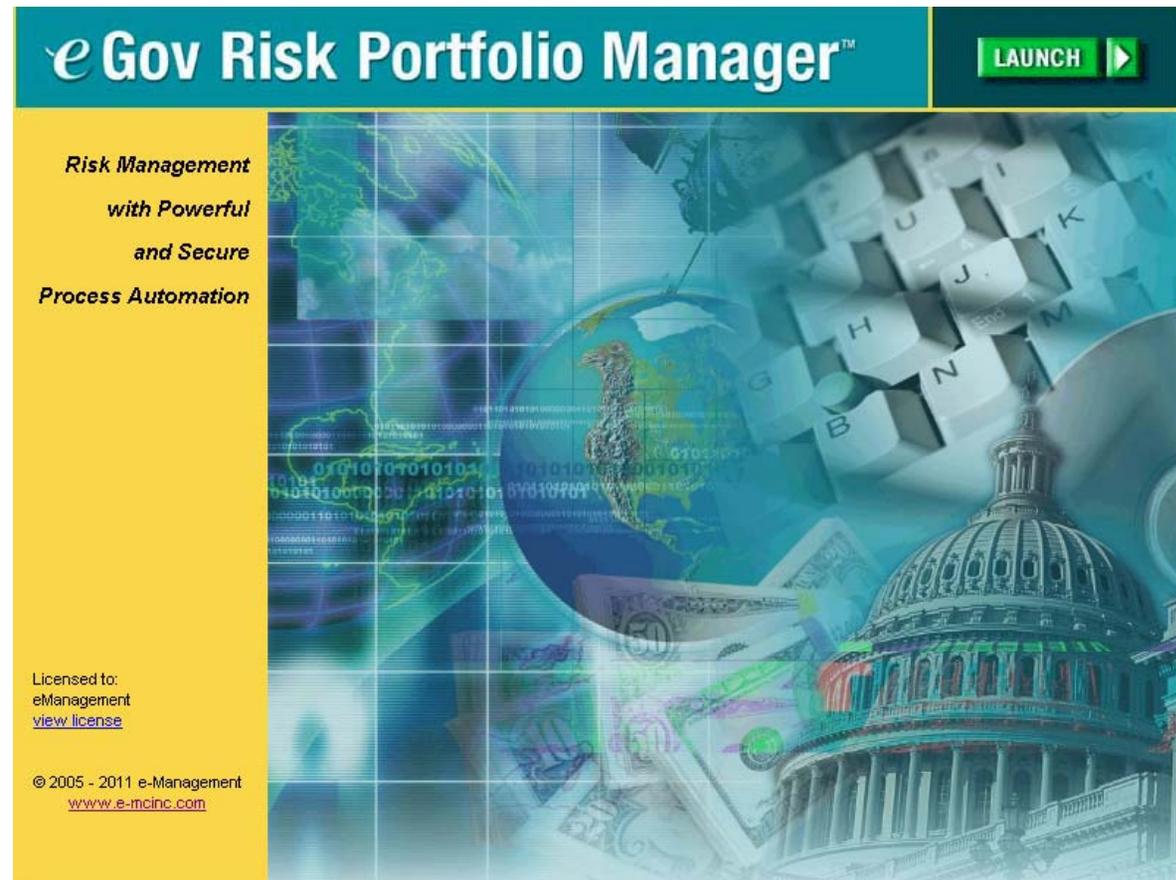
- 1) eGov RPM and use at DOE EM
- 2) Overview of the capabilities of eGov RPM™
- 3) eGov RPM supports the Under Secretary of Energy's Program Cyber Security Plan (PCSP)



e-Gov Risk Portfolio Manager is a multi-user, web based tool used for continuous monitoring

Why use an automated tool for continuous monitoring?

