



CYBERSECURITY LEADERSHIP

Courses and Free Resources

sans.org/cybersecurity-leadership

CYBERSECURITY LEADERSHIP

As the threat landscape continues to evolve, cybersecurity has become more valuable to organizations than ever before. Business leaders now understand the importance of securing high-value information assets and the significant risk associated with a breach or attack.

Organizations need cybersecurity leaders and managers who can pair their technical knowledge with essential leadership skills so they can effectively lead projects, teams, and initiatives in support of business objectives.

The Cybersecurity Leadership focus area delivers applicable and practical approaches to managing cyber risk. This series of hands-on, interactive courses helps current and aspiring cybersecurity leaders take their management skills to the level of their technical knowledge.

SANS Cybersecurity Leadership courses will teach you to:

- Develop your management and leadership skills
- Understand and analyze risk
- Create effective cybersecurity policy
- Build a vulnerability management programme
- Develop strategic security plans that incorporate business and organizational goals
- Effectively engage and communicate with key business stakeholders
- Measure the impact of your security programme
- Establish and mature your security culture
- Protect and lead enterprise and cloud environments

“This training applies to all aspects of my job, from network management to project management.”

—David Chaulk, Enbridge

TRAINING & CERTIFICATION

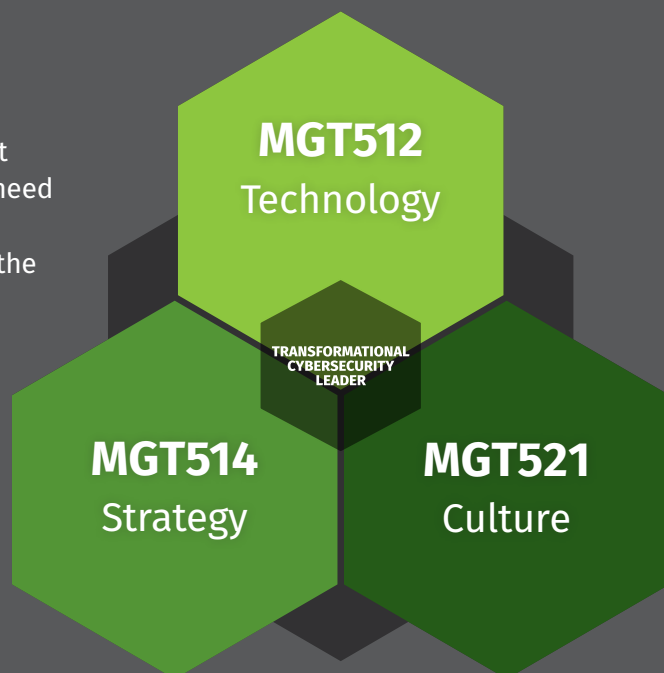
		GIAC CERTIFICATION	PAGE
MGT 512	Security Leadership Essentials for Managers Leading Security Initiatives to Manage Information Risk		7
MGT 514	Security Strategic Planning, Policy, and Leadership Aligning Security Initiatives with Strategy		8
MGT 516	Managing Security Vulnerabilities: Enterprise and Cloud Stop Treating Symptoms – Cure the Disease		9
MGT 520	Leading Cloud Security Design and Implementation Building and Leading a Cloud Security Program		10
MGT 521	Leading Cybersecurity Change: Building a Security-Based Culture Build and Measure a Strong Security Culture to Secure Your Workforce		11
MGT 551	Building and Leading Security Operations Centers Prevent – Detect – Respond People – Process – Technology		12
MGT 553	Cyber Incident Management Open in Case of Emergency		13
SEC 566	Implementing and Auditing Security Frameworks and Controls Building and Auditing Critical Security Controls		14
AUD 507	Auditing & Monitoring Networks, Perimeters, and Systems Controls That Matter – Controls That Work		15
LEG 523	Law of Data Security and Investigations Bridging the Gap Between Legal and Cybersecurity		16
MGT 414	SANS Training Program for the CISSP® Certification Need Training for the CISSP® Exam?		17
MGT 415	A Practical Introduction to Cyber Security Risk Management Cutting Through Academics: Practical Risk management for Cybersecurity		18
MGT 433	Managing Human Risk: Mature Security Awareness Programs People are the Primary Attack Vector. Manage Your Human Risk.		19
MGT 525	Managing Cybersecurity Initiatives & Effective Communication Meet and Exceed Your Security Program's Goals		20
SEC 440	CIS Critical Controls: A Practical Introduction Introduction to Critical Security Controls		21



In an effort to help our students find the right path, SANS Management Curriculum has created two cybersecurity leadership triads that align to help create stronger, more well-rounded cybersecurity leaders.

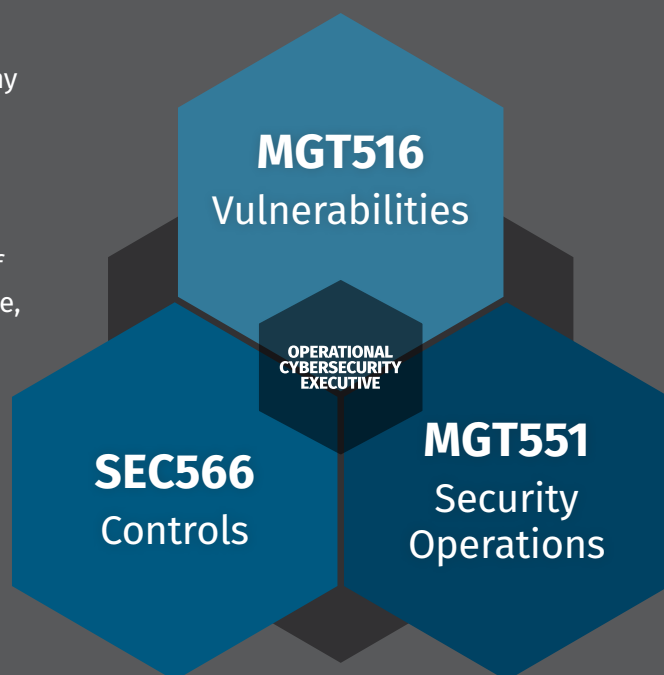
Transformational Cybersecurity Leader

With corporations in need of protecting against an endless and increasing onslaught of information security threats, technology management skills alone are no longer sufficient. Today it is about technology, business strategy, and people. Cybersecurity leaders need to be up to speed on information security issues from a technical standpoint, understand how to implement security planning into the broader business objectives, and be able to build a longer lasting security and risk-based culture. Adjusting employees' and leadership's way of thinking about security in order to prioritise and act to prevent today's most common cybersecurity attacks requires organisational change that affects the foundational culture of the organisation. A transformational cybersecurity leader will be able to strategise and apply concepts, management tools, and methodologies in order to analyse the current situation, identify target state, perform a gap analysis, and develop a comprehensive roadmap that includes employees at all levels of the organisation in every type of job role. The SANS Management Transformational Cybersecurity Leader triad ensures a cyber security manager is proficient in all three key pillars by providing a complete, curated package of education to support you along your path to becoming the strongest cybersecurity leader possible in today's dynamic, online world.



Operational Cybersecurity Executive

As cyber attacks become more common and more expensive, many organisations are making a foundational shift to view operations from the point of view of an adversary, in order to protect their most sensitive information. Despite vulnerability tools and programs being available for several decades, breaches still happen regularly from known vulnerabilities. With a wide range of technologies in use requiring more time and knowledge to manage, a global shortage of cybersecurity talent, an unprecedented migration to cloud, and legal and regulatory compliance often increasing and complicating the matter more, it's no wonder we've seen frustration in the eyes of information assurance engineers, auditors, SOC analysts, and cybersecurity managers who are trying to make a difference in their organisations by better defending their data systems. Some organisations even wonder if they will ever succeed at properly protecting their information. Do not give up! The SANS Operational Cybersecurity Executive triad is here to help you build, grow, and sharpen your cyber defence team!





