SANS MANAGEMENT

CYBER LEADER

2016

COURSE CATALOG

"The blending of management and technologies in a course is challenging. SANS course authors and instructors provide timely information to their students."

-James Lamadrid, Federal Government

Get the right training to build and lead a world-class security team!

sans.org/curricula/management

@secleadership

Dear Colleague,


Frank Kim

As security professionals, we have seen the landscape change. Information security is now more vital, crucial, relevant, and important to the growth of your organization than ever before. As a result, information security teams have more visibility, more budget, and more opportunity. However, with this increased responsibility comes more scrutiny. Security business leaders must learn how to navigate this new world of security.

Security managers and leaders must have the technical proficiency to lead, manage, and build world-class security teams. However, this technical know-how will only get you so far. Combining technical expertise and knowledge with a deep understanding of the business will position you to help your company execute its business strategy.

Whether you are a seasoned information security professional looking to take the next step in your career or a long-time manager wanting to learn more about information security, SANS training will provide you the opportunity to take the next step. Get the right training at the right point in your career and learn how to lead risk-based security programs, manage cutting-edge security projects, and build world-class security teams.

At the SANS Institute, we train the next generation of cyber leaders and managers. Join us and be prepared to be a vital part of the growth of your company.

Be a Cyber Leader!

Sincerely,

Frank Kim

Frank Kim
Chief Information Security Officer
Management Curriculum Lead

SANS MANAGEMENT

CYBER LEADER

CURRICULUM

FOUNDATIONAL

MGT512
SANS Security Leadership Essentials For Managers with Knowledge Compression™
GSLC

MGT525
IT Project Management, Effective Communication, and PMP® Exam Prep
GCPM

MGT414
SANS Training Program for CISSP Certification®
GISP

MGT305
Technical Communication and Presentation Skills for Security Professionals

CORE

MGT514
IT Security Strategic Planning, Policy, and Leadership

LEG523
Law of Data Security and Investigations
GLEG

MGT415
A Practical Introduction to Cyber Security Risk Management

MGT535
Incident Response Team Management

SPECIALIZATION

AUD507
Auditing & Monitoring Networks, Perimeters, and Systems
GSNA

SEC566
Implementing and Auditing the Critical Security Controls – In-Depth
GCCC

MGT433
Securing The Human: How to Build, Maintain and Measure a High-Impact Awareness Program

PMP is registered mark of the Project Management Institute, Inc.

SANS MANAGEMENT

CYBER LEADER

CURRICULUM

by Job Role

SECURITY LEADERSHIP

CISO | CIO | Information Security Officer | Director of IT/Security | Security Manager

MGT512
SANS Security Leadership Essentials For Managers with Knowledge Compression™
GSLC

MGT514
IT Security Strategic Planning, Policy, and Leadership

LEG523
Law of Data Security and Investigations
GLEG

MGT415
A Practical Introduction to Cyber Security Risk Management

MGT535
Incident Response Team Management

PROJECT MANAGEMENT

Security Project Management | Security Program Manager

MGT512
SANS Security Leadership Essentials for Managers with Knowledge Compression™
GSLC

MGT525
IT Project Management, Effective Communication & PMP® Exam Prep
GCPM

MGT305
Technical Communication and Presentation Skills for Security Professionals

RISK & GOVERNANCE

Chief Risk Officer | Risk Manager
Information Security Officer

LEG523
Law of Data Security and Investigations
GLEG

MGT415
A Practical Introduction to Cyber Security Risk Management

LEGAL & PRIVACY

General Counsel | Attorney
Chief Privacy Officer

SEC301
Intro to Information Security
GISF

LEG523
Law of Data Security and Investigations
GLEG

AUDIT & COMPLIANCE

Compliance Officer | Compliance Manager | Auditor | Internal Auditor

MGT512
SANS Security Leadership Essentials for Managers with Knowledge Compression™
GSLC

SEC566
Implementing and Auditing the Critical Security Controls – In-Depth
GCCC

AUD507
Auditing & Monitoring Networks, Perimeters, and Systems
GSNA

MGT415
A Practical Introduction to Cyber Security Risk Management

MGT433
Securing The Human: How to Build, Maintain and Measure a High-Impact Awareness Program

PMP is registered mark of the Project Management Institute, Inc.

MANAGEMENT EVENT SCHEDULE

LIVE TRAINING EVENTS	MGT 512	MGT 514	MGT 433	MGT 415	MGT 305	MGT 525	LEG 523	MGT 535	MGT 414	AUD 507	SEC 301	SEC 566
Las Vegas Las Vegas, NV | Jan 9-14	512								414			
Security East New Orleans, LA | Jan 25-30	512											566
Scottsdale Scottsdale, AZ | Feb 8-13		514							414			
McLean McLean, VA | Feb 15-20											301	
ICS Security SUMMIT Orlando, FL | Feb 16-23			433									
Anaheim Anaheim, CA | Feb 22-27	512										301	
SANS 2016 Orlando, FL | Mar 12-21	512	514	433	415	305	525	523	535	414	507	301	566
Atlanta Atlanta, GA | Apr 4-9									414			
Threat Hunting SUMMIT New Orleans, LA | Apr 12-19								535				
Security West San Diego, CA | May 1-6	512	514	433			525	523	535	414	507	301	566
Cyber Guardian Baltimore, MD | May 9-14	512								414			
Houston Houston, TX | May 9-14						525	523					
SANSFIRE Washington, DC | Jun 11-18	512	514	433		305	525	523	535	414	507	301	566