- Consistent data capture
- Central repository to store data and information accessible via the Web
- Ease of reporting for management and auditors
- Automated control inheritance and control tailoring
- Makes the process easier



DOE EM and the Office of the Under Secretary of Energy Working Together

- Through collaboration, DOE EM and the Under Secretary of Energy have worked together to assess the Office of the Under Secretary of Energy's Continuous Monitoring requirements against eGov RPM capabilities
- EM has shared their implementation experiences, their resources, their lessons learned and their instance of eGov RPM with the Office of the Under Secretary team helping to maximize DOE's technology investments

Slide 4

r4

insert DOE logo on the headerline

ragleyd, 3/17/2011

eGov RPM use at DOE EM

- DOE EM has been using eGov RPM to support cyber security and risk management
- At EM eGov RPM
 - Supports and makes the continuous monitoring effort easier and more efficient
 - Is the Central repository for data and artifacts
 - Reduces expenses during audits by providing auditors read only access to authorized portfolios
 - Enables an enterprise view of risks to allow management to focus on critical risks for better use of resources and funding

Key Features of eGov RPM

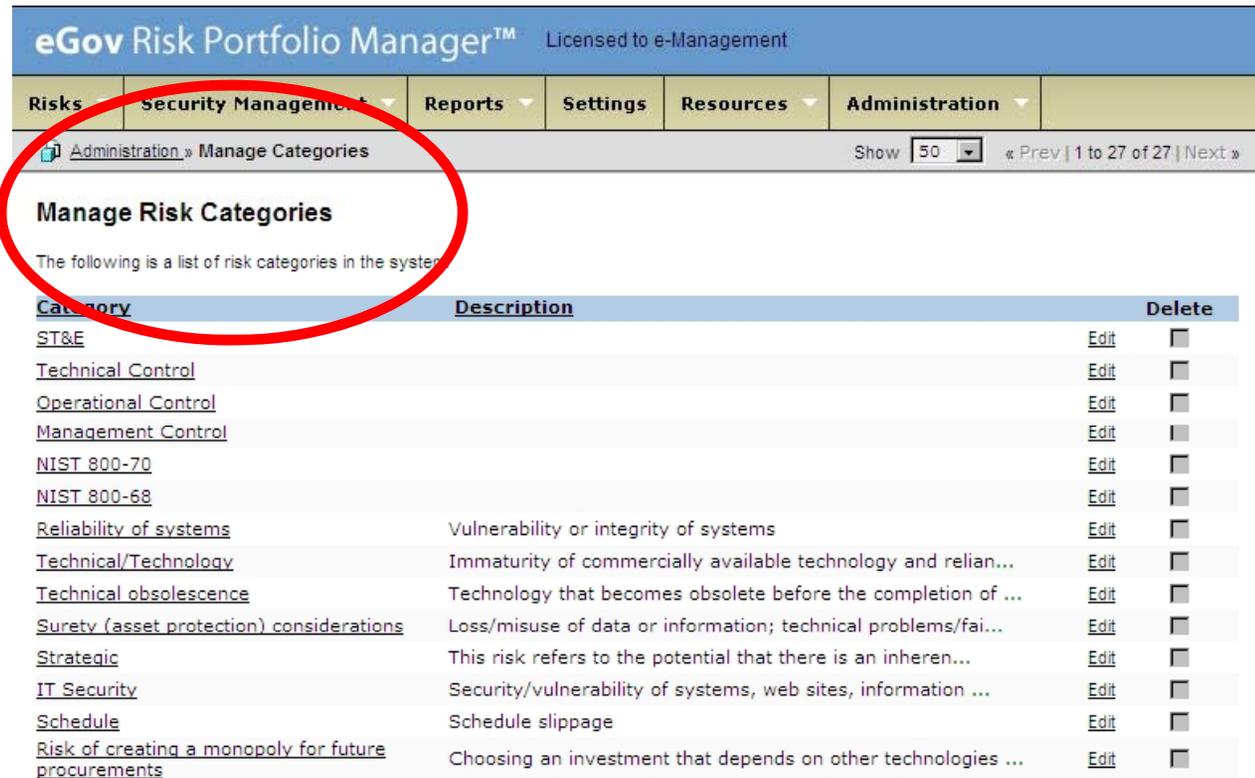
- Continuous Monitoring and tracking
 - System Security Plan
 - Risk Management
 - POA&M Management
 - Secure partitioned data views
 - CyberScope compatible exports
 - Multi-level control baseline inheritance and control tailoring
 - Tool pre-populated with NIST controls
- eGov RPM has been aligned with the Under Secretary of Energy's PCSP
- Customized reports that facilitate and support continuous monitoring Strategies

e-Gov RPM™ groups assets into **portfolios** which can represent accreditation boundaries, organizations, programs, or projects