Cybersecurity Leadership Tabletop Simulation Game

Individuals or teams play to improve the state of security for a fictional organization. Just as in real life, any program has constraints, such as time, money, and resources. Students are required to manage their resources even amongst changing tides and requirements within the organization. They must capitalize on the schedule and available resources to accomplish necessary tasks in a timely and effective manner. Players can interact with one another in order to maximize the results of their program. This type of interactive simulation puts students in real-world scenarios that spur discussion, critical thinking of situations, and melding of different points of view and personalities that they will encounter at work. Just like in the real world, however, unexpected events can arise that delay or even possibly derail a planned strategic initiative. In the game there are multiple events to which players will respond. The decisions that are made in response to these events will alter budgets, time, level of security functions, and ultimately the player's final score.

Cyber42 has seven versions available, each mapping to specific SANS course content:

- **Security Program Capabilities**
MGT512: Security Leadership Essentials for Managers
sans.org/mgt512
- **CISO for a Day**
MGT514: Security Strategic Planning, Policy, and Leadership
sans.org/mgt514
- **Vulnerability Management**
MGT516: Managing Security Vulnerabilities: Enterprise and Cloud
sans.org/mgt516
- **Security Culture**
MGT521: Leading Cybersecurity Change: Building a Security-Based Culture
sans.org/mgt521
- **Security Operations Centers**
MGT551: Building and Leading Security Operations Centers
sans.org/mgt551
- **Industrial Edition**
ICS418: ICS Security Essentials for Managers
sans.org/ics418
- **Ransomware**
MGT512: Security Leadership Essentials for Managers
sans.org/mgt512



"I want to participate again and again. It was just awesome."

—CISO-for-a-Day participant

"I liked how comprehensive the scenarios were. You have to work through several aspects in order to formulate an answer and then get ranked on a number of different facets. The addition of the time constraint to provide your answers is just a nice little bonus of stress but makes it fun. It's good to work through table-top exercises on a management level. Thanks for putting this together."

—Vulnerability Management participant

"Love the scenarios/tabletops and constraints, along with the follow-up discussions around what made each answer the best answer."

—Security Capabilities participant

LEADERSHIP IN CLOUD

ENFORCE 2 FA

If you must have user accounts, enforce Two-Factor Authentication (2 FA) – and make sure your default password policy enforces at least 15 characters.



ENCRYPT

Encrypt everything you have the ability to encrypt: Traffic, Disks, Storage, Containers, Keys, Data... Everything!



DISABLE ACCESS

Disable all public read access on S3 buckets and storage containers of any kind; and if you already did this, go back and double check.



BACKUP

Get Serious about backups; if it's mission critical, it should be backed-up per corporate policy. Did you know: If an adversary has sufficient privilege, a ransomware attack can render your backups unusable?



SANS QUICK WINS IN CLOUD SECURITY

SOME QUICKER
THAN OTHERS

Written by Serge Borso

ENABLE TOOLS

Enable AWS Security Hub or Microsoft Defender for Cloud, and learn how to use these tools to identify weak spots in your implementation.



sans.org/cloud-security
sans.org/sec388
[#SANSCloudAce](https://twitter.com/SANSCloudAce)

Cybersecurity leaders need to stay up-to-date on the latest technologies, such as cloud security, to gain the respect of technical team members, understand what technical staff are actually doing, and appropriately plan and manage security projects and initiatives.

Discover the SANS offerings relevant to cloud security coupled with cybersecurity leadership.

MGT520: Leading Cloud Security Design and Implementation

sans.org/mgt520

SEC388: Introduction to Cloud Computing and Security

sans.org/sec388

MGT512: Security Leadership Essentials for Managers



GSLC
Security Leadership
giac.org/gslc

5
Day Program

30
CPEs

Laptop
Required

You Will Be Able To

- Navigate your organization through the Make sense of different cybersecurity frameworks
- Understand and analyze risk
- Understand the pros and cons of different reporting relationships
- Manage and lead technical teams and projects
- Build a vulnerability management program
- Inject security into modern DevOps workflows
- Strategically leverage a SIEM
- Lead a Security Operations Center (SOC)
- Change behavior and build a security-aware culture
- Effectively manage security projects
- Enable modern security architectures and the cloud
- Build security engineering capabilities using automation and Infrastructure as Code (IaC)
- Get up to speed quickly on information security issues and terminology
- Establish a minimum standard of security knowledge, skills, and abilities
- Speak the same language as technical security professionals

Who Should Attend

- Security Managers
 - Newly appointed information security officers
 - Recently promoted security leaders who want to build a security foundation for leading and building teams
 - Aspiring CISOs
- Security Professionals
 - Technically skilled security administrators who have recently been given leadership responsibilities
 - Team leads with responsibility for a specific security function who want to understand what other teams are doing and broaden their knowledge
- Managers
 - Managers who want to understand what technical people are telling them
 - Leaders who need an understanding of security from a management perspective

Leading Security Initiatives to Manage Information Risk

Take this course to learn the key elements of any modern security program. MGT512 covers a wide range of security topics across the entire security stack. Learn to quickly grasp critical information security issues and terminology, with a focus on security frameworks, security architecture, security engineering, computer/network security, vulnerability management, cryptography, data protection, security awareness, application security, DevSecOps, cloud security, and security operations.

The course uses the **Cyber42 leadership simulation game** to put you in real-world scenarios that spur discussion and critical thinking of situations that you will encounter at work. Throughout the class you will participate in twenty-three Cyber42 activities.

This course will help your organization:

- Develop leaders that know how to build a modern security program
- Anticipate what security capabilities need to be built to enable the business and mitigate threats
- Create higher performing security teams

Hands-On Training

MGT512 uses case scenarios, group discussions, team-based exercises, in-class games, and a security leadership simulation to help students absorb both technical and management topics. About 60–80 minutes per day is dedicated to these learning experiences using the Cyber42 leadership simulation game. This web application based game is a continuous tabletop exercise where students play to improve security culture, manage budget and schedule, and improve security capabilities at a fictional organization. This puts you in real-world scenarios that spur discussion and critical thinking of situations that you will encounter at work.

Course Author Statement

“Technical professionals who are thrust into management roles need to learn how to convey security concepts in ways that non-technical people can understand. At the same time, managers who are new to security need to learn more about the different domains of cybersecurity. In both cases, there is a need to learn about the work of managing security. That is why this course focuses on the big picture of securing the enterprise, from governance all the way to the technical security topics that serve as the foundation for any security manager. Ultimately, the goal of the course is to ensure that you, the advancing manager, can make informed choices to improve security at your organization.”

—Frank Kim



GSLC
Security Leadership
giac.org/gslc

GIAC Security Leadership

The GIAC Security Leadership (GSLC) certification validates a practitioner's understanding of governance and technical controls focused on protecting, detecting, and responding to security issues. GSLC certification holders have demonstrated knowledge of data, network, host, application, and user controls along with key management topics that address the overall security lifecycle.

“I would recommend this course as it is a great intro to both the business and technical aspects of aspiring CISO work.”

—Ian D. U.S. Military

- Cryptography concepts and applications for managers, networking concepts and monitoring for managers
- Managing a security operations center, application security, negotiations and vendors, and program structure
- Managing security architecture, security awareness, security policy, and system security
- Risk management and security frameworks, vulnerability management, incident response and business continuity

MGT514: Security Strategic Planning, Policy, and Leadership



GSTRT
Strategic Planning, Policy
& Leadership
giac.org/gstrt

5
Day Program

30
CPEs

Laptop
Required

You Will Be Able To

- Develop security strategic plans that incorporate business and organizational drivers
- Develop and assess information security policy
- Use management and leadership techniques to motivate and inspire your teams
- Utilize multicloud IAM and cloud Single Sign-On to provide secure access to resources across cloud accounts and providers

Who Should Attend

- CISOs
- Information security officers
- Security directors
- Security managers
- Aspiring security leaders
- Security personnel who have team lead or management responsibilities
- Anyone who wants to go beyond technical skills
- Technical professionals who want to learn to communicate with senior leaders in business terms

“The knowledge gained in class will directly translate to an increased maturity in my organization’s security policy as topics and principles discussed are implemented.”