COMMUNITY SANS EVENTS												
New York, NY Jan 25-29							523					
Denver, CO Feb 8-13									414			
Portland, OR Jan 4-8											301	
Chantilly, VA Jan 11-15											301	
New York, NY Feb 8-12											301	
Las Vegas, NV Mar 7-11											301	
Madison, WI Mar 28 - Apr 1											301	
Chicago, IL Apr 4-8											301	
Sacramento, CA Jun 13-17												566
Chicago, IL Jun 13-17												566
Herndon, VA Mar 28 - Apr 1												566

SIMULCAST EVENTS												
Feb 22-26											301	
Mar 12-13			433									

VLIVE EVENTS												
Apr 25 - Jun 1									414			
Jul 11 - Aug 10											301	

WHO SHOULD ATTEND:

- All newly appointed information security officers
- Technically-skilled administrators who have recently been given leadership responsibilities
- Seasoned managers who want to understand what their technical people are telling them

MGT512

SANS Security Leadership Essentials for Managers with Knowledge Compression™

Five-Day Program | 33 CPEs | Laptop NOT Needed

This completely updated course is designed to empower advancing managers who want to get up to speed quickly on information security issues and terminology. You won't just learn about security, you will learn how to *manage* security. Lecture sections are intense; the most common student comment is that it's like drinking from a fire hose. The diligent manager will learn vital, up-to-date knowledge and skills required to supervise the security component of any information technology project. Additionally, the course has been engineered to incorporate the NIST Special Publication 800 (series) guidance so that it can be particularly useful to U.S. government managers and supporting contractors.

"Every IT security professional should attend no matter what their position. This information is important to everyone."
-John Flood, NASA

Essential security topics covered in this management track include 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, culminating with our management practicum. The material uses Knowledge Compression™, special charts, and other proprietary SANS techniques to help convey the key points of critical slides and keep the information flow rate at a pace senior executives demand every teaching hour of the course. The course has been evaluated and approved by CompTIA's CAQC program for Security+ 2008 to ensure that managers and their direct reports have a common baseline for security terminology and concepts. You will be able to put what you learn into practice the day you get back into the office.

"Tremendously valuable experience!! Learned a lot and also validated a lot of our current practices. Thank you!!" -Chad Gray, Booz Allen Hamilton

Knowledge Compression™

Maximize your learning potential!

Knowledge Compression™ is an optional add-on feature to a SANS class which aims to maximize the absorption and long-term retention of large amounts of data over a relatively short period of time. Through the use of specialized training materials, in-class reviews, examinations and test-taking instruction, Knowledge Compression™ ensures students have a solid understanding of the information presented to them. By attending classes that feature this advanced training product, you will experience some of the most intense and rewarding training programs SANS has to offer, in ways that you never thought possible!

SANS
MGT512

TRAINING EVENTS:

Las Vegas
Las Vegas, NV
January 9-14

Security East
New Orleans, LA
January 25-30

Anaheim
Anaheim, CA
February 22-27

SANS 2016
Orlando, FL
March 12-21

SANSFIRE
Washington, DC
June 11-18

www.giac.org/gleg

www.sans.edu


www.sans.org/8570

www.sans.org/ondemand

www.sans.org/selfstudy

MGT514
IT Security Strategic Planning, Policy, and Leadership

Five-Day Program | 30 CPEs | Laptop Recommended

As security professionals we have seen the landscape change. Cybersecurity is now more vital and relevant to the growth of your organization than ever before. As a result, information security teams have more visibility, more budget, and more opportunity. However, with this increased responsibility comes more scrutiny.

This course teaches security professionals how to navigate this new world of security by developing strategic plans, creating effective information security policy, and developing management and leadership skills.

"The instructor was great – very active, engaging, and thorough. There were great industry examples and well-led conversations."
-Jason Popp, Nordstrom Inc.

Develop Strategic Plans

Strategic planning is hard for IT and IT security professionals because we spend so much time responding and reacting. We almost never do strategic planning until we get promoted to a senior position, and then we are not equipped with the skills we need to run with the pack. MGT514 will teach you how to develop strategic plans that resonate with other IT and business leaders.

Create Effective Information Security Policy

Policy is a manager's opportunity to express expectations for the workforce, set the boundaries of acceptable behavior, and empower people to do what they ought to be doing. It is easy to get wrong. Have you ever seen a policy and responded by saying "No way, I am not going to do that"? Most of us have. Policy must be aligned with an organization's culture. In MGT514, we break down the steps to policy development so that you have the ability to design and assess policies that can successfully guide your organization.

"The course had really good case studies and examples which prompted useful class discussion – this helped in understanding."
-Alexis Brownings, CERT-UK

Develop Management and Leadership Skills

Leadership is a skill that must be learned, exercised, and developed to better ensure organizational success. Strong leadership is brought about primarily through selfless devotion to the organization and staff, tireless effort in setting the example, and having the vision to see and effectively use available resources toward the end goal.

