SANS Technology Institute

Master of Science

In

Information Security Management

Course Descriptions

March 2014

SANS Technology Institute

Master of Science in Information Security Management

The Master of Science in Information Security Management (MSISM) Program is designed to accelerate the development of information security Managers by providing practical experience that can be immediately applied on the job. Students learn from the industry experts how to see the world from an attacker's view, audit information systems, assess legal implications of an incident, and develop risk-based secure enterprise-level solutions that enable an organization's business processes to function in spite of the increasing threat presence. In addition to developing hands-on technical skills, the program emphasizes the development of communication and leadership skills that will improve the student's ability to implement information security solutions within their organization.

ISM 5000 Research & Communications Methods

SANS class: MGT 305 Research & Communications Methods
Assessment: Oral Presentation, Writing Exercise
0.5 Credit Hours | $625

ISM 5000 covers strategies for conducting research and the oral and written communication that follows. The class allows the student to refine their ability to research and write professional quality reports, and to create and deliver oral presentations. Topics such as developing a convincing argument, synthesizing research and writing technical reports for non-technical audiences, and managing the communication environment are covered. Students participate in an editing exercise as well as a hands-on report writing and presentation development workshop, with a required oral presentation assessment.

ISM 5100 Enterprise Information Security

SANS class: MGT 512 Security Leadership Essentials
Assessment: GIAC GSLC, Paper
4 Credit Hours | $5,000

ISM 5100 is the introductory, survey course in the information security management master's program. It establishes the foundations for developing, assessing and managing security functions at the end-user, network and enterprise levels of an organization. The faculty instruction, readings, exam, and required student paper are coordinated to introduce and develop the core technical, management, and enterprise-level capabilities that will be developed throughout the master's program.

ISM 5200 Hacking Techniques & Incident Response

SANS class: SEC504 Hacker Techniques, Exploits & Incident Handling
Assessment: GIAC GCIH, NetWars Continuous
4 Credit Hours | $5,000

By adopting the viewpoint of a hacker, ISM 5200 provides an in-depth focus into the critical activity of incident handling. Students are taught how to manage intrusions by first looking at the techniques used by attackers to exploit a system. Students learn responses to those techniques, which can be adopted within the framework of

the incident handling process to handle attacks in an organized way. The faculty instruction, lab exercises, exam, and NetWars simulation are coordinated to develop and test a student's ability to utilize the core capabilities required for incident handling.

ISM 5300 Building Security Awareness

SANS class: MGT 433 Securing the Human: Building and Deploying an Effective Security Awareness Program
Assessment: Writing Exercise
1 Credit Hour | $1,250

One of the most effective ways to secure the human factor in an enterprise is an active awareness and education program that goes beyond compliance and leads to actual changes in behaviors. In ISM 5300, students learn the key concepts and skills to plan, implement, and maintain an effective security awareness programs that make organizations both more secure and compliant. In addition, metrics are introduced to measure the impact of the program and demonstrate value. Finally, through a series of labs and exercises, students develop their own project and execution plan, so they can immediately implement a customized awareness program for their organization.

ISM 5400 IT Security Planning, Policy & Leadership

SANS class: MGT 514 IT Security Strategic Planning, Policy, and Leadership
Assessment: Writing Exercises
3 Credit Hours | $3,750

ISM 5400 covers the entire strategic planning process: how to plan the plan, horizon analysis, visioning, environmental scans (SWOT, PEST, Porter's etc.), historical analysis, mission, vision, and value statements. The course also reviews the planning process core, candidate initiatives, the prioritization process, resource and IT change management in planning, how to build a roadmap, setting up assessments, and revising the plan.

ISM 5500 Research Presentation 1

Assessment: Oral Presentation
1 Credit Hour | $1,250

ISE 5500 gives students the ability to convert written material to a persuasive oral presentation such as might be appropriate in an enterprise environment. Students use research material written in a previous course in the curriculum to build and deliver a 30-minute presentation, typically given at a SANS training conference.

ISM 5600 Legal Issues in Data Security and Investigations

SANS class: LEG 523 Legal Issues in Information Technology and Security
Assessment: GIAC GLEG, Paper
4 Credit Hours | $5,000

ISM 5600 introduces students to the new laws on privacy, e-discovery, and data security so students can bridge the gap between the legal department and the IT department. It also provides students with skills in the analysis and use of contracts, policies, and records management procedures.

