



Training...Knowledge...Competency...Success



Office of the Associate CIO for Cyber Security
Office of the Chief Information Officer



Course Catalog

Training resources available from
**IM-31, Policy, Guidance, and Planning Division;
SANS Institute; or DOE Online Learning Center (OLC)**


The courses listed in this catalog have been identified as training resources that either provide general cyber security awareness material or have been selected to satisfy cyber security training and awareness recommendations for general users and for personnel with job responsibilities identified as key cyber security functional roles. These roles include the Chief Information Officer (CIO), Information Owner/Steward, Chief Information Security Officer (CISO), Authorizing Official (AO), AO Designated Representative (AODR), Common Control Provider, Information System Owner, Cyber Security Program Manager (CSPM), Information System Security Officer (ISSO), Information Security Architect, Information System Security Engineer, and the Security Control Assessor. Additionally, this catalog contains recommended role-based training modules and/or SANS Institute¹ courses that address core competency knowledge requirements for cyber security professionals.

¹ Descriptions for recommended SANS Institute courses were paraphrased from SANS overview material. For additional information and scheduling for SANS courses, visit www.sans.org.

General Cyber Security Awareness




Title	Transmission Medium	Description	Course Number	Date
Information Technology (IT) Security Basics & Literacy		This course introduces several cyber security foundational topics such as threats and vulnerabilities; malicious code; principles of confidentiality, integrity, and availability; General Support Systems (GSS); Major Applications (MAs); critical infrastructure protection; disaster recovery and business resumption plans; privacy act; etc. Accessed via OLC.	49930i	3/08/07
Information Security Awareness		This course focuses on managing cyber threats and vulnerabilities. Examples of attacks are given to include passive, active, malicious and non-malicious insider, etc. This class addresses risks associated with remote users. Accessed via OLC.	#fgov_01_a12_1e_enus	6/03/08

Annual Cyber Security Refresher Briefing

Title	Transmission Medium	Description	Course Number	Date
Information Systems Security Awareness v5		This course is required to be successfully completed by all DOE employees annually. The course address major security disciplines to include technical, logical, physical, operational, and personnel security as well as describes DOE-specific cyber security requirements. This course is ISSLoB compliant. Accessed via OLC.	ISSAv5	2012

DOE EBK Role-Based Courses

Authorizing Official (AO)/AO Designated Representative

Title	Transmission Medium	Description	Course Number	Date
Authorizing Official (AO)/AO Designated Representative Role-Based Training		This course is designed for AOs and AODRs who must understand the concepts of risk management to ensure Cyber security within DOE. Understanding risk management concepts is particularly important for the AO, who is charged with the decision to accept (or reject) residual risk on behalf of the DOE. Accessed via OLC.	zdoe_it_a01_fg_enus	2/12
Information Security & Risk Management		The course addresses risk management principles to include risk categories, security planning, threat analysis, vulnerability and asset evaluation, and risk analysis, evaluation, and mitigation. Accessed via OLC.	243962	7/27/07
Security Architecture & Design		This course addresses the Certification & Accreditation (C&A) Security Evaluation Process as well as the common principles behind computer architectures and security models. The course utilizes CISSP language. Accessed via OLC.	243975	7/27/07

Information System Security Officer (ISSO)

Title	Transmission Medium	Description	Course Number	Date
Introduction to Information Security	www.sans.org	This introductory certification course is the fastest way to get up to speed in information security. This entry-level course covers a broad spectrum of security topics and is liberally sprinkled with real life examples. A balanced mix of technical and managerial issues makes this course appealing to attendees who need to understand the salient facets of information security basics and the basics of risk management.	SEC301	--
SANS Security Essentials Bootcamp Style	www.sans.org	Maximize training time in security by learning the full SANS Security Essentials curriculum needed to qualify for the GSEC certification. In this course the student will learn the language and underlying theory of cyber	SEC401	--