Effective leadership entails persuading team members to accomplish their objectives, removing the obstacles preventing them from doing it, and maintaining the well-being of the team in support of the organization's mission. MGT514 will teach you to use management tools and frameworks to better lead, inspire, and motivate your teams.

WHO SHOULD ATTEND:

- CISOs
- Information security officers
- Security directors
- Security managers
- Aspiring security leaders
- Other security personnel who have team-lead or management responsibilities

SANS
MGT514

TRAINING EVENTS:

Scottsdale
Scottsdale, AZ
February 8-13

SANS 2016
Orlando, FL
March 12-21

Security West
San Diego, CA
May 1-6

SANSFIRE
Washington, DC
June 11-18

WHO SHOULD ATTEND:

- Individuals who need to prepare for the Project Management Professional (PMP)® Exam
- Security professionals who are interested in understanding the concepts of IT project management
- Managers who want to understand the critical areas of making projects successful
- Individuals working with time, cost, quality, and risk-sensitive projects and applications
- Anyone who would like to utilize effective communication techniques and proven methods to relate better to people
- Anyone in a key or lead engineering/design position who works regularly with project management staff

SANS MGT525

TRAINING EVENTS:

SANS 2016
Orlando, FL
March 12-21

SANSFIRE
Washington, DC
June 11-18

MGT525

IT Project Management, Effective Communication, and PMP® Exam Prep

Six-Day Program | 36 CPEs | Laptop NOT Needed

SANS MGT525: IT Project Management, Effective Communication, and PMP® Exam Prep is offered by The SANS Institute, a PMI® Registered Education Provider (R.E.P.). R.E.P.s provide the training necessary to earn and maintain the Project Management Professional (PMP)® and other professional credentials.

This course has been recently updated to fully prepare you for the 2016 PMP® exam changes. During this class you will learn how to improve your project planning methodology and project task scheduling to get the most out of your critical IT resources. We will utilize project case studies that highlight information technology services as deliverables. MGT525 follows the basic project management structure from the *PMBOK® Guide – Fifth Edition* and also provides specific techniques for success with information assurance initiatives. Throughout the week, we will cover all aspects of IT project management 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. A copy of the *PMBOK® Guide – Fifth Edition* is provided to all participants. You can reference the *PMBOK® Guide* and use your course material along with the knowledge you gain in class to prepare for the 2016 updated Project Management Professional (PMP)® Exam and the GIAC Certified Project Manager Exam.

"Within the first five minutes I knew this would be a very different (and welcomed) experience than prior training with other vendors. SANS' attention to detail is evident in every slide." -Jayme Jordan, Raytheon

The project management process is broken down into core process groups that can be applied across multiple areas of any project, in any industry. Although our primary focus is the application to the InfoSec industry, our approach is transferable to any projects that create and maintain services as well as general product development. We cover in-depth how cost, time, quality, and risks affect the services we provide to others. We will also address practical human resource management as well as effective communication and conflict resolution. You will learn specific tools to bridge the communications gap between managers and technical staff.

"I think this is an awesome course that provides the knowledge and tools that I can use right when I get back to work."
-Johnny Matamoros Jr., Freeman

GCPM
www.giac.org/gcpm

SANS Technology Institute
www.sans.edu

PMI Registered Education Provider — Project Management Institute

LEG523

Law of Data Security and Investigations

Five-Day Program | 30 CPEs | Laptop NOT Needed

- New for live delivery 2015: Sony Pictures' alleged denial of service attack on sites dumping its stolen corporate data.
- New for live delivery as of October 2014: Home Depot's legal and public statements about payment card breach.
- New legal tips on confiscating and interrogating mobile devices.
- New for live delivery as of April 2014: Course covers lawsuit by credit card issuers against Target's QSA and security vendor, Trustwave.
- New for live delivery as of January 2014: The public response by retailer Target to a major payment card security incident.

New law on privacy, e-discovery and data security is creating an urgent need for professionals who can bridge the gap between the legal department and the IT department. SANS LEG523 provides this unique professional training, including skills in the analysis and use of contracts, policies and records management procedures.

This course covers the law of business, contracts, fraud, crime, IT security, liability and policy – all with a focus on electronically stored and transmitted records. It also teaches investigators how to prepare credible, defensible reports, whether for cyber crimes, forensics, incident response, human resource issues or other investigations.

The course also provides training and continuing education for many compliance programs under information security and privacy mandates such as GLBA, HIPAA, FISMA, and PCI-DSS. In addition, LEG523 is associated with the coveted GLEG certification, which strengthens the credibility of forensics investigators as witnesses in court and can help a forensics consultant win more business.

Each successive day of this five-day course builds upon lessons from the earlier days in order to comprehensively strengthen your ability to help your enterprise (public or private sector) cope with illegal hackers, botnets, malware, phishing, unruly vendors, data leakage, industrial spies, rogue or uncooperative employees, or bad publicity connected with IT security. We will cover breaking stories ranging from Home Depot's legal and public statements about payment card breach to the lawsuit by credit card issuers against Target's QSA and security vendor, Trustwave.