The screenshot displays the eGov Risk Portfolio Manager interface. The top navigation bar includes 'Risk', 'Security Management', 'Reports', 'Settings', 'Resources', and 'Administration'. The main content area is divided into two panes. The left pane, titled 'Portfolios and Projects', shows a tree view with a red circle around the 'Under Secretary of Energy' folder and its sub-items: 'Environmental Management (EM)', 'Electricity Delivery and Energy Relia', 'Energy Efficiency and Renewable En', 'Fossil Energy (FE)', 'Legacy Management (LM)', and 'Nuclear Energy (NE)'. The right pane, titled 'Risk Repository: Under Secretary of Energy', shows a search bar, a 'Show 50' dropdown, and pagination controls. Below this, there are filters for 'View by: Risks' and 'Status: Open', along with a checkbox for 'List all risks for Under Secretary of E children'. A blue banner indicates 'No risks found for Under Secretary of Energy.' and a 'New' button is visible. A blue box with an arrow points to the tree view, containing the text: 'Groupings of assets meaningful to your organization are recorded and centrally managed by the tool'. The footer includes '©2005-2011 e-Management, Inc. All Rights Reserved Worldwide'.

Grouping risks by risk category

e-Gov RPM comes out of the box with a standard set of risk categories and also allow the organizations to add their own custom categories for tracking risks



The screenshot displays the eGov Risk Portfolio Manager interface. The navigation bar includes 'Risks', 'Security Management', 'Reports', 'Settings', 'Resources', and 'Administration'. The 'Administration' menu is expanded, showing 'Administration » Manage Categories' which is circled in red. Below this, the page title is 'Manage Risk Categories' and it states 'The following is a list of risk categories in the system'. A table lists various risk categories with their descriptions and edit/delete options.

Category	Description	Delete
ST&E		Edit <input type="checkbox"/>
Technical Control		Edit <input type="checkbox"/>
Operational Control		Edit <input type="checkbox"/>
Management Control		Edit <input type="checkbox"/>
NIST 800-70		Edit <input type="checkbox"/>
NIST 800-68		Edit <input type="checkbox"/>
Reliability of systems	Vulnerability or integrity of systems	Edit <input type="checkbox"/>
Technical/Technology	Immaturity of commercially available technology and relian...	Edit <input type="checkbox"/>
Technical obsolescence	Technology that becomes obsolete before the completion of ...	Edit <input type="checkbox"/>
Surety (asset protection) considerations	Loss/misuse of data or information; technical problems/fai...	Edit <input type="checkbox"/>
Strategic	This risk refers to the potential that there is an inheren...	Edit <input type="checkbox"/>
IT Security	Security/vulnerability of systems, web sites, information ...	Edit <input type="checkbox"/>
Schedule	Schedule slippage	Edit <input type="checkbox"/>
Risk of creating a monopoly for future procurements	Choosing an investment that depends on other technologies ...	Edit <input type="checkbox"/>

eGov RPM Key Risk Features

- Risks can be associated with NIST controls or defined **custom controls**
- Users can track and report on **residual risks**
- An **executive dashboard** of the organization's overall risk posture is available
- A **Derivative Classifier Review** function is available for reviewing aggregated data that together represent potentially sensitive information (Mosaic Effect)

- **Sources**, such as OMB Memoranda, DOE directives, GAO reports, or Audit reports can be used to identify risk details
- **Source ID numbers**, such as section numbers from standards or policies, can be associated with each risk
- **Assessor** roles can be customized
- **URLs** to other web sites containing additional risk information can be associated to each risk

eGov RPM supports the Under Secretary of Energy's PCSP

- Records the organizational impact level
- Categorizes the information system
- Enables a user with the proper permissions to select/tailor the baseline of security controls to include the CAG
- Helps the user implement the security controls
- Assesses security controls
- Authorizes the information system
- Monitors security controls
- Continuously monitor risks

Records the organizational impact level

The screenshot displays the eGov Risk Portfolio Manager interface. The top navigation bar includes 'Risks', 'Security Management', 'Reports', 'Settings', 'Resources', and 'Administration'. The current path is 'Security Management > Security Plan > System Identification'. A left sidebar shows a tree view under 'Moderate Impact' with categories like 'Environmental Management (E)', 'Field Site', 'Business Systems', 'DMZ', 'Electricity Delivery and Energy', 'Energy Efficiency and Renewab', 'Fossil Energy (FE)', 'Legacy Management (LM)', and 'Nuclear Energy (NE)'. A central dropdown menu is open, listing documents such as 'Organizational Impact', 'Authority to Operate', 'COOP & Contingency Plan', 'Certification Letter', 'Security Assessment', 'Privacy Impact Assessment', 'Configuration Management', 'Incident Response Plan', 'Contingency Plan', 'Other Supporting Documents', and 'Download All'. A 'Save Baseline' button and a date field set to '2/31/2011' are also visible. A blue-bordered callout box on the right contains the text: 'Document repository for this off-line process'. Below the dropdown, a text box states: 'The formal name for this Accreditation Boundary is Business System. It has been assigned to this boundary.'