Title	Transmission Medium	Description	Course Number	Date
		security. <i>SPECIAL NOTE: This course is endorsed by the Committee on National Systems (CNSS) NSTISSI 4013 Standard for Systems Administrators in Information Systems Security (INFOSEC).</i>		
Advanced Security Essentials – Enterprise Defender	www.sans.org	Security 501 is a follow up to SEC401 SANS Security Essentials and continues to focus on more technical areas that are needed to protect an organization. The core focus of the course is on prevention, detection, and reaction.	SEC501	--
Hacker Techniques, Exploits and Incident Handling	www.sans.org	This course addresses the latest cutting-edge insidious attack vectors and the legendary attacks that are still prevalent in today's cyber world. This course includes a time-tested, step-by-step process for responding to computer incidents; a detailed description of how attackers undermine systems so that professionals can prepare, detect, and respond to them; and a hands-on workshop for discovering security holes. Finally, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence.	SEC504	--
Foundations of Auditing Information Systems	www.sans.org	This course is designed for security and assurance professionals, system administrators, and business and operational auditors who want to develop the technical and operational knowledge of information system auditing. This course is a careful balance of the audit process, governance, and compliance regulations, as well a hands-on introduction to the latest technology tools.	AUD407	--
Securing the Human: Building and Deploying an Effective Security Awareness Program	www.sans.org	In this challenging course, the student will learn the key concepts and skills to plan, implement, and maintain an effective cyber security awareness program that makes an organization both more secure and compliant. In addition, the student will develop metrics to measure the impact of the awareness program and demonstrate value. Finally, through a series of labs and exercises, the student will develop their own project and execution plan, so that they can immediately implement a customized awareness program in their organization.	MGT433	--

DOE EBK Core Competency/NICE Workforce Framework Courses

Data Security Core Competency/Securely Provision

Title	Transmission Medium	Description	Course Number	Date
Advanced Security Essentials – Enterprise Defender	www.sans.org	Security 501 is a follow up to SEC401 SANS Security Essentials and continues to focus on more technical areas that are needed to protect an organization. The core focus of the course is on prevention, detection, and reaction.	SEC501	--
Perimeter Protection In-Depth	www.sans.org	This course provides in-depth training on TCP/IP for firewalls; wire products and assessments; host level security, etc.	SEC502	--
Implementing and Auditing the Twenty Critical Controls In-Depth	www.sans.org	This course helps the student master specific, proven techniques and tools needed to implement and audit the Top Twenty Most Critical Security Controls. The Top 20 Security Controls are rapidly becoming accepted as the highest priority list of what must be done and proven before anything else at nearly all security conscious organizations.	SEC566	--
Foundations of Auditing Information Systems	www.sans.org	This course is designed for security and assurance professionals, system administrators, and business and operational auditors who want to develop the technical and operational knowledge of information system auditing. This course is a careful balance of the audit process, governance, and compliance regulations, as well a hands-on introduction to the latest technology tools.	AUD407	--
Auditing Networks, Perimeters & Systems	www.sans.org	This course is organized to provide a risk-driven method for tackling the task of designing an enterprise security validation program. After covering a variety of high-level audit issues and general audit best practices, the students will have the opportunity to dive deep into the technical how-to for determining the key controls that can be used to provide a level of assurance to an organization.	AUD507	--

Title	Transmission Medium	Description	Course Number	Date
Defending Web Applications Security Essentials	www.sans.org	DEV522 covers the OWASP Top 10 to help the student better understand web application vulnerabilities. Mitigation strategies from an infrastructure, architecture, and coding perspective will be discussed alongside real-world implementations.	DEV522	--

Incident Management Core Competency/Protect & Defend-Incident Response

Title	Transmission Medium	Description	Course Number	Date
Hacker Techniques, Exploits and Incident Handling	www.sans.org	This course addresses the latest cutting-edge insidious attack vectors and the legendary attacks that are still prevalent in today's cyber world. This course includes a time-tested, step-by-step process for responding to computer incidents; a detailed description of how attackers undermine systems so that professionals can prepare, detect, and respond to them; and a hands-on workshop for discovering security holes. Finally, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence.	SEC504	--
Computer Forensics Investigations – Windows In-Depth	www.sans.org	This course focuses on the critical knowledge of the Windows OS that every digital forensic analyst must know to investigate computer incidents successfully. The student will learn how computer forensic analysts focus on collecting and analyzing data from computer systems to track user-based activity that could be used internally or in civil/criminal litigation.	FOR408	--
Advanced Computer Forensic Analysis and Incident Response	www.sans.org	This course provides the student with the tools and techniques necessary to master advanced incident response, investigate data breach intrusions, find tech-savvy rogue employees, counter the Advanced Persistent Threat (APT), and conduct complex digital forensic cases.	FOR508	--

IT Systems Operations & Maintenance Core Competency/Operate & Maintain - System Administration