"Coming from an intense IT operations background, it was extremely valuable to receive an understanding of my security role from a legal point of view." -John Ochman, BD

Recent updates to the course address hot topics such as legal tips on confiscating and interrogating mobile devices, the retention of business records connected with cloud computing and social networks like Facebook and Twitter, and analysis and response to the risks and opportunities surrounding open-source intelligence gathering.

Over the years this course has adopted an increasingly global perspective. Non-U.S. professionals attend LEG523 because there is no training like it anywhere else in the world. For example, a lawyer from the national tax authority in an African country took the course because electronic filings, evidence and investigations have become so important to her work. International students help the instructor, U.S. attorney Benjamin Wright, constantly revise the course and include more content that crosses borders.

www.giac.org/gleg

www.sans.edu

www.sans.org/ondemand

www.sans.org/selfstudy

WHO SHOULD ATTEND:

- Investigators
- Security and IT professionals
- Lawyers
- Paralegals
- Auditors
- Accountants
- Technology managers
- Vendors
- Compliance officers
- Law enforcement
- Privacy officers
- Penetration testers

SANS LEG523

TRAINING EVENTS:

SANS 2016
Orlando, FL
March 12-21

Security West
San Diego, CA
May 1-6

Houston
Houston, TX
May 9-14

SANSFIRE
Washington, DC
June 11-18

WHO SHOULD ATTEND:

- Security awareness training officers
- Chief Security Officers (CSO's) and security management
- Security auditors, governance and compliance officers
- Training, human resources and communications staff
- Organizations regulated by the Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act (FISMA),
- Family Educational Rights and Privacy Act (FERPA), Payment Card Industry-Data Security Standards
- (PCI-DSS), ISO/IEC 27001, Family Educational Rights and Privacy Act (FERPA), Sarbanes-Oxley Act (SOX), or any other compliance-driven standards.
- Anyone responsible for planning, deploying, or maintaining an awareness program

SANS

MGT433

TRAINING EVENTS:

ICS Security Summit
Orlando, FL
February 16-23

SANS 2016
Orlando, FL
March 12-21

Security West
San Diego, CA
May 1-6

SANSFIRE
Washington, DC
June 11-18

MGT433

Securing The Human: How to Build, Maintain and Measure a High-Impact Awareness Program

Two-Day Course | 12 CPEs | Laptop NOT Needed

Organizations have invested a tremendous amount of money and resources into securing technology, but little if anything into securing their employees and staff. As a result, people, not technology, have become their weakest link in cybersecurity. The simplest way for cyber attackers to hack into your organization is to target your employees. Unless, of course, you take the steps necessary to stop them. The most effective way to secure the human element is to establish a high-impact security awareness program that goes beyond just compliance and changes behaviors. This intense two-day course will teach you the key concepts and skills needed to build, maintain and measure just such a program. All course content is based on lessons learned from hundreds of security awareness programs from around the world. You will learn not only from your instructor, but from extensive interaction with your peers, as well. Finally, through a series of labs and exercises, you will develop your own custom security awareness plan that you can implement as soon as you return to your organization.

"As always, this SANS course offers information I can immediately apply to my organization!"
Leon Noseworthy, Collect of North Alantic-Qatar

You Will Learn:

- The Security Awareness Maturity Model and how to use it as the roadmap for your awareness program
- How to effectively engage and communicate within your organization
- How to identify and mitigate the top human risks to your organization
- How to sustain your security awareness program over the long term, including updating content and communication methods and, ultimately, changing your organization's culture
- How to measure the impact of your awareness program, track reduction in human risk, and communicate the value of such a program to management

"This course fully encompasses everything it will take to build an awareness program in just 2 days! Great materials, resources and tool kit."
-Sadaf Amini, Sony Network Entertainment

Author Statement

Having been actively involved in information security for more than 15 years, I have seen one constant factor: people are the weakest link. What amazes me is that so many security professionals agree on this point, but so few do anything about it. I am determined to change that. I am extremely excited about MGT433, as we provide organizations with the skills and resources they need to build a high-impact security awareness program that will not only change behaviors, but also measure that change.
-Lance Spitzner

SANS Technology Institute
www.sans.edu

MGT415

A Practical Introduction to Cyber Security Risk Management

NEW!

Two-Day Course | 12 CPEs | Laptop Required

In this course, students will learn the practical skills necessary to perform regular risk assessments for their organizations. The ability to perform a risk assessment is crucial for organizations hoping to defend their systems. There are simply too many threats, too many potential vulnerabilities, and not enough resources to create an impregnable security infrastructure. Therefore every organization, whether it does so in an organized manner or not, will make priority decisions on how best to defend its valuable data assets. Risk assessment should be the foundational tool used to facilitate thoughtful and purposeful defense strategies.

You Will Be Able To:

- Perform a complete risk assessment.
- Inventory an organization's most critical information assets.
- Assign a data owner and custodian to an information asset.
- Assign classification values to critical information assets.
- Prioritize risk remediation efforts as a result of performing a risk assessment.
- Evaluate risk management models for use in your own organization.