Categorizes Information System

The screenshot displays the eGov Risk Portfolio Manager interface. The top navigation bar includes 'Risks', 'Security Management', 'Reports', 'Settings', 'Resources', and 'Administration'. The 'Security Management' dropdown menu is open, showing options such as 'Security Plan', 'SP 800-53A', 'SP 800-60', 'POA&M Summary', 'System Level POA&M', 'Program Level POA&M', 'Edit Classes', 'Edit Families', 'Edit Controls', and 'Manage Baselines'. A mouse cursor is hovering over 'SP 800-60'. The background shows a tree view of information systems and a list of categories like 'Controls and Oversight', 'Regulatory Development', 'Planning and Budgeting', etc.

The eGov RPM tool comes pre-populated with the NIST 800-60 data categorization publication

Enables a user with the proper permissions to select the applicable security controls

The screenshot displays the 'eGov Risk Portfolio Manager' interface. The main navigation bar includes 'Risks', 'Security Management', 'Reports', 'Settings', 'Resources', and 'Administration'. The current page is 'System Identification' under 'Security Management'. A left sidebar shows a tree view of organizational units, with 'Business Systems' selected. Below this is a 'FIPS 199 Impact Assessment' section with a grid of checkboxes for 'Low', 'Mod', and 'High' impact levels. The main content area has tabs for 'SYSTEM IDENTIFICATION', 'MANAGEMENT CONTROLS', 'OPERATIONAL CONTROLS', 'TECHNICAL CONTROLS', and 'ORG SPECIFIC'. The 'SYSTEM IDENTIFICATION' tab is active, showing fields for 'Expected Completion Date' (12/31/2011) and 'DAA Approval Date' (10/05/2009). A dropdown menu for 'Inherited Baseline' is open, showing options: '-- NONE --', '-- NONE -- Business Systems Controls', and 'Field Site'. A text box below describes the system name: 'Business Systems'. At the bottom, there is a table for 'Information System Owner' with columns for Name, Title, Agency, Address, E-mail, and Phone.

Name	Title	Agency	Address	E-mail	Phone
1 User Name	Chief Information	Field Site	Field Site	user@email.com	888-555-1212
2 User Name	Cyber Security Mi	Field Site	Field Site	user@email.com	888-555-1212
3 User Name	ISSM	Field Site	Field Site	user@email.com	888-555-1212
4 User Name	ISSO	Field Site	Field Site	user@email.com	888-555-1212

Multi-level control baseline inheritance and control tailoring

Enables a user with the proper permissions to select/tailor the baseline of security controls to include the CAG

eGov Risk Portfolio Manager™ Licensed to e-Management

Risks Security Management Reports Settings Resources Administration

Security Plan » System Identification » Tailoring Controls

Tailoring Controls

Reset to Default

Control Code	Control Name	Inh.	Low	Mod	High	Other	CAG	Enabled	Edit	Enhancement
AC-1	ACCESS CONTROL POLICY AND PROCEDURES		✓	✓	✓	✗	✓	✓		
AC-10	CONCURRENT SESSION CONTROL		✗	✗	✓	✗	✗	✗		
AC-11	SESSION LOCK		✗	✓	✓	✗	✗	✗		
AC-12			✗	✗	✗	✗	✗	✗		
AC-13			✗	✗	✗	✗	✗	✗		
AC-14			✓	✓	✓	✗	✗	✓		
AC-15			✗	✗	✗	✗	✗	✗		
AC-16			✗	✗	✗	✗	✗	✗		
AC-17			✓	✓	✓	✗	✓	✓		
AC-18			✓	✓	✓	✗	✓	✓		
AC-19			✓	✓	✓	✗	✓	✓		
AC-2			✓	✓	✓	✗	✓	✓		