Title	Transmission Medium	Description	Course Number	Date
SANS Security Essentials Bootcamp Style	www.sans.org	Maximize training time in security by learning the full SANS Security Essentials curriculum needed to qualify for the GSEC certification. In this course the student will learn the language and underlying theory of cyber security. <i>SPECIAL NOTE: This course is endorsed by the Committee on National Systems (CNSS) NSTISSI 4013 Standard for Systems Administrators in Information Systems Security (INFOSEC).</i>	SEC401	--
Perimeter Protection In-Depth	www.sans.org	This course provides in-depth training on TCP/IP for firewalls; wire products and assessments; host level security, etc.	SEC502	--

Network & Telecommunication Security Core Competency/Operate & Maintain – Network Services

Title	Transmission Medium	Description	Course Number	Date
Advanced Security Essentials – Enterprise Defender	www.sans.org	Security 501 is a follow up to SEC401 SANS Security Essentials and continues to focus on more technical areas that are needed to protect an organization. The core focus of the course is on prevention, detection, and reaction.	SEC501	--
Perimeter Protection In-Depth	www.sans.org	This course provides in-depth training on TCP/IP for firewalls; wire products and assessments; host level security, etc.	SEC502	--
Intrusion Detection In-Depth	www.sans.org	This course provides practical hands-on intrusion detection and traffic analysis from top practitioners/authors in the field. This course provides instruction on the theory of TCP/IP, examining packets, using Snort to analyze traffic, and becoming familiar with the tools and techniques for traffic and intrusion analysis.	SEC503	--
Web App Penetration Testing and Ethical Hacking	www.sans.org	In this intermediate to advanced level class, the student will learn the art of exploiting Web applications so that he/she can effectively identify flaws in internal Web applications before an adversary does.	SEC542	--

Title	Transmission Medium	Description	Course Number	Date
		Through detailed, hands-on exercises and training from a seasoned professional, the student will be taught the four-step process for Web application penetration testing.		
Network Penetration Testing and Ethical Hacking	www.sans.org	This course prepares the student with the skills necessary to conduct successful penetration testing and ethical hacking projects. The course starts with proper planning, scoping and recon, and then dives deep into scanning, target exploitation, password attacks, and wireless and web apps with detailed hands-on exercises and practical tips for doing the job safely and effectively.	SEC560	--
Implementing and Auditing the Twenty Critical Controls In-Depth	www.sans.org	This course helps the student master specific, proven techniques and tools needed to implement and audit the Top Twenty Most Critical Security Controls. The Top 20 Security Controls are rapidly becoming accepted as the highest priority list of what must be done and proven before anything else at nearly all security conscious organizations.	SEC566	--

Security Risk Management Core Competency

Title	Transmission Medium	Description	Course Number	Date
Security Risk Management (SRM) Role-Based Training		This course addresses the Security Risk Management (SRM), including the DOE Risk Management Approach (RMA) and Contractor Assurance System. This course emphasizes a cultural shift toward a risk-based versus compliance-based approach and recognizes the importance of contractors in supporting DOE's missions. Accessed via OLC.	zdoe_srm_a02_fg_enus	09/12

Strategic Security Management Core Competency/Protect & Defend – Security Program Management

Title	Transmission Medium	Description	Course Number	Date
SANS Security Leadership	www.sans.org	This course addresses the following essential	MGT512	--


Title	Transmission Medium	Description	Course Number	Date
Essentials for Managers with Knowledge Comprehension		security topics: network fundamentals and applications; power; cooling and safety; architectural approaches to defense in depth; cyber attacks; vulnerability assessment and management; security policies; contingency and continuity planning; awareness management; risk management analysis; incident handling; Web application security; and offensive and defensive information warfare.		
IT Security Strategic Planning, Policy and Leadership	www.sans.org	This course covers three focus areas critical to senior management: mastering the strategic planning process; creating effective information security policy; and developing management and leadership skills.	MGT514	--

System & Application Security Core Competency/Securely Provision & Operate& Maintain – System Security Analysis and Assurance





Title	Transmission Medium	Description	Course Number	Date
SANS Security Essentials Bootcamp Style	www.sans.org	Maximize training time in security by learning the full SANS Security Essentials curriculum needed to qualify for the GSEC certification. In this course the student will learn the language and underlying theory of cyber security. <i>SPECIAL NOTE: This course is endorsed by the Committee on National Systems (CNSS) NSTISSI 4013 Standard for Systems Administrators in Information Systems Security (INFOSEC).</i>	SEC401	--
Advanced Security Essentials – Enterprise Defender	www.sans.org	Security 501 is a follow up to SEC401 SANS Security Essentials and continues to focus on more technical areas that are needed to protect an organization. The core focus of the course is on prevention, detection, and reaction.	SEC501	--
Perimeter Protection In-Depth	www.sans.org	This course provides in-depth training on TCP/IP for firewalls; wire products and assessments; host level security, etc.	SEC502	--
Implementing and Auditing the Twenty Critical Controls In-Depth	www.sans.org	This course helps the student master specific, proven techniques and tools needed to implement and audit the Top Twenty Most Critical Security Controls. The Top 20 Security	SEC566	--