SELFSTUDY WITH THIS COURSE
sans.org/selfstudy

SANS MGT415

TRAINING EVENTS:

SANS 2016
Orlando, FL
March 12-21

MGT305

Technical Communication and Presentation Skills for Security Professionals

One-Day Course | 6 CPEs | Laptop Required

This course is designed for every IT professional in your organization. In this course we cover the top techniques that will show any attendee how to research and write professional quality reports, and how to create outstanding presentation materials. Attendees will also get a crash course on advanced public speaking skills.

We cover step by step how to work through the process of identifying critical ideas, how to properly research them, how to develop a strong argument in written form, and how to put it all down on paper. We also discuss some of the most common mistakes that can negatively impact the reception of your work and show how to avoid them. Attendees can expect to see the overall quality of their reports improve significantly as a result of this material.

Writing the presentation is only half of the battle, though. How do you stand up in front of a group of five or even five thousand and speak? We will share tips and techniques of top presenters that you can apply to give the best presentation of your career. Additionally, students will have the opportunity to work up and deliver a short presentation to the class followed by some personal feedback from one of SANS' top speakers.

SANS Technology Institute
www.sans.edu

SELFSTUDY WITH THIS COURSE
www.sans.org/selfstudy

SANS MGT305

TRAINING EVENTS:

SANS 2016
Orlando, FL
March 12-21

SANSFIRE
Washington, DC
June 11-18

WHO SHOULD ATTEND:

- Information security engineers and managers
- IT managers
- Operations managers
- Risk management professionals
- IT/system administration/ network administration professionals
- IT auditors
- Business continuity and disaster recovery staff

MGT535
Incident Response Team Management

Two-Day Course | 12 CPEs | Laptop NOT Needed

This course discusses the often-neglected topic of managing an incident response team. Given the frequency and complexity of today's cyber attacks, incident response is a critical function for organizations. Incident response is the last line of defense.

Detecting and efficiently responding to incidents requires strong management processes, and managing an incident response team requires special skills and knowledge. A background in information security management or security engineering is not sufficient for managing incidents. On the other hand, incident responders with strong technical skills do not necessarily become effective incident response managers. Special training is necessary.

You Will Learn:

- Fundamentals of incident response
- How to establish requirements
- How to set up operations
- Communications
- How to make operations work
- Legal and regulatory issues
- Training, education, and awareness

Author Statement

"Incident response management is a dynamic and challenging endeavor fraught with high personnel turnover, rapid technology shifts, minimal funding, and a nearly impossible objective of defending an organization from every conceivable threat. I managed incident response teams and created incident response capabilities where none existed before. Incident response is the most challenging position to hold in Information Assurance, as you are the team that is called upon at the worst time, to fight the hardest battles. Through this course, I intend to equip each one of you to navigate difficult political environments, understand complicated technology, analyze the data and information provided by technical staff, and translate this information into business-relevant information that will make the organization more resilient for the long term."
-Chris Crowley

"The training was valuable to me because it put a lot of things in perspective with my job but providing good content to take back with me. It was worth the training."
-Charles Sanders, NASA

SELFSTUDY
WITH THIS COURSE
www.sans.org/selfstudy

SANS
MGT535

TRAINING EVENTS:

SANS 2016
Orlando, FL
March 12-21

Threat Hunting Summit
New Orleans, LA
April 12-19

Security West
San Diego, CA
May 1-6

SANSFIRE
Washington, DC
June 11-18

MGT414
SANS Training Program for CISSP® Certification®

Six-Day Program | 46 CPEs | Laptop NOT Needed

Eric Conrad and Seth Misenar, authors of the bestselling *Syngress CISSP® Study Guide*, have fully updated the course to address the 2016 version of the CISSP® exam.

"This course breaks the huge CISSP study books down into manageable chunks, and helped me focus and identify weaknesses. The instructor's knowledge and teaching skills are excellent."
-Jeff Jones, Constellation Energy Group

MGT414: SANS Training Program for CISSP® Certification is an accelerated review course designed to prepare you to pass the exam. The course takes into account the 2015 updates to the CISSP® exam and prepares students to navigate all types of questions included on the new version of the exam.

This course focuses solely on the 8 domains of knowledge as determined by $(ISC)^2$. Each domain of knowledge is dissected into its critical components, and those components are then discussed in terms of their relationship with one another and with other areas of information security.

After completion of this course, students will have a strong working knowledge of the 8 domains of knowledge and be better placed to pass the exam.

You Will Be Able To:

- Understand the 8 domains of knowledge that are covered on the CISSP® exam.
- Analyze questions on the exam and be able to select the correct answer.
- Apply the knowledge and testing skills learned in class to pass the CISSP® exam.
- Understand and explain all of the concepts covered in the 8 domains of knowledge.
- Apply the skills learned across the 8 domains to solve security problems when you return to work

You Will Receive With This Course:

- Course books for each of the 8 domains
- 320 questions to test knowledge and preparation for each domain

Over the past 4 years, 98% of all surveyed students who took SANS MGT414 and then took the CISSP® Certification Exam passed, compared to a national average of around 70% for other prep courses.