Multi-level control baseline inheritance and control tailoring (cont'd)

Helps the user implement the security controls

eGov Risk Portfolio Manager™ Licensed to e-Management

Search : Find Advanced S

Risks Security Management Reports Settings Resources Administration

March 17, 2011 Logged in a

Security Management > Security Plan > Management Controls

Moderate Impact

CNTL CONTROL NAME

- PM-6 INFORMATION SECURITY MEASURES OF PERFORMANCE
- PM-7 ENTERPRISE ARCHITECTURE
- PM-8 CRITICAL INFRASTRUCTURE PLAN
- PM-9 RISK MANAGEMENT STRATEGY
- PM-10 SECURITY AUTHORIZATION PROCESS
- PM-11 MISSION/BUSINESS PROCESS DEFINITION
- RA-1 RISK ASSESSMENT POLICY AND PROCEDURES
- RA-2 SECURITY CATEGORIZATION
- RA-3 RISK ASSESSMENT
- RA-5 VULNERABILITY SCANNING
- SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES
- SA-2 ALLOCATION OF RESOURCES
- SA-3 LIFE CYCLE SUPPORT
- SA-4 ACQUISITIONS
- SA-5 INFORMATION SYSTEM DOCUMENTATION

SYSTEM IDENTIFICATION MANAGEMENT CONTROLS OPERATIONAL CONTROLS TECHNICAL CONTROLS ORG SPECIFIC

Control Menu Print Save

Type in keyword(s) separated by a space Search Ar

Authorized to Edit Business Systems

RA-5 VULNERABILITY SCANNING

Control

This control is in place. Using the vendor named tool and/or other standard techniques, the Field Site ISSO scans for SANS Top 20 vulnerabilities in the Field Site Business Systems boundary on a regular basis.

Original 800-53 text: The organization scans for vulnerabilities in the information system [Assignment: organization-defined frequency] or when significant new vulnerabilities potentially affecting the system are identified and reported.

Priority Code P1 - Implement P1 security controls first

Deviation None Equivalency Exception

Justification

Approver

Associated Risk --Select--

Deviation Status --Select-- Action Date

Level of Effectiveness

- Level-1 Control Objective Documented in a Security Plan
- Level-2 Security Control Documented as Procedure
- Level-3 Procedures have been Implemented
- Level-4 Procedures and Security Controls have been Implemented
- Level-5 Procedures & Controls are fully integrated into a Comprehensive Program

Supplemental Guidance The security categorization of the information system guides the frequency and comprehensiveness of the vulnerability scans.

Show Page : 1 2 3

Pre-populated with NIST 800-53 controls

- Control Enhancement
- Organization Policy
- Technology Control Mapping
- Documented Risk

Helps the user implement the security controls (cont'd)

The screenshot displays the eGov Risk Portfolio Manager interface. The top navigation bar includes 'Risks', 'Security Management', 'Reports', 'Settings', 'Resources', and 'Administration'. The main content area is titled 'Moderate Impact' and shows a list of controls on the left and a detailed configuration form on the right. The control being viewed is 'MMP-1' with the name 'MSMP-5 MEDIA TRANSPORT ENERGY PCSP: DAT-50, DAT-55, DAT-75'. The configuration form includes fields for 'Control' (with a text area containing the control description), 'Priority Code', 'Deviation' (with radio buttons for None, Equivalency, and Exception), 'Justification', 'Approver', 'Associated Risk', 'Deviation Status', 'Level of Effectiveness' (with radio buttons for Level-1 through Level-5), and 'Supplemental Guidance'. A red '1' is visible in the 'Level of Effectiveness' section.

You can supplement NIST's controls with controls specific to your environment

Assesses security controls

eGov Risk Portfolio Manager™ Licensed to e-Management

Risks Security Management Reports Settings Resources Administration

Security Plan » System Identification » Tailoring Controls

Tailoring Controls

Reset to Default

Control Code	Control Name	Inh.	Low	Mod	High	Other	CAG	Enabled	Edit	Enhancement
AC-1	ACCESS CONTROL POLICY AND PROCEDURES		✓	✓	✓	✗	✓	✓		
AC-10	CONCURRENT SESSION CONTROL		✗	✗	✓	✗	✗	✗		
AC-11	SESSION LOCK		✗	✓	✓	✗	✗	✗		
AC-12	SESSION TERMINATION		✗	✗	✗	✗	✗	✗		
AC-13	SUPERVISION AND REVIEW ? ACCESS CONTROL									
AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION									
AC-15	AUTOMATED MARKING									
AC-16	SECURITY ATTRIBUTES									
AC-17	REMOTE ACCESS									
AC-18	WIRELESS ACCESS									
AC-19	ACCESS CONTROL FOR MOBILE DEVICES									
AC-2	ACCOUNT MANAGEMENT									