SANS Technology Institute

ISM 5700 Situational Response Practicum

Assessment: Oral Presentation, Writing Exercise
1 Credit Hour | $1,250

In ISE 5700, a small group of students is given an information security scenario that is partly based on current events, and requires a broad knowledge of information security concepts. Their task is to evaluate the scenario and to recommend a course of action. This experience is a timed 24-hour event and culminates in a group written report and presentation at the end of the 24-hour preparation time.

ISM 5800 IT Security Project Management

SANS class: MGT 525 IT Project Management, Effective Communication, and PMP® Exam Prep
Assessment: GIAC GCPM
3 Credit Hours | $3,750

In ISM 5800 you will learn how to improve your project planning methodology and project task scheduling to get the most out of your critical IT resources. The course utilizes project case studies that highlight information technology services as deliverables. ISM 5800 follows the basic project management structure from the PMBOK® Guide 5th edition and also provides specific techniques for success with information assurance initiatives. All aspects of IT project management are covered - from initiating and planning projects through managing cost, time, and quality while your project is active, to completing, closing, and documenting as your project finishes.

ISM 5900 Research Presentation 2

Assessment: Oral Presentation
1 Credit Hour | $1,250

ISE 5900 gives a chance to further develop their skills at converting written material into a persuasive oral presentation such as might be appropriate in an enterprise environment. Students use research material written from previous courses in the curriculum to build and deliver a 30-minute presentation, either at a SANS training conference, or in an online environment.

ISM 6000 Standards Based Implementation of Security

SANS class: SEC 566 Implementing and Auditing the Twenty Critical Security Controls
Assessment: Exam, Paper
4 Credit Hours | $5,000

Cybersecurity attacks are increasing and evolving so rapidly that is more difficult than ever to prevent and defend against them. ISM 6000 will help you to ensure that your organization has an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches. As threats evolve, an organization's security should too. Standards based implementation takes a prioritized, risk-based approach to security and shows you how standardized controls are the best way to block known attacks and mitigate damage from successful attacks.

SANS Technology Institute

ISM 6100 Security Project Practicum

Assessment: Writing Exercise
2 Credit Hours | $2,500

In ISM 6100, a small group of students is given an information security project that requires a broad knowledge of information security concepts. Their task is to evaluate the project assignment and to recommend a course of action. This experience is a timed 30-day event. Students receive the project assignment from faculty, and must respond with a project plan to address the assignment within 5 days. The group then uses their plan to address the assignment, and deliver a written report at the end of the 30-day period.

ISM 6200 Auditing Networks, Perimeters and Systems

SANS class: AUD 507 Auditing Networks, Perimeters, and Systems
Assessment: GIAC GSNA, Paper
4 Credit Hours | $5,000

ISM 6200 is organized specifically to provide a risk driven method for tackling the enormous task of designing an enterprise security validation program. After covering a variety of high level audit issues and general audit best practice, students 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. Tips on how to repeatably verify these controls and techniques for continuous monitoring and automatic compliance validation are given from real world examples.

ISM 6900 Information Security Fieldwork

Assessment: Oral Presentation
0.5 Credit Hours | $625

In ISM 6900, students move into the field to prepare and present on a project that will help increase computer security awareness. Students devise their own project content, based upon a defined need. Students are also responsible for inviting an audience to review the results of their project work . It is expected that at least one representative from the student's own organization (place of employment) will be present to provide evidence of the presentation.

MSISM Capstone

Assessment: GSM
0 Credit Hours

The GSM exam Capstone experience is a two day hands-on lab exercise where students demonstrate their ability to formulate and implement policies and solutions that demonstrate a thorough understanding of security foundations and practical applications of information technology. Students work through scenarios which require them to: construct information security approaches that balance organizational needs, apply standards-based approaches to information security risk management, and devise incident response strategies.

SANS Technology Institute

MSISM: Technical Electives

Candidates for the MSISM will choose one course from the following MSISE Advanced Technical Electives:

Courses in Cyber Defense

ISE 6215 Advanced Security Essentials

SANS class: SEC 501 Advanced Security Essentials - Enterprise Defender
Assessment: GIAC GCED
3 Credit Hours | $3,750

ISE 6215 reinforces the theme that prevention is ideal, but detection is a must. Students will learn how to ensure that their organizations constantly improve their security posture to prevent as many attacks as possible. A key focus is on data protection, securing critical information no matter whether it resides on a server, in robust network architectures, or on a portable device.