Take advantage of SANS' CISSP® Get Certified Program currently being offered.
sans.org/gissp

www.giac.org/gisp

www.sans.org/8570

Bundle OnDemand with this course
www.sans.org/ondemand

SelfStudy with this course
www.sans.org/selfstudy

WHO SHOULD ATTEND:

- Security professionals who are interested in understanding the concepts covered in the CISSP® exam as determined by $(ISC)^2$
- Managers who want to understand the critical areas of network security
- System, security, and network administrators who want to understand the pragmatic applications of the CISSP® 10 domains
- Security professionals and managers looking for practical ways the 10 domains of knowledge can be applied to the current job
- In short, if you desire a CISSP® or your job requires it, MGT414 is the training for you to get GISP certified

SANS
MGT414

TRAINING EVENTS:

Las Vegas
Las Vegas, NV | Jan 9-14

Scottsdale
Scottsdale, AZ | Feb 8-13

SANS 2016
Orlando, FL | Mar 12-21

Atlanta
Atlanta, GA | Apr 4-9

Security West
San Diego, CA | May 1-6

Cyber Guardian
Baltimore, MD | May 9-14

SANSFIRE
Washington, DC | Jun 11-18

Community SANS
Denver, CO | Feb 8-13

vLive Events
Apr 25 - Jun 1

WHO SHOULD ATTEND:

- Auditors seeking to identify key controls in IT systems
- Audit professionals looking for technical details on auditing
- Managers responsible for overseeing the work of an audit or security team
- Security professionals newly tasked with audit responsibilities
- System and network administrators looking to better understand what an auditor is trying to achieve, how auditors think, and how to better prepare for an audit
- System and network administrators seeking to create strong change control management and detection systems for the enterprise

SANS
AUD507

TRAINING EVENTS:

SANS 2016
Orlando, FL
March 12-21

Security West
San Diego, CA
May 1-6

SANSFIRE
Washington, DC
June 11-18

AUD507
Auditing & Monitoring Networks, Perimeters, and Systems

Six-Day Program | 36 CPEs | Laptop Required

One of the most significant obstacles facing many auditors today is how exactly to go about auditing the security of an enterprise. What systems really matter? How should the firewall and routers be configured? What settings should be checked on the various systems under scrutiny? Is there a set of processes that can be put into place to allow an auditor to focus on the business processes rather than the security settings? All of these questions and more will be answered by the material covered in this course.

"This course is full of relevant, timely, current content, delivered in a highly engaging style. This course is a must for IT auditors and security specialists."
-Brooks Adams, Georgia Southern University

This course is specifically organized 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 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. Tips on how to repeatedly verify these controls and techniques for automatic compliance validation will be given from real-world examples.

One of the struggles that IT auditors face today is helping management understand the relationship between the technical controls and the risks to the business that that these controls address. In this course, these threats and vulnerabilities are explained based on validated information from real-world situations. The instructor will take the time to explain how this can be used to raise the awareness of management and others within the organization to build an understanding of why these controls specifically and auditing in general are important. From these threats and vulnerabilities, we will explain how to build the ongoing compliance monitoring systems and how to automatically validate defenses through instrumentation and automation of audit checklists.

"In 20+ years of industry experience, I have never seen a smoother intro to batch progress to branching and looping. Well done!"
-Michael Decker, CNS Security

A great audit is more than marks on a checklist; it is the understanding of what the underlying controls are, what the best practices are, and why. Sign up for this course and experience the mix of theory, hands-on exercises, and practical knowledge.

SEC566

Implementing and Auditing the Critical Security Controls – In-Depth

Five-Day Program | 30 CPEs | Laptop Required

Cybersecurity attacks are increasing and evolving so rapidly that it is more difficult than ever to prevent and defend against them. Does your organization have an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches? This course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security (CIS).

As threats evolve, an organization's security should too. To enable your organization to stay on top of this ever-changing threat scenario, SANS has designed a comprehensive course on how to implement the Critical Security Controls, a prioritized, risk-based approach to security. Designed by private and public sector experts from around the world, the Controls are the best way to block known attacks and mitigate damage from successful attacks. They have been adopted by the U.S. Department of Homeland Security, state governments, universities, and numerous private firms.

"I'm leaving the class with a great mindset aimed at evaluating the current environment and controls. SEC566 was good information with a great instructor!" -Tom Kozelsky, Nexeo Solution

The Controls are specific guidelines that CISOs, CIOs, IGs, systems administrators, and information security personnel can use to manage and measure the effectiveness of their defenses. They are designed to complement existing standards, frameworks, and compliance schemes by prioritizing the most critical threat and highest payoff defenses, while providing a common baseline for action against risks that we all face.

The Controls are an effective security framework because they are based on actual attacks launched regularly against networks. Priority is given to Controls that (1) mitigate known attacks (2) address a wide variety of attacks, and (3) identify and stop attackers early in the compromise cycle.

The British government's Center for the Protection of National Infrastructure describes the Controls as the "baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defence."

SANS' in-depth, hands-on training will teach you how to master the specific techniques and tools needed to implement and audit the Critical Controls. It will help security practitioners understand not only how to stop a threat, but why the threat exists, and how to ensure that security measures deployed today will be effective against the next generation of threats.