—Mike Parkin, Chapters Health System

Aligning Security Initiatives with Strategy

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 gives you tools to become a security business leader who can build and execute strategic plans that resonate with other business executives, create effective information security policy, and develop management and leadership skills to better lead, inspire, and motivate your teams.

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. These policies 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.

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.

Hands-On Training

MGT514 uses business case studies, fictional companies, and the Cyber42 leadership simulation game to put you in real-world scenarios that spur discussion and critical thinking of situations that you will encounter at work. This web application-based game is a continuous tabletop exercise where students play to improve security culture, manage budget and schedule, and improve security capabilities at a fictional organization. This puts you in real-world scenarios that spur discussion and critical thinking of situations that you will encounter at work.

The course also uses case studies from Harvard Business School, case scenarios, team-based exercises, and discussions that put students in real-world situations. You will be able to use these same activities with your own team members at work.



GSTRT
Strategic Planning,
Policy & Leadership
giac.org/gstrt

GIAC Strategic Planning, Policy, and Leadership

The GIAC Strategic Planning, Policy, and Leadership (GSTRT) certification validates a practitioner’s understanding of developing and maintaining cyber security programs as well as proven business analysis, strategic planning, and management tools. GSTRT certification holders have demonstrated their knowledge of building and managing cyber security programs with an eye towards meeting the needs of the business, board members, and executives.

- Business and Threat Analysis
- Security Programs and Security Policy
- Effective Leadership and Communications

“This course is great content for leaders within the field. It pushes people to stop always focusing on the technical aspects of cybersecurity and really understand what the business needs from its security function as a whole to enable the business”

—Alexander Walker, TechVets

MGT516: Managing Security Vulnerabilities: Enterprise and Cloud

5
Day Program

30
CPEs

Laptop
Required

You Will Be Able To

- Create, implement, or mature your vulnerability management program and get buy-in from your stakeholders
- Implement techniques for building and maintaining an accurate and useful inventory of IT assets in the enterprise and the cloud
- Identify processes and technologies that are effective across both infrastructure and applications and how to configure them appropriately
- Identify which common false positives or false negatives to be aware of in your identification arsenal
- Know how to prioritize unblocked vulnerabilities for treatment based on a variety of techniques
- Effectively report and communicate vulnerability data within your organization
- Identify and report on the risk associated with vulnerabilities that are blocked and cannot currently be prioritized for remediation
- Have a better understanding of modern treatment capabilities and how to better engage with treatment teams
- Make vulnerability management more fun and engaging for all those involved
- Differentiate how to deal with application layer vulnerabilities versus infrastructure vulnerabilities
- Have an understanding of how our strategies and techniques might change as we move to the cloud, implement private cloud, or roll out DevOps within our organizations

Who Should Attend

- CISOs
- Vulnerability program managers and analysts managing vulnerabilities in the enterprise or cloud
- Information security managers, architects, analysts, officers, and directors
- Aspiring information security leaders
- Risk management, business continuity and disaster recovery professionals
- IT operations managers and administrators
- Cloud service managers, administrators, integrators, developers, and brokers
- Cloud service security and risk managers
- Government IT professionals who manage vulnerabilities in the enterprise or cloud (FedRAMP, NIST CSF)

Stop Treating Symptoms. Cure The Disease.

Whether your vulnerability management program is well established or you are just getting started, this course will help you think differently about vulnerability management. You will learn how to move past the hype to successfully prioritize the vulnerabilities that are not blocked, then clearly and effectively communicate the risk associated with the rest of the vulnerabilities in your backlog that, for a variety of reasons, cannot currently be remediated. You'll also learn what mature organizations are doing to ease the burden associated with vulnerability management across both infrastructure and applications as well as across both their cloud and non-cloud environments. MGT516 is based on the Prepare, Identify, Analyze, Communicate, and Treat (PIACT) Model.

MGT516 helps you think strategically about vulnerability management in order to mature your organization's program, but it also provides tactical guidance to help you overcome common challenges. By understanding and discussing solutions to typical issues that many organizations face across both traditional and cloud operating environments, you will be better prepared to meet the challenges of today and tomorrow. Knowing that many organizations are adopting cloud services in addition to continuing to manage their more traditional operating environments, we'll also look at different cloud service types throughout the course and how they impact the program both positively and negatively. We will highlight some of the tools and processes that can be leveraged in each of these environments and present new and emerging trends.

Business Takeaways

This course will help your organization:

- Understand what is working and what is not working in modern day vulnerability programs
- Anticipate and plan for the impacts related to cloud operating environments
- Realize why context matters and how to gather, store, maintain, and utilize contextual data effectively
- Effectively and efficiently communicate vulnerability data and its associated risk to key stakeholders
- Determine how to group vulnerabilities meaningfully to identify current obstacles or deficiencies
- Know which metrics will drive greater adoption and change within the organization

"A great course to utilize if new to cloud vulnerability management."

—Amaan Mughal

"Excellent labs. More fun than I thought possible with vulnerability management."

—Page Jeffery, Newmont

MGT520: Leading Cloud Security Design and Implementation

5
Day Program

30
CPEs

Laptop
Required

You Will Be Able To

- Define a strategy for securing a workload in the cloud for medium-size and large enterprises that can support their business objectives
- Establish a security roadmap based on the security strategy that can support a fast-paced cloud adoption and migration path while maintaining a high degree of security assurance
- Understand the security basics of the cloud environment across different types of service offerings, then explain and justify to other stakeholders the decisions within the security roadmap
- Build an effective plan to mature a cloud security posture over time, leveraging security capabilities offered by cloud providers to leapfrog in security capabilities
- Explain the security vision of the organization in the cloud domain to your Board Directors and executives, collaborate with your peers, and engage your workforce, driving the security culture change required for the cloud transformation

Who Should Attend

The primary target audience for this course is managers and directors who are in a position to lead or make key decisions on the IT transformation to cloud environments.

Prerequisites

Students should have three to five years of experience in IT and/or cybersecurity. This course covers the core areas of security leadership in migrating workloads to the cloud environment and assumes a basic understanding of technology, networks, and security.

Notice to Students

This course will have limited overlap with the SANS SEC488: Cloud Security Essentials course because it will provide foundational information on cloud services and cloud security to ensure that students are on the same page. This course focuses on what managers, directors, and security leaders need to know about developing their cloud security plan/roadmap and managing implementation of cloud security capabilities.

Aligning Security Initiatives with Strategy

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 gives you tools to become a security business leader who can build and execute strategic plans that resonate with other business executives, create effective information security policy, and develop management and leadership skills to better lead, inspire, and motivate your teams.

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. These policies 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.

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.

Hands-On Training

MGT514 uses business case studies, fictional companies, and the Cyber42 leadership simulation game to put you in real-world scenarios that spur discussion and critical thinking of situations that you will encounter at work. This web application-based game is a continuous tabletop exercise where students play to improve security culture, manage budget and schedule, and improve security capabilities at a fictional organization. This puts you in real-world scenarios that spur discussion and critical thinking of situations that you will encounter at work.

The course also uses case studies from Harvard Business School, case scenarios, team-based exercises, and discussions that put students in real-world situations. You will be able to use these same activities with your own team members at work.

“This type of training, i.e., cloud security from a management perspective, is rare and the quality of this one is definitely amazing.”

—Benoit Ramillon, UEFA

“I feel like there was a lot of valuable material and would be very relevant for people creating a cloud security program.”