Despite an organization's best effort at preventing attacks and protecting its critical data, some attacks will still be successful. Therefore students will also learn how to detect attacks in a timely fashion through an in-depth understanding the traffic that flows on networks, scanning for indications of an attack. The course also includes instruction on performing penetration testing, vulnerability analysis, and forensics.

ISE 6220 Network Perimeter Protection

SANS class: SEC 502 Perimeter Protection In-Depth
Assessment: GIAC GPPA
3 Credit Hours | $3,750

ISE 6220 provides a comprehensive analysis of a wide breadth of technologies. In fact, this is probably the most diverse course in the STI catalog, as mastery of multiple security techniques is required to defend networks from remote attacks. The course moves beyond a focus on single operating systems or security appliances. The course teaches that a strong security posture must be comprised of multiple layers. The course was developed to give students the knowledge and tools necessary at every layer to ensure their network is secure.

ISE 6230: Securing Windows with the Critical Security Controls

SANS class: SEC 505 Securing Windows with the Critical Security Controls
Assessment: GIAC GCWN
3 Credit Hours | $3,750

ISE 6230 shows students how to secure Windows and how to minimize the impact of these changes on users of these changes. Through live demonstrations of the important steps, students follow along on their laptops. Where other courses focus on detection or remediation after the fact, the goal of this course is to prevent the infection in the first place. Students learn to write PowerShell scripts, but don't need any prior scripting experience.

ISE 6235: Securing Linux/Unix

SANS class: SEC 506 Securing Linux/Unix
Assessment: GIAC GCUX
3 Credit Hours | $3,750

ISE 6235 provides students with experience in in-depth coverage of Linux and Unix security issues, examining how to mitigate or eliminate general problems that apply to all Unix-like operating systems, including vulnerabilities in the password authentication system, file system, virtual memory system, and applications that commonly run on Linux and Unix. This course provides specific configuration guidance and practical, real-world examples, tips, and tricks.

Courses in Penetration Testing & Ethical Hacking

ISE 6315: Web App Penetration Testing and Ethical Hacking

SANS class: SEC 542 Web App Penetration Testing and Ethical Hacking
Assessment: GIAC GWAPT
3 Credit Hours | $3,750

ISE 6315 is a highly technical information security course in offensive strategies where students learn the art of exploiting Web applications so they can find flaws in enterprise Web apps before they are otherwise discovered and exploited. Through detailed, hands-on exercises students learn the four-step process for Web application penetration testing. Students will inject SQL into back-end databases, learning how attackers exfiltrate sensitive data. They then utilize cross-site scripting attacks to dominate a target infrastructure in a unique hands-on laboratory environment. Finally students explore various other Web app vulnerabilities in-depth with tried-and-true techniques for finding them using a structured testing regimen.

ISE 6320: Network Penetration Testing and Ethical Hacking

SANS class: SEC 560 Network Penetration Testing and Ethical Hacking
Assessment: GIAC GPEN
3 Credit Hours | $3,750

ISE 6320 prepares students 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. Students will participate in an intensive, hands-on Capture the Flag exercise, conducting a penetration test against a sample target organization.

ISE 6325: Mobile Device Security

SANS class: SEC 575 Mobile Device Security and Ethical Hacking
Assessment: GIAC GMOB
3 Credit Hours | $3,750

ISE 6325 helps students resolve their organization's struggles with mobile device security by equipping then with the skills needed to design, deploy, operate, and assess a well-managed secure mobile environment. From practical policy development to network architecture design and deployment, and mobile code analysis to penetration testing and ethical hacking, this course teaches students to build the critical skills necessary to support the secure deployment and use of mobile phones and tablets in their organization.

ISE 6330: Wireless Penetration Testing

SANS class: SEC 617 Wireless Ethical Hacking, Penetration Testing, and Defenses
Assessment: GIAC GAWN
3 Credit Hours | $3,750

ISE 6330 takes an in-depth look at the security challenges of many different wireless technologies, exposing students to wireless security threats through the eyes of an attacker. Using readily available and custom-developed tools, students will navigate through the techniques attackers use to exploit WiFi networks, Bluetooth devices, and a variety of other wireless technologies. Using assessment and analysis techniques, this course will show students how to identify the threats that expose wireless technology and build on this knowledge to implement defensive techniques that can be used to protect wireless systems.

