SANS | GIAC CERTIFICATIONS

CYBERSECURITY LEADERSHIP

Courses and Free Resources

sans.org/cybersecurity-leadership

SANS CURRICULUM FOCUS AREA

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

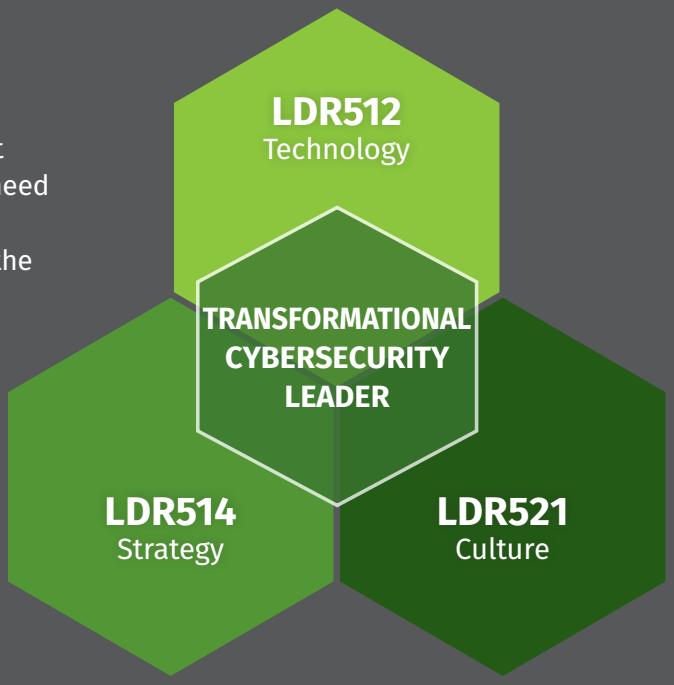
"This training applies to all aspects of my job, from network management to project management."
—David Chaulk, **Enbridge**

TRAINING & CERTIFICATION

In an effort to help our students find the right path, SANS Cybersecurity Leadership 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 organizational change that affects the foundational culture of the organization. A transformational cybersecurity leader will be able to strategize and apply concepts, management tools, and methodologies in order to analyze the current situation, identify target state, perform a gap analysis, and develop a comprehensive roadmap that includes employees at all levels of the organization in every type of job role. The SANS Management Transformational Cybersecurity Leader triad ensures a cybersecurity 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 organizations 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 organizations by better defending their data systems. Some organizations 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!

LDR512: **Security Leadership Essentials for Managers**

GSLC
Security Leadership
giac.org/gslc

5 Day Program | 30 CPEs | Laptop Required

You Will Be Able To

- 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 perspect

Leading Security Initiatives to Manage Information Risk

Take this course to learn the key elements of any modern security program. LDR512 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 built to enable the business and mitigate threats
- Create higher performing security teams

Hands-On Training

LDR512 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

"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**

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.

- 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

LDR514: **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 strategic security plans
- Create effective information security policy
- Understand the different phases of the strategic planning process
- Increase your knowledge of key planning tools
- Cultivate fundamental skills to create strategic plans that protect your company
- Enable key innovations
- Facilitate working effectively with your business partners
- Advance security strategic plans that incorporate business and organizational drivers
- Foster and assess information security policy
- Use management and leadership techniques to motivate and inspire your team

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 LDR514, 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. LDR514 will teach you to use management tools and frameworks to better lead, inspire, and motivate your teams.

Hands-On Training

LDR514 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 cybersecurity programs as well as proven business analysis, strategic planning, and management tools. GSTRT certification holders have demonstrated their knowledge of building and managing cybersecurity 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**

LDR516: **Building and Leading Vulnerability Management Programs**

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. LDR516 is based on the Prepare, Identify, Analyze, Communicate, and Treat (PIACT) Model.

LDR516 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
- Design 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 associate 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
- Understand what remediation capabilities are available to assist technology teams in resolving vulnerabilities and proactively addressing new ones

"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**

LDR520: **Cloud Security for Leaders**

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.

Strategically maximize your cloud investment.

Cloud Security Strategy is a comprehensive plan to protect the organization's data, workload, and infrastructure residing in the cloud(s) environment.