—Jeff Henderson

MGT521: Leading Cybersecurity Change: Building a Security-Based Culture

5
Day Program

30
CPEs

Laptop
Not Needed

You Will Be Able To

- More effectively communicate the business value of cybersecurity to your Board of Directors and executives, improve collaborate with your peers, and more effectively engage your workforce
- Explain what organizational culture is, its importance to cybersecurity, and how to map and measure both your organization's overall culture and security culture
- Align your cybersecurity culture to your organization's strategy, including how to leverage different security frameworks and maturity models
- Explain what organizational change is, identify different models for creating change, and learn how to apply those models
- Enable and secure your workforce by integrating cybersecurity into all aspects of your organization's culture
- Dramatically improve both the effectiveness and impact of your security initiatives, such as DevSecOps, Cloud migration, Vulnerability Management, Security Operations Center and other related security deployments
- Create and effectively communicate business cases to leadership and gain their support for your security initiatives
- How to measure your security culture and how to present the impact of a strong security culture to leadership
- Leverage numerous templates and resources from the Digital Download Package and Community Forum that are part of the course and which you can then build on right away

Who Should Attend

- Chief information security officers
- Chief risk officers/Risk management leaders
- Security awareness/Engagement managers
- Senior security managers who lead large-scale security Initiatives
- Information security managers, officers, and directors
- Information security architects and consultants
- Aspiring information security leaders
- Business continuity/Disaster recover leaders
- Privacy/Ethics officers

Build and Measure a Strong Security Culture

Drawing on real-world lessons from around the world, the SANS MGT521 course will teach you how to leverage the principles of organizational change in order to develop, maintain, and measure a security-driven culture. Through hands-on instruction and a series of interactive labs and exercises, you will apply these concepts to a variety of different real-world security initiatives and quickly learn how to embed cybersecurity into your organization's culture immediately.

Apply findings from Daniel Kahneman's Nobel prize-winning research, Thayer and Sunstein's Nudge Theory, and Simon Sinek's Golden Circle. Learn how Spock, Homer Simpson, the Elephant and Rider and the Curse of Knowledge all are keys to building a strong cybersecurity culture at your company.

Business Takeaways

- Create a far more secure workforce, both in their attitudes about cybersecurity and also in employee behaviors
- Enable the security team to create far stronger partnerships with departments and regions throughout the organization
- Dramatically improve the ROI of cybersecurity initiatives and projects through increased success and impact
- Improve communication between the cybersecurity team and business leaders
- Create stronger and more positive attitudes, perceptions and beliefs about the cybersecurity team

Hands-On Training

This five-section course includes 16 interactive labs that walk you through exercises and apply the lessons learned to a variety of typical real-world security situations and challenges. Many of the labs are carried out as teams, ensuring that you learn not only from the course materials but from other students and their experiences. Finally, the last section is a capstone event as you work through a series of case studies to see which team can create the strongest security culture. Culture is a very human and global challenge, and as such we want to expose you to as many different situations and perspectives as possible.

Notice to Students

The course is recommended for more senior and/or more experienced cybersecurity managers, officers, and awareness professionals. If you are new to cybersecurity, we recommend some of SANS's more basic courses, such as SEC301, SEC401, or MGT433.

"I am so happy with this material focusing on embedding secure values into our global culture – exactly what my company needs help with NOW."

—Lindsay O'Bannon, Deloitte Global

"Lance was fantastic! He made the course super engaging and covered all information thoroughly, making sure to draw in and leverage student experience to make the course richer."

—Anna Troutman

MGT551: Building and Leading Security Operations Centers



GSOM
Security Operations
Manager
giac.org/gsom

5
Day Program

30
CPEs

Laptop
Required

You Will Be Able To

- Collect the most important logs and network data
- Build, train, and empower a diverse team
- Create playbooks and manage detection use cases
- Use threat intelligence to focus your budget and detection efforts
- Utilize threat hunting and active defense strategies
- Implement efficient alert triage and investigation workflow
- Implement effective incident response planning and execution
- Choose metrics and a long-term strategy to improve the SOC
- Implement team member training, retention, and prevention of burnout
- Understand SOC assessment through capacity planning, purple team testing, and adversary emulation

Who Should Attend

This course is intended for those who are looking to build a Security Operations Center for the first time or improve the one their organization is already running.

Ideal student job roles for this course include:

- Security Operations Center managers or leads
- Security directors
- New Security Operations team members
- Lead/senior SOC analysts
- Technical CISOs and security directors

“A ton of useful things I will take back and use starting Monday. This week I learned more than I could have learned in months on my own.”

—Zac Scholl, Zendesk

Managers must show alignment to the business and demonstrate real value – a challenge when the threats are constantly changing and sometimes unseen. Managing a security operations center (SOC) requires a unique combination of technical knowledge, management skills, and leadership ability. MGT551 bridges gaps by giving students the technical means to build an effective defense and the management tools to build an effective team. Common questions SOC leaders face are:

- How do we know our security teams are aligned to the unique threats facing our organization?
- How do we get consistent results and prove that we can identify and respond to threats in time to minimize business impact?
- How can we build an empowering, learning environment where analysts can be creative and solve problems while focusing on the mission at hand?

Whether you are looking to build a new SOC or take your current team to the next level, MGT551 will super-charge your people, tools, and processes. Each section of MGT551 is packed with hands-on labs and introductions to some of the industry's best free and open source tools, and each day concludes with Cyber42 SOC leadership simulation exercises. Students will learn how to combine SOC staff, processes, and technology in a way that promotes measurable results and covers all manner of infrastructure and business processes. Most importantly, students will learn how to keep the SOC growing, evolving, and improving over time.

Business Takeaways

- Strategies for aligning cyber defense to organizational goals
- Tools and techniques for validating security tools and processes
- Methodologies for recruiting, hiring, training, and retaining talented defenders and effective management and leadership techniques for technical teams
- Practical approaches to optimising security operations that can be applied immediately

Hands-On Training

While this course is focused on management and leadership, it is by no means limited to non-technical processes and theory. The course uses the Cyber42 interactive leadership simulation game to put you in real-world scenarios that spur discussion and critical thinking of situations that you will encounter at work. Throughout the five days of instruction, students will work on fifteen hands-on exercises covering everything from playbook implementation to use case database creation, attack and detection capability prioritisation and visualisation, and purple team planning, threat hunting, and reporting. Attendees will leave with a framework for understanding where their SOC should be focusing its efforts, how to track and organize defensive capabilities, and how to drive, verify, and communicate SOC improvements.



GSOM
Security Operations
Manager
giac.org/gsom

GIAC Security Operations Manager

The GSOM certification validates a professional's ability to run an effective security operations center. GSOM-certified professionals are well-versed in the management skills and process frameworks needed to strategically operate and improve a SOC and its team.

- Designing, planning, and managing an effective SOC program
- Prioritisation and collection of logs, development of alert use cases, and response playbook generation
- Selecting metrics, analytics, and long-term strategy to assess and continuously improve SOC operations

2
Day Course

12
CPEs

Laptop
Not Needed

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 their own organization

Who Should Attend

- Security managers
 - Newly appointed information security officers who will be leading incidents
 - Recently promoted security leaders who want to understand incident management better
- Security Professionals
 - Technically skilled security staff who have recently been given incident commander responsibilities
 - Team leads with responsibility to support cyber incidents and who may need to remediate systems
- Managers
 - Managers who want to understand how to manage technical people during an incident
 - Leaders who need an understanding of cyber incidents from a management perspective
- Legal/HR/PR staff
 - Staff who are new to cyber incident management but may be called upon to provide critical support in tense situations and who want to understand better what may be expected from them

Open in Case of Emergency

You can't predict or pick when your organization will face a major cyber incident, but you can choose how prepared you are when you face it. While there are broad technical aspects to cyber incidents there is also a myriad of other activities that generally falls to executives, managers, legal, press, and human relations staff. These include communicating both internally and externally, considering the battle rhythm and a look at methodologies for tracking information gathered and released to the public.

This course empowers you to become an effective incident management team member or leader; ensuring you fully understand the different issues facing incident commanders in the immediate, short and medium term. As well as becoming comfortable with terminology, you will understand what preparatory work you can undertake at different stages to help you get ahead of the situation. MGT553 was developed to ensure efficient management of a diverse range of incidents with a focus on cyber; however, the methodology, concepts and guidance will apply to many regular major and critical incidents.