Title	Transmission Medium	Description	Course Number	Date
		Controls are rapidly becoming accepted as the highest priority list of what must be done and proven before anything else at nearly all security conscious organizations.		
Auditing Networks, Perimeters & Systems	www.sans.org	This course is organized to provide a risk-driven method for tackling the task of designing an enterprise security validation program. After covering a variety of high-level audit issues and general audit best practices, the students will have the opportunity to dive deep into the technical how-to for determining the key controls that can be used to provide a level of assurance to an organization.	AUD507	--



Master Listing (Alphabetical Order)

Title	Transmission Medium	Description	Course Number	Date
Advanced Computer Forensic Analysis and Incident Response	www.sans.org	This course provides the student with the tools and techniques necessary to master advanced incident response, investigate data breach intrusions, find tech-savvy rogue employees, counter the Advanced Persistent Threat (APT), and conduct complex digital forensic cases.	FOR508	--
Advanced Security Essentials – Enterprise Defender	www.sans.org	Security 501 is a follow up to SEC401 SANS Security Essentials and continues to focus on more technical areas that are needed to protect an organization. The core focus of the course is on prevention, detection, and reaction.	SEC501	--
Auditing Networks, Perimeters & Systems	www.sans.org	This course is organized to provide a risk-driven method for tackling the task of designing an enterprise security validation program. After covering a variety of high-level audit issues and general audit best practices, the students will have the opportunity to dive deep into the technical how-to for determining the key controls that can be used to provide a level of assurance to an organization.	AUD507	--
Authorizing Official (AO)/AO Designated Representative Role-Based Training		This course is designed for AOs and AODRs who must understand the concepts of risk management to ensure Cyber security within DOE. Understanding risk management concepts is particularly important for the AO, who is charged with the decision to accept (or reject) residual risk on behalf of the DOE. Accessed via OLC.	zdoe_it_a01_fg_enus	2/12
Computer Forensics Investigations – Windows In-Depth	www.sans.org	This course focuses on the critical knowledge of the Windows OS that every digital forensic analyst must know to investigate computer incidents successfully. The student will learn how computer forensic analysts focus on collecting and analyzing data from computer systems to track user-based activity that could be used internally or in civil/criminal litigation.	FOR408	--

Title	Transmission Medium	Description	Course Number	Date
Defending Web Applications Security Essentials	www.sans.org	DEV522 covers the OWASP Top 10 to help the student better understand web application vulnerabilities. Mitigation strategies from an infrastructure, architecture, and coding perspective will be discussed alongside real-world implementations.	DEV522	--
Foundations of Auditing Information Systems	www.sans.org	This course is designed for security and assurance professionals, system administrators, and business and operational auditors who want to develop the technical and operational knowledge of information system auditing. This course is a careful balance of the audit process, governance, and compliance regulations, as well a hands-on introduction to the latest technology tools.	AUD407	--
Hacker Techniques, Exploits and Incident Handling	www.sans.org	This course addresses the latest cutting-edge insidious attack vectors and the legendary attacks that are still prevalent in today's cyber world. This course includes a time-tested, step-by-step process for responding to computer incidents; a detailed description of how attackers undermine systems so that professionals can prepare, detect, and respond to them; and a hands-on workshop for discovering security holes. Finally, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence.	SEC504	--
Implementing and Auditing the Twenty Critical Controls In-Depth	www.sans.org	This course helps the student master specific, proven techniques and tools needed to implement and audit the Top Twenty Most Critical Security Controls. The Top 20 Security Controls are rapidly becoming accepted as the highest priority list of what must be done and proven before anything else at nearly all security conscious organizations.	SEC566	--