Cloud adoption is popular across all types of industries, and many organizations are taking strategic advantage of the cost and speed benefits of transitioning to the cloud. Since cloud environments differ significantly from traditional on-premises IT environments, in terms of protection requirements and threat vectors, the traditional network perimeter is no longer the most effective defense in cloud solutions. Organizations are migrating mission-critical workloads and sensitive data to private and public cloud solutions without always understanding the numerous key decisions needed for an organization's successful cloud transition. This cloud security implementation course walks the audience through the journey to mature their cloud security in each of the relevant security domains of could security strategy from beginning to high maturity state.

LDR520 complements traditional IT management techniques that leaders are accustomed to and helps with making appropriately informed decisions around strategy, financial investment, and necessary team technical knowledge and skill. We cover the key objectives of security controls in the cloud environment, including planning, deploying, and running the environment from the starting point to a progressively more mature state. There will be a focus on locking down the environment, securing the data, maintaining compliance, enhancing security visibility to the operations, and managing the security response on a continuous basis. Students will learn the essentials to lead the security effort for the cloud transition journey.

Business Takeaways

- Establish cloud security program supporting the fast pace business transformation
- Understand current and future maturity level of the cloud security in contrast to the industry benchmarks
- Make informed decisions on cloud security program
- Anticipate the security capabilities and guardrails to secure the cloud environment
- Safeguard the enterprise data as workloads are migrated to the cloud

Hands-On Cloud Security Strategy Training

LDR520 uses case scenarios, group discussions, team-based security leadership simulations with embedded real life technical components to help students absorb both technical and management topics. About 60 minutes per day is dedicated to these learning experiences using the Cyber42 leadership simulation game. This web application-based game is a continuous 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.

"Team is collaborative. We are all able to bounce ideas off of each other comfortably and using AWS to get hands-on makes it feel more real than if we were answering questions on a quiz."

—Richard Sanders, **Best Western International**

LDR521: **Security Culture for Leaders**

5 Day Program | 30 CPEs | Laptop Required

You Will Be Able To

- Explain what organizational culture is, its importance to security, and how to map and measure both your organization's overall culture and security culture
- Align your security culture to your organization's strategy, including how to leverage different security frameworks and maturity models
- Effectively communicate the business value of security to your Board of Directors and executives and more effectively engage and motivate your workforce
- Enable and secure your workforce by integrating security 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, incident detection and response, and other related security projects
- Create and effectively communicate business cases to leadership and gain their support for your security initiatives
- Ability to measure your security culture, how to make those measurements actionable, and how to present the maturity and value of your 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 immediately

Who Should Attend

- Chief information security officers
- Chief risk officers/Risk management leaders
- Security awareness, engagement or culture 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

What is a Security Culture?

Security culture is your workforce's shared attitudes, perceptions, and beliefs about cybersecurity. It is what they think and feel about your security team, your security policies, and your security training. The more positive their attitudes towards your security team, the more they will trust your security team. The higher their perception that your security team is committed to your company's mission, the more likely they will exhibit more secure behaviors. The greater their belief in your security training, the more likely they will commit to your organization's security culture.

Build and Measure a Strong Security Culture

Drawing on real-world lessons from around the world, the SANS LDR521 security culture for leadership course will teach you how to leverage the principles of organizational change to develop, maintain, and measure a strong security culture. Through hands-on instruction and a series of interactive labs and exercises, you will apply these concepts to various real-world security initiatives and quickly learn how to embed security into your organization's culture, from senior leadership on down.

Apply findings from Daniel Kahneman's Nobel prize-winning research, Thayler 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 are all keys to building a strong security culture at your company.

Business Takeaways

- Create a far more engaged and secure workforce, not only in their attitudes about security but also in their behaviors
- Dramatically improve the ROI of security initiatives and projects through increased success and impact
- Strengthen communication between the security team and business executives
- Instill stronger and more positive attitudes, perceptions, and beliefs about the security team
- Construct simpler, more effective security policies and governance

Hands-On Training

The first four sections of the course leverage 12 interactive team labs, enabling you to apply the lessons learned to a variety of real-world security situations and challenges. These team labs enable you to learn not only from the instructor and course materials but also from your fellow students' expertise and 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. Leveraging the Cyber42 simulation game environment, you are put in real-world scenarios that spur discussion and critical thinking of situations that you will encounter at work. A Laptop is required for the Cyber 42 leadership simulation capstone.