This course will help your organization:

- Develop staff that know how to lead or contribute to a cyber incident management team
- Manage your incidents more effectively and thus resolve them quicker
- Understand the gaps in your security incident plans and response strategies
- Create higher performing security teams

Author Statement

"Of my 28 years in cyber security, I've spent over 11 of them in incident response and later incident management. During that time, I've seen a wide range of approaches to handling cyber incidents, some good and others less so. One common issue was that most people on the Incident team had never been part of a major incident and thus they lacked confidence, forward planning, and were easily stunned when the incident took a turn they had not predicted.

"This course is designed to demystify incident management, to provide attendees with a framework to not only deal with the matters at hand, but also to plan for the subsequent phases, so they are technically ready and mentally prepared. Cyber incidents, such as ransomware, can be devastating, not only to the networks, but also the team charged with investigating, mitigating, reporting and remediating the damage. In addition to the core incident management aspects, we cover the mental health of the team, the operational tempo and how to spot people suffering under pressure. I believe that this course, enriched with the anecdotes of the SANS incident response instructors' own toe-curling incidents will prepare your team for anything attackers and bots throw at them. When you are prepared and ready, you can respond better, faster and get control of the situation quicker facilitating a rapid return to business as usual."

—Steve Armstrong

"Brilliant insight. Excellent content. An absolute must course for anyone dealing with incident management."

—Gary Smith

"All was very relevant and well delivered. All extremely useful information."

—Peter Leonhardt

SEC566: Implementing and Auditing Security Frameworks and Controls



GIACC
Critical Controls
giac.org/gccc

5
Day Program

30
CPEs

Laptop
Required

You Will Be Able To

- Apply a security framework based on actual threats that is measurable, scalable, and reliable in stopping known attacks and protecting organizations' important information and systems
- Understand the importance of each control and how it is compromised if ignored, and explain the defensive goals that result in quick wins and increased visibility of networks and systems
- Identify and utilize tools that implement controls through automation
- Create a scoring tool to measure the effectiveness of each controls the effectiveness of each control
- Employ specific metrics to establish a baseline and measure the effectiveness of security controls
- Competently map critical controls to standards such as the NIST Cybersecurity Framework, NIST SP 800-171, the CMMC, and more
- Audit each of the CIS Critical Controls, with specific, proven templates, checklists, and scripts provided to facilitate the audit process

Who Should Attend

- Information assurance auditors
- System implementers or administrators
- Network security engineers
- IT administrators
- Department of Defense personnel and contractors
- Staff and clients of federal agencies
- Private sector organizations looking to improve information assurance processes and secure their systems
- Security vendors and consulting groups looking to stay current with frameworks for information assurance
- Alumni of SEC440, MGT516, MGT551, MGT512, SEC401, and SEC501

Prioritising defenses to stop attacks with the appropriate cyber controls.

In addition to defending their information systems, many organizations have to comply with a number of cybersecurity standards and requirements as a prerequisite for doing business. Dozens of cybersecurity standards exist throughout the world and most organizations must comply with more than one such standard. As threats and attack surfaces change and evolve, an organization's security should as well. To enable your organization to stay on top of this ever-changing threat scenario, SANS has mapped the most commonly utilized cybersecurity frameworks into one comprehensive, comparative approach that enables organizations to streamline efforts and assets to properly defend their networks while meeting required standards.

SEC566 will enable you to master the specific and proven techniques and tools needed to implement and audit the controls defined in the Center for Internet Security's CIS Controls (v71/8.0), the NIST Cybersecurity Framework (CSF), the Cybersecurity Maturity Model Certification (CMMC), ISO/IEC 27000, and many other common industry standards and frameworks. Students will learn how to merge these various standards into a cohesive strategy to defend their organization and comply with industry standards. SANS' in-depth, hands-on training will teach security practitioners to 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. SEC566 shows security professionals how to implement the controls in an existing network through cost-effective automation. For auditors, CIOs, and risk officers, this course is the best way to understand how you will measure whether their cybersecurity controls are effectively implemented.

Business Takeaways

- Maximize compliance analyst's time in mapping frameworks by learning a comprehensive controls matrix
- Reduce duplicate efforts of administrators implementing cybersecurity controls from different standards and frameworks
- Enjoy peace of mind that your organization has a comprehensive strategy for defense and compliance
- Report the status of cybersecurity defense efforts to senior leadership in clear terms

"Loved this course. It provides a method of measuring your security posture and applying the concept to any organization."

—John M., U.S. Military



GIACC
Critical Controls
giac.org/gccc

GIAC Critical Controls Certification

The GIAC Critical Controls Certification is the only certification based on the Critical Security Controls, a prioritized, risk-based approach to security. This certification ensures that candidates have the knowledge and skills to implement and execute the Critical Security Controls recommended by the Council on Cybersecurity, and perform audits based on the standard.

- Background, purpose, and implementation of the CIS Critical Controls
- Account monitoring, application software security, boundary defense, and controlled use of administrative privileges and need-to-know access
- Data protection and data recovery capability; email and web browser protections; inventory and control of hardware and software assets; and limitation and control of network ports
- Maintenance, monitoring, and analysis of audit logs; secure configurations for hardware, software, and network devices; and wireless access control

AUD507: Auditing & Monitoring Networks, Perimeters, and Systems



GSNA
Systems and
Network Auditor
giac.org/gsna

6
Day Program

36
CPEs

Laptop
Required

You Will Be Able To

- Apply risk-based decision making to the task of auditing enterprise security
- Understand the different types of controls (e.g., technical vs. non-technical) essential to performing a successful audit
- Conduct a proper risk assessment of an enterprise to identify vulnerabilities and develop audit priorities
- Establish a well-secured baseline for computers and networks as a standard to conduct audit against
- Perform a network and perimeter audit using a repeatable process
- Audit virtualisation hosts and container environments to ensure proper deployment and configuration
- Utilize vulnerability assessment tools effectively to provide management with the continuous remediation information necessary to make informed decisions about risk and resources
- Audit a web application's configuration, authentication, and session management to identify vulnerabilities attackers can exploit
- Utilize scripting to build a system which will baseline and automatically audit Active Directory and all systems in a Windows domain
- Utilize scripting to build a system which will baseline and automatically audit Linux systems

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
- Anyone looking to implement effective continuous monitoring processes within the enterprise

Controls That Matter – Controls That Work

This course 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 practices, students will have the opportunity to delve into the technical “how-to” for determining the key controls that can be used to provide a high level of assurance to an organization. Real-world examples provide students with tips on how to verify these controls in a repeatable way, as well as many techniques for continuous monitoring and automatic compliance validation. These same real-world examples help the students learn how to be most effective in communicating risk to management and operations staff.

Students will leave the course with the know-how to perform effective tests of enterprise security in a variety of areas. The combination of high-quality course content, provided audit checklists, in-depth discussion of common audit challenges and solutions, and ample opportunities to hone their skills in the lab provides a unique setting for students to learn how to be an effective enterprise auditor.

Business Takeaways

- Gain confidence in whether you have the correct security controls and they are working well
- Lower your audit costs with effective, efficient security audits
- Improve relevance of IT audit reporting, allowing the organization to focus on what really matters
- Improve security compliance while reducing compliance and security risks, protecting your reputation and bottom line

“AUD507 has obvious practical applications, and it’s great to see some of the most infamous hacking methods explained and executed in real time. In the labs, I’m getting hands-on experience with the tools. The opportunity to learn how to interpret the results taught me more in one afternoon than I’ve picked up here-and-there over an entire career.”

—Tyler Messa, AWS



GSNA
Systems and Network Auditor
giac.org/gsna

GIAC Systems and Network Auditor

The GIAC Systems and Network Auditor (GSNA) certification validates a practitioner’s ability to apply basic risk analysis techniques and to conduct technical audits of essential information systems. GSNA certification holders have demonstrated knowledge of network, perimeter, and application auditing as well as risk assessment and reporting.