Title	Transmission Medium	Description	Course Number	Date
Information Security Awareness		This course focuses on managing cyber threats and vulnerabilities. Examples of attacks are given to include passive, active, malicious and non-malicious insider, etc. This class also addresses risks associated with remote users. Accessed via OLC.	#fgov_01_a12_1e_enus	6/03/08
Information Security & Risk Management		The course addresses risk management principles to include risk categories, security planning, threat analysis, vulnerability and asset evaluation, and risk analysis, evaluation, and mitigation. Accessed via OLC.	243962	7/27/07
Information Systems Security Awareness v5		This course is required to be successfully completed by all DOE employees annually. The course address major security disciplines to include technical, logical, physical, operational, and personnel security as well as describes DOE-specific cyber security requirements. This course is ISSLoB compliant. Accessed via OLC.	ISSAv5	2012
Information Technology (IT) Security Basics & Literacy		This course introduces several cyber security foundational topics such as threats and vulnerabilities; malicious code; principles of confidentiality, integrity, and availability; General Support Systems (GSS); Major Applications (MAs); critical infrastructure protection; disaster recovery and business resumption plans; privacy act; etc. Accessed via OLC.	49930i	3/08/07
IT Security Strategic Planning, Policy and Leadership	www.sans.org	This course covers three focus areas critical to senior management: mastering the strategic planning process; creating effective information security policy; and developing management and leadership skills.	MGT514	--
Introduction to Information Security	www.sans.org	This introductory certification course is the fastest way to get up to speed in information security. This entry-level course covers a broad spectrum of security topics and is liberally sprinkled with real life examples. A balanced mix of technical and managerial issues makes this course appealing to attendees who need to understand the salient facets of	SEC301	--

Title	Transmission Medium	Description	Course Number	Date
		information security basics and the basics of risk management.		
Intrusion Detection In-Depth	www.sans.org	This course provides practical hands-on intrusion detection and traffic analysis from top practitioners/authors in the field. This course provides instruction on the theory of TCP/IP, examining packets, using Snort to analyze traffic, and becoming familiar with the tools and techniques for traffic and intrusion analysis.	SEC503	--
Network Penetration Testing and Ethical Hacking	www.sans.org	This course prepares the student with the skills necessary to conduct successful penetration testing and ethical hacking projects. The course starts with proper planning, scoping and recon, and then dives deep into scanning, target exploitation, password attacks, and wireless and web apps with detailed hands-on exercises and practical tips for doing the job safely and effectively.	SEC560	--
Perimeter Protection In-Depth	www.sans.org	This course provides in-depth training on TCP/IP for firewalls; wire products and assessments; host level security, etc.	SEC502	--
SANS Security Essentials Bootcamp Style	www.sans.org	Maximize training time in security by learning the full SANS Security Essentials curriculum needed to qualify for the GSEC certification. In this course the student will learn the language and underlying theory of cyber security. <i>SPECIAL NOTE: This course is endorsed by the Committee on National Systems (CNSS) NSTISSI 4013 Standard for Systems Administrators in Information Systems Security (INFOSEC).</i>	SEC401	--
SANS Security Leadership Essentials for Managers with Knowledge Comprehension	www.sans.org	This course addresses the following essential security topics: network fundamentals and applications; power; cooling and safety; architectural approaches to defense in depth; cyber attacks; vulnerability assessment and management; security policies; contingency and continuity planning; awareness management; risk management analysis; incident handling; Web application security; and offensive and defensive information warfare.	MGT512	--

Title	Transmission Medium	Description	Course Number	Date
Securing the Human: Building and Deploying an Effective Security Awareness Program	www.sans.org	In this challenging course, the student will learn the key concepts and skills to plan, implement, and maintain an effective cyber security awareness program that makes an organization both more secure and compliant. In addition, the student will develop metrics to measure the impact of the awareness program and demonstrate value. Finally, through a series of labs and exercises, the student will develop their own project and execution plan, so that they can immediately implement a customized awareness program in their organization.	MGT433	--
Security Architecture & Design		This course addresses the Certification & Accreditation (C&A) Security Evaluation Process as well as the common principles behind computer architectures and security models. The course utilizes CISSP language. Accessed via OLC.	243975	7/27/07
Security Risk Management (SRM) Role-Based Training		This course addresses the Security Risk Management (SRM), including the DOE Risk Management Approach (RMA) and Contractor Assurance System. This course emphasizes a cultural shift toward a risk-based versus compliance-based approach and recognizes the importance of contractors in supporting DOE's missions. Accessed via OLC.	zdoe_srm_a02_fg_enus	09/12
Web App Penetration Testing and Ethical Hacking	www.sans.org	In this intermediate to advanced level class, the student will learn the art of exploiting Web applications so that he/she can effectively identify flaws in internal Web applications before an adversary does. Through detailed, hands-on exercises and training from a seasoned professional, the student will be taught the four-step process for Web application penetration testing.	SEC542	--