Mission adjusted baseline

- Identification of System Administration
- System Administration, Networking, and Security Institute (SANS) Consensus Audit Guidelines (CAG)

Authorizes the Information System

The screenshot displays the eGov Risk Portfolio Manager interface. The top navigation bar includes 'Risks', 'Security Management', 'Reports', 'Settings', 'Resources', and 'Administration'. The left sidebar shows a tree view of portfolios and projects, with 'Business Systems' selected. The main content area shows the 'Risk Profile' for 'AC-06 Local System Administrator Rights' with a Risk ID of 8883. The profile details include a description, a category of 'Technical Control', and a source of 'Internal'. The 'Mitigation Plan Required' checkbox is checked, and the 'Plan of Action Required' checkbox is also checked. The 'Assessed by' field is populated with 'EM-72 M1'.

Risk Profile: AC-06 Local System Administrator Rights Risk Id: 8883

Name: AC-06 Local System Administrator Rights

Description: In some cases user requirements to install software mandate individuals have administrative rights to their systems. Nefari could use these systems to launch an attack on the internal r includes some systems and information that requires addition protection. Users with administrator or root access can downlo install software including hacker tools, override security contro opt out of other protective measures. Mitigation: Field Site us security controls to restrict administrative rights when applicat

Category: Technical Control

Mitigation Plan Required

Risk Acceptable

Plan of Action Required

Source: Internal **Assessed by:** EM-72 M1

Source ID: **Entry Date:**

Capture data for reporting as well as artifacts that result from offline processes

- POA&M
- Security Authorization Package (off-line)
- Risk Determination
- Risk Acceptance

Monitors Security Controls

The screenshot displays a web-based risk management application. On the left, a navigation pane titled 'Portfolios and Projects' shows a tree structure under 'Under Secretary of Energy', including 'Environmental Management (EM)', 'Field Site', 'Business Systems', 'DMZ', 'Electricity Delivery and Energy Reliability (OE)', 'Energy Efficiency and Renewable Energy (EE)', 'Fossil Energy (FE)', 'Legacy Management (LM)', and 'Nuclear Energy (NE)'. Below this is an 'Actions' section with icons for 'New', 'Edit', and 'Delete', along with 'Expand All' and 'Collapse All' links.

The main content area shows the breadcrumb path: 'Risks » Risk Repository: Business Systems » Risk Item: AC-06 Local System Administrator Rights » Mitigation Plan'. Below this, the 'Portfolio Name' is 'Business Systems'. The 'Risk Profile' is 'AC-06 Local System Administrator Rights' and the 'Risk Id' is '8883'. There are four tabs: 'Risk Item', 'Mitigation Plan' (selected), 'Plan of Action and Milestones', and 'Audit Trail'.

The 'Mitigation Action' section contains the text: 'Remove administrative rights from all systems.' Below this is a dropdown menu with 'ABC' selected. The 'Mitigation Results' section contains the text: 'Some users require administrative rights to perform'. Below this is another dropdown menu with 'ABC' selected.

The 'After Mitigation is Applied' section has two checked checkboxes: 'Leftover residual risk remains' and 'New residual risks have'. The 'Responsible' field is 'Daniel Bright', 'Due Date' is '04/1', and 'Status' is 'Underway'. The 'Closed Date' field is empty.

The 'Security Control' section has two columns: 'Management' and 'Operational'. Below these are two empty boxes. At the bottom, there are sections for 'Consensus Audit Guidelines' and 'PCSP', each with expand/collapse icons.