- Auditing, risk assessments, and reporting
- Network and perimeter auditing and monitoring, web application auditing
- Auditing and monitoring in windows and Unix environments



5
Day Program

30
CPEs

Laptop
Not Needed

You Will Be Able To

- Work better with other professionals at your organization who make decisions about the law of data security and investigations
- Exercise better judgment on how to comply with privacy and technology regulations, both in the United States and in other countries
- Evaluate the role and meaning of contracts for technology, including services, software, and outsourcing
- Help your organization better explain its conduct to the public and to legal authorities
- Anticipate cyber law risks before they get out of control
- Implement practical steps to cope with technology law risk
- Better explain to executives what your organization should do to comply with information security and privacy law
- Better evaluate technologies, such as digital archives and signatures, to comply with the law and serve as evidence
- Make better use of electronic contracting techniques to get the best terms and conditions
- Exercise critical thinking to understand the practical implications of technology laws and industry standards (such as the Payment Card Industry Data Security Standard).

Who Should Attend

- Investigators
- Security and IT professionals
- Lawyers
- Staff at government regulatory agencies
- Auditors
- Insider threat analysts
- Technology managers
- Vendors
- Compliance officers
- Law enforcement personnel
- Privacy officers
- Penetration testers
- Cyber incident and emergency responders around the world (including private sector, law enforcement, national guard, and civil defense, among others)

LEG523 is constantly updated to address changing trends and current events, including:

- Supply chain terms and conditions
- The rising influence of the European Union's General Data Protection Regulation (GDPR) in interpretation of cybersecurity law in the United States and around the world
- Understanding cyber insurance for a ransomware event
- Facing a cyber crisis? Filing a lawsuit in the courts of another country
- The arrest and criminal indictment of two Coalfire penetration testers in Iowa
- How to balance the right to data privacy versus the right to data security under GDPR and the new California Consumer Privacy Act
- Adopt peer review of cybersecurity program to better evidence legal compliance
- Video demonstration of how technical expert witnesses can handle adversarial cross-examination in a live online court hearing
- Creative insertion of terms, comments, and conditions in blockchain to influence commercial relationships such as contracts for technology services
- How to make better legal records of digital assets and trading platforms

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 cybersecurity team. SANS LEG523 provides this unique professional training, including skills in the analysis and use of contracts, policies, and insurance security questionnaires.

This course covers the law of crime, policy, contracts, liability, compliance, cybersecurity, and active defense – 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 Global Information Assurance Certification (GLEG) associated with LEG523 demonstrates to employers that you have absorbed the sophisticated content of this course and are ready to put it to use. This coveted GIAC certification distinguishes any professional – whether a cybersecurity specialist, auditor, lawyer, or forensics expert – from the rest of the pack. It also strengthens the credibility of forensics investigators as witnesses in court and can help a forensics consultant win more business. And the value of the certification will only grow in the years to come as law and security issues become even more interconnected.

The course also provides training and continuing education for many compliance programs under information security and privacy mandates such as GLBA, HIPAA, FISMA, GDPR, and PCI-DSS.

Each successive section of this course builds upon lessons from the earlier sections in order to comprehensively strengthen your ability to help your public or private sector enterprise cope with illegal hackers, botnets, malware, phishing, unruly vendors, data leakage, industrial spies, rogue or uncooperative employees, or bad publicity connected with cybersecurity. We cover topical stories, such as Home Depot's legal and public statements about its payment card breach and lawsuits against QSA security vendor Trustwave filed by cyber insurance companies and credit card issuers (third parties with which Trustwave had no relationship!).

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. Professionals from outside the United States 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.

One thing that sets this course apart is its emphasis on ethics. The course teaches practical lessons on ethical performance by cyber defenders and digital investigators.

MGT414: SANS Training Program for CISSP® Certification



GISP
Information Security
Professional
giac.org/gisp

6
Day Program

52
CPEs

Laptop
Not Needed

You Will Be Able To

- Understand the eight 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 eight domains of knowledge
- Apply the skills learned across the eight domains to solve security problems when you return to work

What You Will Receive

- Electronic courseware for each of the eight domains
- 320 questions to test knowledge and preparation for each domain
- MP3 audio files of the complete course lectures

Who Should Attend

- Security professionals who are interested in understanding the concepts covered on the CISSP® exam as determined by (ISC)²
- Managers who want to understand the critical areas of information security
- System, security, and network administrators who want to understand the pragmatic applications of the CISSP® eight domains
- Security professionals and managers looking for practical ways the eight domains of knowledge can be applied to their current job

“This course really pulls a lot together for me and it has been hugely valuable. I know parts of this are going to impact my approach to my work from the first day back.”

—Merewyn Boak, Apple

Need training for the CISSP® exam?

SANS MGT414: SANS Training Program for CISSP® Certification is an accelerated review course that is specifically designed to prepare students to successfully pass the Certified Information Systems Security Professional (CISSP®) exam.

MGT414 focuses solely on the eight domains of knowledge as determined by (ISC)² that form a critical part of the CISSP® exam. 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 completing the course, students will have:

- Detailed coverage of the eight domains of knowledge
- The analytical skills required to pass the CISSP® exam
- The technical skills required to understand each question
- The foundational information needed to become a Certified Information Systems Security Professional (CISSP®)

External Product Notice:

The CISSP® exam itself is not hosted by SANS. You will need to make separate arrangements to take the CISSP® exam. Please note as well that the GISP exam offered by GIAC is NOT the same as the CISSP® exam offered by (ISC)².

Course Authors' Statement

“The CISSP® certification has been around for nearly 25 years. The exam is designed to test your understanding of the Common Body of Knowledge, which may be thought of as the universal language of information security professionals. It is often said to be a mile wide and two inches deep. The CISSP® exam covers a lot of theoretical information that is critical for a security professional to understand. However, this material can be dry, and since most students do not see the direct applicability to their jobs, they find it boring. The goal of this course is to bring the eight domains of knowledge of the CISSP® to life. The practical workings of this information can be discovered by explaining important topics with stories, examples, and case studies. We challenge you to attend the SANS CISSP® training course and find the exciting aspect of the eight domains of knowledge!”

—Eric Conrad and Seth Misenar



GISP
Information Security
Professional
giac.org/gisp

GIAC Information Security Professional

The GIAC Information Security Professional (GISP) certification validates a practitioner's knowledge of the eight domains of cybersecurity knowledge as determined by (ISC)² that form a critical part of CISSP® exam. GISP certification holders will be able to demonstrate knowledge of asset security, communications and network security, identity and access management, security and risk management, security assessment and testing, security engineering, security operation, and software development security.

- Asset Security
- Communications and Network Security
- Identity and Access Management
- Security and Risk Management
- Security Assessment and Testing
- Security Engineering
- Security Operation
- Software Development Security

MGT415: A Practical Introduction to Cyber Security Risk Management

2
Day Course

12
CPEs

Laptop
Required

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 their own organization

Who Should Attend

- Any security engineers, compliance directors, managers, auditors – basically any SANS alumni potentially
- Auditors
- Directors of security compliance
- Information assurance management
- System administrators

What You Will Receive

- Electronic Courseware for learning how to perform risk management
- A unique course spreadsheet tool for performing risk management
- Open source tools for performing risk management
- MP3 audio files of the complete course lecture

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

Author Statement

Most every time we talk with an organization, whether that be a private company or a government agency, we meet people who want to use risk assessment as a tool, but are not actually using it as they could. No organization has enough resources to do everything they would like to defend themselves. At some point a priority decision has to be made. We either make those decisions individually based on whatever need seems to be the most pressing in from of us today, or we take a methodical approach, getting as much input from the business as possible. Risk management is the tool we have available for taking the methodical path.

This course has been written with practicality and usability in mind. Risk models and learning ALE to pass a certification test is fine. But to defend our systems, we need practical skills in risk assessment. This course will teach students the hands-on skills necessary to immediately start using risk assessment as a tool to defend their organization.

– James & Kelli Tarala

“Excellent introduction to the area of risk assessment.”