The course shows security professionals how to implement the controls in an existing network through cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the Controls are effectively implemented.

www.giac.org/gccc

www.sans.edu

WITH THIS COURSE
www.sans.org/ondemand

WITH THIS COURSE
www.sans.org/selfstudy

WHO SHOULD ATTEND:

- All newly appointed information security officers
- Technically-skilled administrators who have recently been given leadership responsibilities
- Seasoned managers who want to understand what their technical people are telling them

SANS SEC566

TRAINING EVENTS:

Security East
New Orleans, LA
January 25-30

SANS 2016
Orlando, FL
March 12-21

Security West
San Diego, CA
May 1-6

SANSFIRE
Washington, DC
June 11-18

Community SANS
Sacramento, CA | Jun 13-17
Chicago, IL | Jun 13-17
Herndon, VA | Mar 28-Apr 1

SANS MANAGEMENT FACULTY

Frank Kim *SANS Certified Instructor*

As CISO at the SANS Institute Frank leads the security risk function for the most trusted source of computer security training, certification, and research in the world. He also helps shape, develop, and support the next generation of security leaders through teaching, developing courseware, and leading the management and software security curricula. Prior to the SANS Institute, Frank was Executive Director of Cyber Security at Kaiser Permanente, where he was accountable for delivering innovative security solutions to meet the unique needs of the nation's largest not-for-profit health plan and integrated health care provider with annual revenue of $55 billion, 9.5 million members, and 175,000 employees. In recognition of his work, Frank was a two-time recipient of the CIO Achievement Award for business-enabling thought leadership. Frank holds degrees from the University of California at Berkeley and is a SANS certified instructor as well as the author of popular courseware on strategic planning, leadership, and application security. @sansappsec

David Hoelzer *SANS Faculty Fellow*

David Hoelzer is the author of more than 20 sections of SANS courseware. He is an expert in a variety of information security fields, having served in most major roles in the IT and security industries over the past 25 years. Recently, David was called upon to serve as an expert witness for the Federal Trade Commission for ground-breaking GLBA Privacy Rule litigation. David has been highly involved in governance at SANS Technology Institute, serving as a member of the Curriculum Committee as well as Audit Curriculum Lead. As a SANS instructor, David has trained security professionals from organizations including NSA, DHHS, Fortune 500 companies, various Department of Defense sites, national laboratories, and many colleges and universities. David is a research fellow for the Center for Cybermedia Research and for the Identity Theft and Financial Fraud Research Operations Center (ITFF/ROC). He also is an adjunct research associate for the UNLV Cybermedia Research Lab and a research fellow with the Internet Forensics Lab. David has written and contributed to more than 15 peer-reviewed books, publications, and journal articles. Currently, David serves as the principal examiner and director of research for Enclave Forensics, a New York/Las Vegas-based incident response and forensics company. He also serves as the chief information security officer for Cyber-Defense, an open-source security software solution provider. In the past, David served as the director of the GIAC Certification program, bringing the GIAC Security Expert certification to life. He holds a BS in IT, Summa Cum Laude, having spent time either attending or consulting for Stony Brook University, Binghamton University, and American Intercontinental University. @david_hoelzer

James Tarala *SANS Senior Instructor*

James Tarala is a principal consultant with Enclave Security and is based out of Venice, Florida. He is a regular speaker and senior instructor with the SANS Institute as well as a courseware author and editor for many SANS auditing and security courses. As a consultant, he has spent the past few years architecting large enterprise IT security and infrastructure architectures, specifically working with many Microsoft-based directory services, e-mail, terminal services, and wireless technologies. He has also spent a large amount of time consulting with organizations to assist them in their security management, operational practices, and regulatory compliance issues, and he often performs independent security audits and assists internal audit groups in developing their internal audit programs. James completed his undergraduate studies at Philadelphia Biblical University and his graduate work at the University of Maryland. He holds numerous professional certifications. @isaudit

Jeff Frisk *SANS Certified Instructor*

Jeff Frisk currently serves as the director of the GIAC certification program and is a member of the STI Curriculum Committee. Jeff holds the PMP certification from the Project Management Institute and GIAC GSEC credentials. He also is the course author for MGT525. He has worked on many projects for SANS and GIAC, including courseware, certification, and exam development. Jeff has an engineering degree from the Rochester Institute of Technology and more than 15 years of IT project management experience with computer systems, high-tech consumer products, and business development initiatives. Jeff has held various positions including managing operations, product development, and electronic systems/computer engineering. He has many years of international and high-tech business experience working with both big and small companies to develop computer hardware/software products and services.