On-going security control assessment, remediation, termination, and acceptance using the risk management system

Monitors Security Controls (cont'd)

Level of Effectiveness

2

Supplemental Guidance

Organization Policy

Technology Control Mapping

Level-1 Control Objective Documented in a Security Policy

Level-2 Security Control Documented as Procedure

List of Risks -- Webpage Dialog

https://www.e-govrpm.com/RPM4/show_documented... Certificate Error

30	CM-6 Configuration Settings	<input type="checkbox"/>
31	IR-04 - Losing a laptop with SUI or worse	<input type="checkbox"/>
32	Electronic devices	<input type="checkbox"/>
33	PL-05 Publish PIAs in new format.	<input type="checkbox"/>
34	AC-06 Local System Administrator Rights	<input type="checkbox"/>
35	IA-07 - Unauthorized disclosure of PII	<input type="checkbox"/>
36	SI - 03 Malicious Code	<input type="checkbox"/>
37	SI-04 - External Attacks	<input type="checkbox"/>
38	SI-04 - Internal Scans or Exploits	<input type="checkbox"/>
39	AC-17 Remote Access	<input type="checkbox"/>
40	SI-03 Malicious code through P2P	<input type="checkbox"/>
41	IA-06 Clear Text Passwords	<input type="checkbox"/>
42	AT-02 Staff Awareness	<input type="checkbox"/>
43	IA-03 Open Network Ports	<input type="checkbox"/>
44	CP-08 Alternate Telecommunications Service	<input checked="" type="checkbox"/>
45	CP-07 Alternate Processing Site	<input type="checkbox"/>
46	CP-06 Alternate Storage Site	<input type="checkbox"/>
47	SI-02 Legacy Servers	<input type="checkbox"/>