Notice to Students

The course is recommended for more senior and/or more experienced cybersecurity leaders, managers, officers, and awareness professionals. If you are new to cybersecurity, we recommend some of SANS's more fundamental courses, such as SEC301, SEC401, or LDR433.

"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**

LDR551: **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

- Construct a strong SOC foundation based on a clear mission, charter, and organizational goals
- 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 detection efforts on true priorities
- Apply threat hunting process and active defense strategies
- Implement efficient alert triage and investigation workflow
- Operate effective incident response planning and execution
- Choose metrics and long-term strategy to improve the SOC
- Employ team member training, retention, and prevention of burnout
- Perform 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 thing than I could have learned in months on my own."

—Zac Scholl, **Zendesk**

Prevent – Detect – Respond | People – Process – Technology

Information technology is so tightly woven into the fabric of modern business that cyber risk has become business risk. SOC managers must align to their organization and demonstrate real value—a challenge when threats are hard to quantify and stakeholder requirements for the security team are often vague and difficult to translate. How does a SOC communicate their value and focus on operations that enable the organization? LDR551 breaks down security operations into clear and atomic functions that can be measured and improved. We then tie these core SOC activities to high-level organizational goals for easy communication with the SOCs constituency. Common questions SOC managers 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 a SOC team that is empowered and continuously improving, where analysts are empowered to 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, LDR551 will super-charge your people, tools, and processes. Each section of LDR551 is packed with hands-on labs that demonstrate key SOC capabilities, 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 organizational requirements. Attackers are always improving, so a SOC that sits still is losing ground. LDR551 will give SOC managers and leaders the tools and mindset required to build the team, process, workflow, and metrics to defend against modern attackers by building the processes for continuously growing, evolving, and improving the SOC team over time.

What is a SOC Manager?

A SOC Manager leads an organization's cybersecurity operations team by developing and guiding implementation of a cyber defense strategy that can minimize the impact of cybersecurity incidents. Leading a SOC is a complex role that requires merging technical and business sensibilities, and the skills to monitor performance, communicate requirements, and demonstrate results up and down the chain of command.

Hands-On SOC Manager Training

While LDR551 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 seventeen hands-on exercises covering everything from playbook implementation to use case database creation, attack and detection capability prioritization and visualization, purple team planning, threat hunting, and reporting. Attendees will leave with a framework for understanding where a SOC manager should be focusing 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 (SOC). 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
- Prioritization 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

LDR553: **Cyber Incident Management**

5 Day Program	30 CPEs	Laptop Required

You Will Be Able To

- Implement various incident response frameworks
- Scoping incidents correctly
- Define the incident management team's objectives
- Effectively managing a team under extreme pressure
- Awareness of human responses to facing catastrophically impactful urgent changes
- Structure, manage, and deliver briefings to upper management and the Board
- Planning and controlling communications when managing a serious incident
- Communicating with attackers and the pros and cons thereof
- Where and how track the incident
- Planning, coordinating, and executing counter compromise activities
- Mastery of incident reports both during and post closure
- Steps to close the incident and return to business as usual
- Understand the constraints of third-party or supply chain incidents
- Plan for and deal with a compromised supply chain 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

Cyber Incident Management (IM) sits above Incident Response (IR) and is tasked to manage incidents that get too big for the Security Operations Center (SOC) and IR. These tend to be the more impactful or larger incidents that IR is not scaled to handle as it requires significant liaison with internal and external partners to coordinate the investigation, forensics, planning, recovery, remediation, and to brief the corporate comms, C-level staff and board as needed. Less technical and more business focused, the IM team will take the output from IR and relay it to the necessary teams as they coordinate wider investigations and hardening, hygiene and impact assessment as they plan towards recovery. A strong IR lead may fulfill the IM role, but during critical incidents IRs are often shoulder deep in malware, systems, logs and images to process to the point where all technically capable IR staff are kept focused on technical tasks. IMs are more business focused and IR is more technically focused.