—Ernie H., U.S. Military

Section Descriptions

SECTION 1: A Practical Introduction to Assessing Cyber Security Risk

TOPICS: Understanding Risk; How to Perform a Simple Risk Assessment; Risk Assessment Case Study; Formal Risk Management Models & Tools

SECTION 2: A Practical Introduction to Managing Cyber Security Risk

TOPICS: Control Focused Risk Management; Event Focused Risk Management; Presenting Risk to Business Owners; Risk Remediation & Response; Tracking Long Term Risk

MGT433: Managing Human Risk: Mature Security Awareness Programs



SSAP
Security Awareness
Professional
giac.org/ssap

2
Day Course

12
CPEs

Laptop
Not Needed

You Will Be Able To

- Understand the Security Awareness Maturity Model and how to leverage it as the roadmap for your awareness program
- Implement key models for learning theory, behavioral change, and cultural analysis
- Explain the difference between awareness, education, and training
- Identify the maturity level of your existing awareness program and the steps to take it to the next level
- Ensure compliance with key standards and regulations
- Define human risk and explain the three different variables that constitute it
- Explain risk assessment processes
- Leverage the latest in Cyber Threat Intelligence and describe the most common tactics, techniques, and procedures used in today's human-based attacks
- Identify, measure, and prioritize your human risks and define the behaviors that manage those risks
- Measure the impact of your awareness program, track reduction in human risk, and communicate the program's value to leadership

Who Should Attend

- Security awareness/communication officers
- Chief security officers, risk officers and security management officials
- Security auditors, and governance, legal, privacy or compliance officers
- Training, human resources and communications staff
- Representatives from organizations regulated by industries such as HIPAA, GDPR, FISMA, FERPA, PCI-DSS, ISO/IEC 27001 SOX, NERC, or any other compliance-driven standard
- Anyone involved in planning, deploying or maintaining a security education, training or communications program

People are the primary attack vector. Manage your human risk.

Learn the key lessons and the roadmap to build a mature awareness program that your workforce will love and that has an impact you can measure. Apply models such as the BJ Fogg Behavior Model, AIDA Marketing funnel, and Golden Circle, and learn about the Elephant vs. the Rider.

The 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. Finally, through a series of labs and exercises, you will develop your own custom plan to implement as soon as you return to your organization.

Business Takeaways:

- Align your security awareness program with your organization's strategic security priorities
- Effectively identify, prioritize and manage your organization's top human risks.
- More closely integrate your security awareness efforts with your security team's overall risk management efforts.
- Make the most of your investment by sustaining your security awareness program long term, going beyond changing behavior to changing culture

Hands-On Training:

A big part of the course is not only learning but applying what you learn working as groups with your peers. Not only does this provide you a far better understanding and application of course content, but enables you to interact and learn from others. This two-day course has five labs. Each lab is approximately 20–30 minutes to complete as a team, with another 20–30 minutes of group discussion, for a total time of three to four hours.

- Lab 1:** Read, analyze and identify the top human risks based on the Verizon Bata Breach Investigations Report
- Lab 2:** Review, identify and prioritize the top human risks in your organization.
- Lab 3:** Identify and document the top behaviors (learning objectives) that manage those risks.
- Lab 4:** Leverage the AIDA marketing model to engage and communicate to your workforce about a new tool roll-out.
- Lab 5:** Create a strategic engagement plan on how you will effectively communicate to and engage your workforce to manage a specific human risk

“Soup to nuts, this course covers the entire designing, building, deploying, and measuring of an effective security awareness program.”

—Chris Sorensen, GE Capital



SSAP
Security Awareness
Professional
giac.org/ssap

SANS Security Awareness Professional

Organizations seek proven leaders who have the expertise and skills to effectively manage and measure human risk. The SANS Security Awareness Professional (SSAP) provides not only this expertise, but also signifies, documents and certifies that the holder has met the requirements to elevate the overall security behavior of the workforce.

The first step to achieving your SSAP is taking the two-day SANS MGT433 course on building mature awareness programs.

MGT525: Managing Cybersecurity Initiatives and Effective Communication



GCPM
Project Manager
giac.org/gcpm

5
Day Program

30
CPEs

Laptop
Required

You Will Be Able To

- Understand predictive/waterfall, adaptive/agile development approaches and how they interact with product and project life cycles.
- Learn how to use and implement lean/agile tools, complexity models, root cause analysis
- Recognize the top failure mechanisms related to security projects, so that your projects can avoid common pitfalls
- Create a project charter which increases stakeholder engagement
- Document project requirements and create requirements traceability matrix to track changes throughout the project lifecycle
- Clearly define the scope of a project in terms of cost, schedule, and technical deliverables
- Develop a project schedule, including critical path tasks and milestones
- Cultivate user stories to drive adaptive sprint cycles
- Create accurate project cost and time estimates
- Develop planned and earned value metrics for your project deliverables and automate reporting functions
- Effectively manage conflict situations and build communication skills with your project team
- Analyze project risks in terms of probability and impact, assign triggers and risk response responsibilities
- Create project earned value baselines and project forecasts based on actual performance
- Communicate effectively with stakeholders, technical staff, and management teams

Who Should Attend

- Security professionals who need to understand the concepts of project management and utilize multiple development approaches
- Managers who want to understand the critical areas of making cybersecurity initiatives 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

Meet and exceed your security program's goals.

SANS MGT525: Managing Security Initiatives and Effective Communication provides the training necessary to maintain the Project Management Professional (PMP)® and other professional credentials. SANS Institute is a PMI® authorized training partner.

This course is focused on delivering bottom line value from security initiatives while following modern adaptive, agile, iterative, and predictive development approaches and leveraging the benefits of increased effective organizational communication. During this class students learn how to improve project planning methodology and project task scheduling to get the most out of critical IT resources. We utilize cybersecurity project case studies to increase practical understanding of real-world issues. MGT525 follows the basic methodologies and principles from the updated PMBOK® Guide, also providing specific implementation techniques for success. Throughout the five sections, all aspects of leading security initiatives—from project business justification analysis, selecting the appropriate development approach that fits your stakeholder and organizational structure using predictive, adaptive, and hybrid implementations tailored to drive value—are covered. We focus on planning for and managing cost, time, quality, and risk while your project is active, to completing, closing, and documenting as your project finishes. A copy of the PMBOK® Guide Seventh edition is provided to all participants. Students can reference the PMBOK® Guide and use course material along with the knowledge gained in class to prepare for the GIAC Certified Project Manager Exam (GCPM) and earn PDUs/CPEs to maintain the Project Management Professional (PMP)® and other professional credentials.

Project management methodologies and frameworks are highlighted that can be applied across any product life cycle, in any industry. Although our primary focus is the application of security initiatives, 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, risk, and compliance aspects 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.

NOTE: PMP® and PMBOK® are registered marks of the Project Management Institute, Inc. PMP® exams are not hosted by SANS. You will need to make separate arrangements to take the PMP® exam and this course is not an official PMP® prep class.

Course Author Statement

“Managing projects to completion, with an alert eye on quality, cost, and time, is something most of us need to do on an ongoing basis. In this course, we break down project management into its fundamental components and galvanize your understanding of the key concepts with an emphasis on practical application and execution of service-based IT and InfoSec projects. Since project managers spend the vast majority of their time communicating with others, throughout the week we focus on traits and techniques that enable effective technical communication. As people are the most critical asset in the project management process, effective and thorough communication is essential.”

—Jeff Frisk



GCPM
Project Manager
giac.org/gcpm

GIAC Certified Project Manager

The GIAC Certified Project Manager (GCPM) certification validates a practitioner's knowledge of technical project management methodology and implementation. GCPM certification holders have demonstrated the critical skill sets associated with making projects successful, including effective communication and time, cost, quality, procurement and risk management of IT projects and application development.