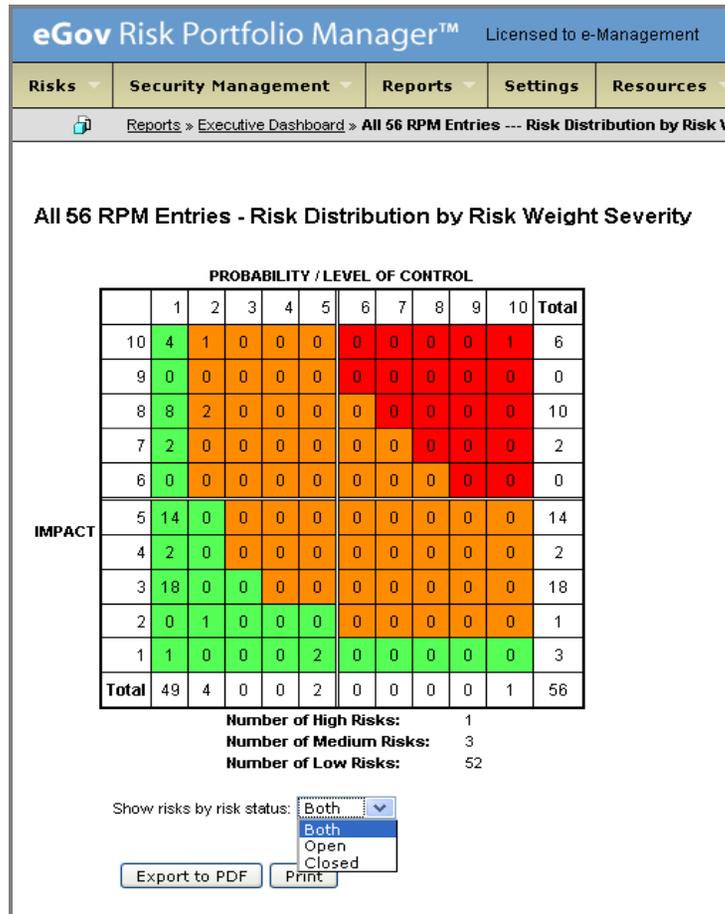
Add Risk Close

https://www.e-govrpm.com/RPM4/show_docu... Internet

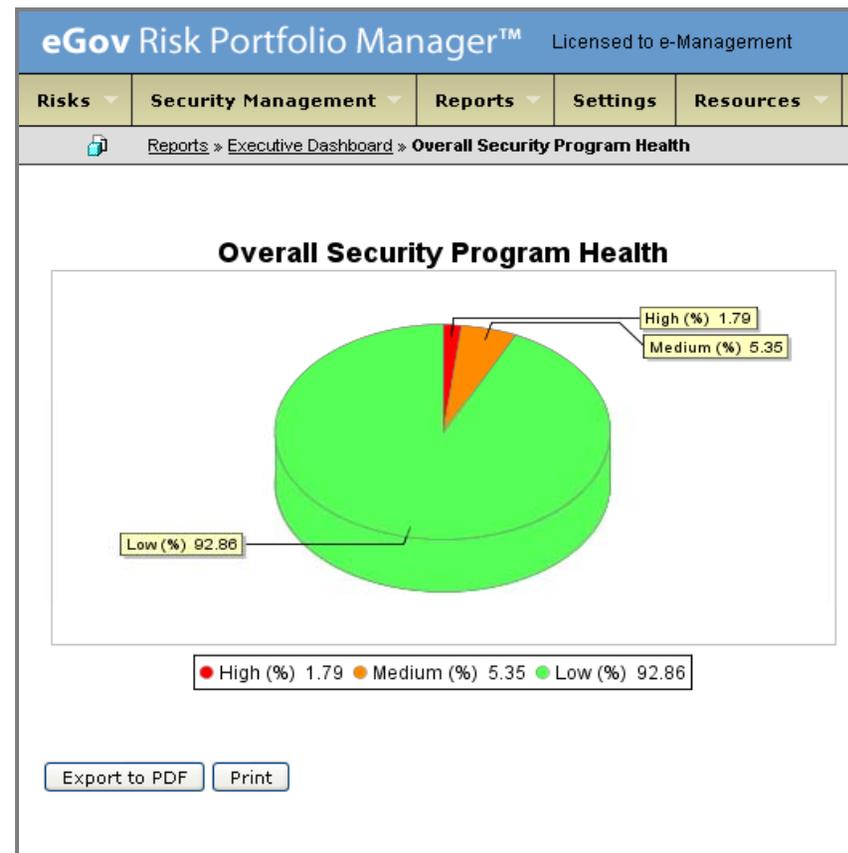
Done in conjunction with Security Plan Management mapping risks to controls

Reports in e-Gov RPM can be displayed in a variety of layouts or presentations

Risk Probability Matrix:



Pie Chart Distribution:



e-Gov RPM™ provides multiple types of reports, at varying degrees of technical detail, to accommodate multiple audiences

The screenshot displays the 'eGov Risk Portfolio Manager™' web application. The top navigation bar includes 'Risks', 'Security Management', 'Reports', 'Settings', 'Resources', and 'Admin'. Below this, a secondary bar contains 'Generate Reports | Executive Dashboard'. The main content area is titled 'Generate Reports' and features a 'Report Selection:' dropdown menu with 'Risk Assessment Report' selected. A 'Sort by:' dropdown menu is set to 'Risk Title'. A 'Categories:' list is visible, including 'Dependencies / Interoperability', 'External', 'Feasibility', 'Initial Cost', 'Life-Cycle Costs', 'Monopoly Creation', 'New Custom Category', 'Operational', 'Organizational and Change Management', 'Overall Risk of Project Failure', 'Reliability of Systems', 'Schedule', 'Security', 'Technical Obsolescence', 'Technological', and 'Technology'. A 'Select all' checkbox is checked at the bottom. On the left, a tree view shows 'New Portfolio' and 'Project 1 Test'.

Conclusions – **Why e-Gov RPM?**

- ❑ **Flexible tool to organize and manage Risks**: e-Gov RPM provides a powerful tool to organize and manage risks in many ways for accreditation boundaries, organizations, programs, projects or software applications
- ❑ **Drive compliance and eliminate redundancy**: e-Gov RPM's pre-populated NIST guidance provides an on screen reference to relevant information and the central repository of risk and security information provides uses access without duplication (e.g. risk management control inheritance)
- ❑ **Save many HOURS in document preparation time**: e-Gov RPM automates the generation of many time consuming data call and report preparation tasks, increasing accuracy and efficiency in reporting
- ❑ **Mature**: e-Gov RPM has been marketed as a product for more than 7 years, has gone through 3 major version upgrades and is used in several different risk management environments
- ❑ **Customized Report**: eGov RPM V4.0 leverages Crystal Reports to provide flexible reports that meet the customer's needs

Contact Information

➤ The Office of the Under Secretary of Energy

Dan Conway

daniel.conway@hq.doe.gov

➤ e-Management

Bill Bodine

Program Manager, e-Management

Contractor to DOE EM

bill.bodine@em.doe.gov

e-Management

1010 Wayne Avenue, Suite 1150, Silver Spring, MD 20910

Phone: 301.565.2988

Fax: 301.565.2995

www.e-mcinc.com

info@e-mcinc.com