SANS MANAGEMENT FACULTY

Benjamin Wright *SANS Senior Instructor*

Benjamin Wright is the author of several technology law books, including Business Law and Computer Security, published by the SANS Institute. With 26 years in private law practice, he has advised many organizations, large and small, on privacy, e-commerce, computer security, and e-mail discovery, and has been quoted in publications around the globe, from the Wall Street Journal to the Sydney Morning Herald. Mr. Wright is known for spotting and evaluating trends, such as the rise of whistleblowers wielding small video cameras. In 2010, Russian banking authorities tapped him for advice on the law of cyber investigations and electronic payments. @benjaminwright

Lance Spitzner *SANS Certified Instructor*

Lance Spitzner is an internationally recognized leader in the field of cyber threat research and security training and awareness. He has helped develop and implement numerous multi-cultural security awareness programs around the world for organizations as small as 50 employees and as large as 100,000. He invented and developed the concept of honeynets, is the author of several books, and has published over thirty security whitepapers. Mr. Spitzner started his security career with Sun Microsystems as a senior security architect, helping secure Sun's customers around the world. He is founder of the Honeynet Project, an international, non-profit security research organization that captures, analyzes, and shares information on cyber threats at no cost to the public. Mr. Spitzner has spoken to and worked with numerous organizations, including the NSA, FIRST, the Pentagon, the FBI Academy, the President's Telecommunications Advisory Committee, MS-ISAC, the Navy War College, the British CESG, the Department of Justice, and the Monetary Authority of Singapore. Before working in information security, Mr. Spitzner served as an armor officer in the Army's Rapid Deployment Force and earned his MBA from the University of Illinois-Chicago. @lspitzner

G. Mark Hardy *SANS Certified Instructor*

G. Mark Hardy is founder and President of the National Security Corporation. He has been providing cybersecurity expertise to government, military, and commercial clients for over 30 years, and is an internationally recognized expert who has spoken at over 250 events world-wide. He serves on the Advisory Board of CyberWATCH, an Information Assurance/ Information Security Advanced Technology Education Center of the National Science Foundation. A retired U.S. Navy Captain, he was privileged to serve in command nine times, including responsibility for leadership training for 70,000 sailors. He also served as wartime Director, Joint Operations Center for U.S. Pacific Command, and Assistant Director of Technology and Information Management for Naval Logistics in the Pentagon, with responsibility for INFOSEC, Public Key Infrastructure, and Internet Security. Captain Hardy was awarded the Defense Superior Service Medal, the Legion of Merit, five Meritorious Service Medals, and 24 other medals and decorations. A graduate of Northwestern University, he holds a BS in Computer Science, BA in Mathematics, Masters in Business Administration, and a Masters in Strategic Studies, and holds the GSLC, CISSP, CISM, and CISA certifications. @g_mark

Christopher Crowley *SANS Certified Instructor*

Christopher Crowley has 15 years of industry experience managing and securing networks. He currently works as an independent consultant in the Washington, DC area. His work experience includes penetration testing, computer network defense, incident response, and forensic analysis. Mr. Crowley is the course author for SANS Management 535 - Incident Response Team Management and holds the GSEC, GCIA, GCIH (gold), GCFA, GPEN, GREM, GMOB, and CISSP certifications. His teaching experience includes SEC401, SEC503, SEC504, SEC560, SEC575, SEC580, and MGT535; Apache web server administration and configuration; and shell programming. He was awarded the SANS 2009 Local Mentor of the Year Award, which is given to SANS Mentors who excel in leading SANS Mentor Training classes in their local communities. @CCrowMontance

For a complete list of SANS instructors, visit
sans.org/instructors

It's an awesome effort: great questions, excellent material, and presentation throughout the (training event) week. I've really enjoyed it and will recommend it to many. Thank you GIAC/SANS!"
– Nicholas B., GCIH

GIAC
The Highest Standard in Cybersecurity Certification.

Job-Specific, Specialized Focus

Today's cyber attacks are highly sophisticated and exploit specific vulnerabilities. Broad and general InfoSec certifications are no longer enough. Professionals need the specific skills and specialized knowledge required to meet multiple and varied threats. That's why GIAC has more than 30 certifications, each focused on specific job skills and each requiring unmatched and distinct knowledge.

Deep, Real-World Knowledge

Theoretical knowledge is the ultimate security risk. Deep, real-world knowledge and hands-on skills are the only reliable means to reduce security risk. Nothing comes close to a GIAC certification to ensure that this level of real-world knowledge and skill has been mastered.

Most Trusted Certification Design

The design of a certification exam impacts the quality and integrity of a certification. GIAC exam content and question design are developed through a rigorous process led by GIAC's on-staff psychometrician and reviewed by experts in each area. More than 78,000 certifications have been issued since 1999. GIAC certifications meet ANSI standards.

SANS | GIAC

DEEPER KNOWLEDGE. ADVANCED SECURITY.

SANS TRAINING FORMATS

LIVE CLASSROOM TRAINING

Multi-Course Training Events

Live instruction from SANS' top faculty, vendor showcase, bonus evening sessions, and networking with your peers

www.sans.org/security-training/by-location/all

Community SANS

Live Training in Your Local Region with Smaller Class Sizes

www.sans.org/community

Private

Live Training at Your Office Location

www.sans.org/private-training

Mentor

Live Multi-Week Training with a Mentor

www.sans.org/mentor

Summit

Live IT Security Summits and Training

www.sans.org/summit

ONLINE TRAINING

OnDemand

E-learning available anytime, anywhere, at your own pace

www.sans.org/ondemand

vLive

Online, evening courses with SANS' top instructors

www.sans.org/vlive

Simulcast

Attend a SANS training event without leaving home

www.sans.org/simulcast

OnDemand Bundles

Extend your training with an OnDemand Bundle including four months of e-learning www.sans.org/ondemand/bundles