- Project management structure and framework
- Time and cost management, communications, and human resources
- Quality and risk management, procurement, stakeholder management, and project integration

SEC440: CIS Critical Controls: A Practical Introduction

2
Day Course

12
CPEs

Laptop
Required

You Will Be Able To

- Understand a security framework and its controls based on recent and evolving threats facing organizations
- Prepare you to interpret a security framework based on data from publicly known attacks, breach reports, and large scale data analytics from the Verizon Data Breach Investigation Report (DBIR), along with data from the Multi-State Information Sharing and Analysis Center® (MS-ISAC®)
- Understand the importance of each control, how it is compromised if ignored, and explain the defensive goals accomplished with each control
- Identify tools that implement controls through automation
- Learn how to create a scoring tool for measuring the effectiveness of each controls the effectiveness of each control
- Identify specific metrics to establish a baseline and measure the effectiveness of security controls

“The 20 Critical Security Controls provide updated/current trends in InfoSec. The course provided an excellent explanation of the controls and how to apply them.”

—Dan Sherman, RIC Audit FRB

Introduction to Critical Security Controls

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? Does your organization need an on-ramp to implementing a prioritized list of technical protections?

In February of 2016, then California Attorney General, Vice President Kamala Harris recommended that “The 20 controls in the Center for Internet Security’s Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization’s environment constitutes a lack of reasonable security.”

SANS has designed SEC440 as an introduction to the CIS Critical Controls, in order to provide students with an understanding of the underpinnings of a prioritized, risk-based approach to security. The technical and procedural controls explained in the CIS Controls were proposed, debated and consolidated by various private and public sector experts from around the world. Previous versions of the CIS Controls were prioritized with the first six CIS Critical Controls labeled as “cyber hygiene” and now the CIS Controls are now organized into Implementation Groups for prioritisation purposes.

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 course introduces security and compliance professionals to approaches for implementing 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.

Section Descriptions

SECTION 1: Introduction and Critical Controls 1–9

Section 1 will introduce you to Critical Controls 1–9, including the name, purpose, and why each matters in the bigger picture of cybersecurity.

- **CIS Critical Control 1:** Inventory and Control of Enterprise Assets
- **CIS Critical Control 2:** Inventory and Control of Software Assets
- **CIS Critical Control 3:** Data Protection
- **CIS Critical Control 4:** Secure Configuration of Enterprise Assets and Software
- **CIS Critical Control 5:** Account Management
- **CIS Critical Control 6:** Access Control Management
- **CIS Critical Control 7:** Continuous Vulnerability Management
- **CIS Critical Control 8:** Audit Log Management
- **CIS Critical Control 9:** Email and Web Browser Protections

SECTION 2: Critical Controls 10–18 and Conclusion

Section 2 will introduce you to Critical Controls 10–18, including the name, purpose, and why each matters in the bigger picture of cybersecurity.

- **Critical Control 10:** Malware Defenses
- **Critical Control 11:** Data Recovery
- **Critical Control 12:** Network Infrastructure Management
- **Critical Control 13:** Network Monitoring and Defense
- **Critical Control 14:** Security Awareness and Skills Training
- **Critical Control 15:** Service Provider Management
- **Critical Control 16:** Application Software Security
- **Critical Control 17:** Incident Response Management
- **Critical Control 18:** Penetration Testing

SANS CYBERSECURITY LEADERSHIP INSTRUCTORS



Frank Kim

Faculty Fellow | @fykim

Frank is the Founder of ThinkSec, a security consulting and CISO advisory firm, as well as a SANS Fellow and lead for both the SANS Cybersecurity Leadership and SANS Cloud Security curricula, overseeing two dozen SANS courses in the two fastest growing curricula.



John Hubbard

Senior Instructor | @SecHubb

John is a Security Operations Center (SOC) consultant and speaker. He is the course author of two SANS courses, SEC450: Blue Team Fundamentals – Security Operations and Analysis and MGT551: Building and Leading Security Operations Centers.



Randy Marchany

Senior Instructor | @randymarchany

Randy is the Chief Information Security Officer of Virginia Tech and the Director of Virginia Tech's IT Security Laboratory and has 25 years experience as a systems administrator, IT auditor, and security specialist.



Lance Spitzner

Senior Instructor | @lspitzner

Lance Spitzner has over 20 years of security experience in cyber threat research, security architecture and awareness training. He helped pioneer the fields of deception and cyber intelligence with his creation of honeynets and founding of The HoneyNet Project.



James Tarala

Senior Instructor | @isaudit

As a consultant with Enclave Security, James has spent the past several years designing large enterprise security and infrastructure architectures, helping organizations to perform security assessments, and communicating enterprise risk to senior leadership teams.



Benjamin Wright

Senior Instructor | @benjaminwright

Benjamin Wright is a practicing attorney based in Dallas, Texas, focusing on technology law. He is the author and sole instructor of LEG523: Law of Data Security and Investigations. Through that course since 2003, Ben has taught thousands of students around the globe.



Steve Armstrong

Principal Instructor | @nebulator

Steve Armstrong's career began more than 25 years ago when he joined the UK Royal Air Force (RAF), bringing with him a love of IT and a desire to protect others. Steve is the author of the new MGT553: Cyber Incident Management course.



Russell Eubanks

Principal Instructor | @russelleubanks

As founder and owner of Security Ever After, Russell is responsible for assessing the cybersecurity of many diverse organizations and increasing their maturity while decreasing the probability of a breach. Russell is co-author of MGT521 and SEC405 courses for SANS.



David R. Miller

Principal Instructor | @DRM_CyberDude

David has been a network engineer, consultant, security designer and architect, author, and technical instructor since the early 1980s and has specialized in IT security and compliance work in the recent years. David is the lead instructor for the CISSP certification course—MGT414.



Clay Risenhoover

Principal Instructor | @AuditClay

Clay is the president of Risenhoover Consulting, Inc., an IT management consulting firm. Founded in 2003, RCI provides IT audit and IT management consulting services to clients in multiple sectors. Clay is the lead author for AUD507 and the sole author of the brand new SEC557 course.



Jeff Frisk

Certified Instructor

Jeff Frisk serves as the Director of Global Information Assurance Certification (GIAC) Program, where he has been for the past 15 years. He is the author of MGT525, which bridges technical, leadership, and communication skills into one.



David Hazar

Certified Instructor | @HazarDSec

David is a security consultant focused on vulnerability management, application security, cloud security, and DevOps. David has 20+ years of broad, deep technical experience gained from a wide variety of IT functions held throughout his career. David is a co-author for MGT516.



Jason Lam

Certified Instructor | @jasonlam_sec

Jason holds a leadership role at a large global financial company. In this role, he's accountable for global direction and management of cybersecurity defense and response. Jason is co-author for SEC522 as well as sole author of MGT520.



My-Ngoc Nguyen

Certified Instructor | @MenopN

My-Ngoc Nguyen (pronounced Mee-Nop Wynn) is the CEO/Principal Consultant for Secured IT Solutions. She brings 20 years of experience in information systems and technology, with over 15 years focused on cyber security for both the government and commercial sectors.



Mark Orlando

Certified Instructor | @markaorlando

Mark Orlando is a co-author of MGT551 and the Co-Founder and CEO of Bionic Cyber. Prior to Bionic, Mark built, assessed, and managed security teams at the Pentagon, the White House, the Department of Energy, and numerous Fortune 500 clients.



Jonathan Risto

Certified Instructor | @jonathanristo

Jonathan has over 20 years working in network design, IP telephony, service development, security and project management. Currently, he works for the Canadian Government conducting cybersecurity research in the areas of vulnerability management and automated remediation. Jonathan is the co-author for MGT516.



Brian Ventura

Certified Instructor | @brianwifaneye

Brian Ventura has more than 20 years of industry experience with a diverse background including working in large, international organizations building global solutions, small-medium businesses providing all IT support, and government and private sector.



Mark Williams

Certified Instructor

Mark Williams currently holds the position of Enterprise Information Security Architect at BlueCross BlueShield of Tennessee. He has more than 20 years of international high-tech business experience working with major multinational organizations, governments, and private firms.



SANS CYBERSECURITY LEADERSHIP



Landing Page – sans.org/cybersecurity-leadership



Twitter – [@secleadership](https://twitter.com/secleadership)



LinkedIn – [SANS Security Leadership](https://www.linkedin.com/company/sans-security-leadership)



Discord – sansurl.com/leadership-discord