ISE 6360: Advanced Network Penetration Testing

SANS class: SEC 660 Advanced Penetration Testing, Exploits, and Ethical Hacking
Assessment: GIAC GXPN
3 Credit Hours | $3,750

ISE 6360 builds upon ISE 6320 – Network Penetration Testing and Ethical Hacking. This advanced course introduces students to the most prominent and powerful attack vectors, allowing students to perform these attacks in a variety of hands-on scenarios. This course is an elective course in the Penetration Testing & Ethical Hacking certificate program, and an elective choice for the master's program in Information Security Engineering.

Courses in Digital Forensics & Incident Response

ISE 6420: Computer Forensic Investigations - Windows

SANS class: FOR 408 Computer Forensic Investigations - Windows In-Depth
Assessment: GIAC GCFE
3 Credit Hours | $3,750

ISE 6420 Computer Forensic Investigations – Windows focuses on the critical knowledge of the Windows Operating System that every digital forensic analyst needs to investigate computer incidents successfully. Students learn how computer forensic analysts focus on collecting and analyzing data from computer systems to track user-based activity that can be used in internal investigations or civil/criminal litigation. The course covers the methodology of in-depth computer forensic examinations, digital investigative analysis, and media exploitation so each student will have complete qualifications to work as a computer forensic investigator helping to solve and fight crime.

ISE 6425: Advanced Computer Forensic Analysis and Incident Response

SANS class: FOR 508 Advanced Computer Forensic Analysis and Incident Response
Assessment: GIAC GCFA
3 Credit Hours | $3,750

ISE 6425 teaches the necessary capabilities for forensic analysts and incident responders to identify and counter a wide range of threats within enterprise networks, including economic espionage, hacktivism, and financial crime syndicates. The course shows students how to work as digital forensic analysts and incident response team members to identify, contain, and remediate sophisticated threats-including nation-state sponsored Advanced Persistent Threats and financial crime syndicates. Students work in a hands-on lab developed from a real-world targeted attack on an enterprise network in order to learn how to identify what data might be stolen and by whom, how to contain a threat, and how to manage and counter an attack.

ISE 6440: Advanced Network Forensic Analysis

SANS class: FOR 572 Advanced Network Forensics and Analysis
Assessment: Exam
3 Credit Hours | $3,750

ISE 6440 focuses on the most critical skills needed to mount efficient and effective post-incident response investigations. Moving beyond the host-focused experiences in ISE 6420 and ISE 6425, ISE 6440 covers the tools, technology, and processes required to integrate network evidence sources into investigations, covering high-level NetFlow analysis, low-level pcap exploration, and ancillary network log examination. Students will employ a wide range of open source and commercial tools, exploring real-world scenarios to help the student learn the underlying techniques and practices to best evaluate the most common types of network-based attacks.

ISE 6460: Malware Analysis and Reverse Engineering

SANS class: FOR 610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques
Assessment: GIAC GREM
3 Credit Hours | $3,750

ISE 6460 teaches students how to examine and reverse engineer malicious programs – spyware, bots, Trojans, etc. – that target or run on Microsoft Windows, within browser environments such as JavaScript or Flash files, or within malicious document files (including Word and PDF). The course builds a strong foundation for reverse-engineering malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger and other tools. The malware analysis process taught in this class helps students understand how incident responders assess the severity and repercussions of a situation that involves malicious software and plan recovery steps. Students also experience how forensics investigators learn to understand key

characteristics of malware discovered during the examination, including how to establish indicators of compromise (IOCs) for scoping and containing the incident.

Additional Electives – Software Development

ISE 6615: Defending Web Applications Security Essentials

SANS class: DEV 522 Defending Web Applications Security Essentials
Assessment: GIAC GWEB
3 Credit Hours | $3,750

ISE 6615 covers the OWASP Top 10 and provides students with a better understanding of web application vulnerabilities, enabling them to properly defend organizational web assets. Mitigation strategies from an infrastructure, architecture, and coding perspective are discussed alongside real-world implementations that really work. The testing aspect of vulnerabilities is also covered so students can ensure their application is tested for the vulnerabilities discussed in class.