Open in Case of Emergency

LDR553 looks at all the common and major cyber incident types, explains what the key issues are, and how plan a recovery. Whilst you may have a full team of technical staff standing by to find, understand, and remove the attackers, they need information, tasking, managing, supporting, and listening to maximize their utilization and effectiveness. We focus on building a team to remediate the incident, on managing that team, on distilling the critical data for briefing, and how to run that briefing. We look at communication at all levels from the hands-on team to the executives and Board, investigative journalists, and even the attackers.

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. LDR553 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.

Business Takeaways

- Develop staff that know how to lead or contribute to a cyber incident management team
- Manage your incidents more effectively
- Resolve incidents quicker
- Understand the gaps in your security incident plans and response strategies
- Create higher performing security incident teams
- Plan ahead to handle some of the most devastating potential attacks

"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 CIS Controls**

GCCC 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
- Compliance Analysts
- IT Administrators
- Department of Defense (DoD) personnel or contractors
- Federal agencies or clients
- 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

NICE Framework Work Roles

- Security Control Assessor (SP-RSK-002)

What are CIS Controls?

The CIS Controls (formerly known as Critical Security Controls) are a recommended set of prioritized cyber defense best practices. They provide specific and actionable ways to protect against today's most pervasive and dangerous attacks. SANS provides CIS Controls v8 training, research, and certification. Version 8, released in May 2021, is a Change to the Entire Controls Ecosystem and provides backwards compatibility with previous versions and a migration path for users of prior versions to move to v8. Whether you use the CIS Controls or another control framework to guide your security improvement program, it is critical to understand that a controls list is simply a starting point. With the release of version 8, CIS added new tools and guides to the CIS controls ecosystem to help organizations:

- Implement, track, measure, and assess controls
- Prioritize controls based on evolving threats
- Justify investment in CIS Controls implementation
- Implement CIS Controls best practices for mobile devices and applications
- Apply CIS Controls best practices to cloud environments
- Comply with multiple frameworks by providing a map of regulatory frameworks

Organizations need to defend their information systems and there are many solutions, requirements and tools to navigate. Which solutions should be implemented first? What will reduce the most risk and defend against the most common attacks? SANS and CIS have mapped the most common and likely threats and attacks to a prioritized list of mitigations called the CIS Controls. These controls are regularly reviewed to ensure they continue to mitigate the the ever-evolving threat and surface-area landscape. By following the CIS Controls, organizations will reduce cyber risk, measure, and report on residual risk.

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. Students will gain direct knowledge of the CIS Controls and ecosystem of tools to implement CIS controls across organizations complex networks, including cloud assets and third-party risk. Additional tools to measure both CIS Control coverage as well as assess risk throughout the program will be provided. This in-depth, hands-on critical security controls 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 CIS 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 cybersecurity control effectiveness. In addition, CIS Controls are mapped to other frameworks to ensure compliance as well as security leveraging the CIS Controls.

"I would recommend this course to anyone that is going to be a ISSO or ISSM or CISO."

—Matthew S., **US Military**

GCCC 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.

AUD507: **Auditing Systems, Applications, and the Cloud**

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 properly 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, covering systems, applications, and the cloud. 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 including systems, applications, and the cloud. 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, perimetre, and application auditing as well as risk assessment and reporting.

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

LDR414: **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 LDR414: 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.

LDR414 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

LDR433: **Managing Human Risk**

SSAP
Secururity Awareness Professional
giac.org/ssap

3 Day Course | 18 CPEs | Laptop Not Needed

You Will Be Able To

- Master how to map and benchmark your program's maturity against your peers'.
- Understand the Security Awareness Maturity Model and how to leverage it as the roadmap for your program
- Ensure compliance with key standards and regulations
- Implement models for learning theory, behavioral change, and cultural analysis
- 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
- Define what security culture is and the common indicators of a strong security culture
- Explain your organization's overall culture and how to most effectively align cybersecurity with and embed into your organization'sculture
- Measure the impact of your program, track reduction in human risk, and how to communicate to senior leadership the value of the program

Who Should Attend

- Security awareness, training, engagement or culture officers
- 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, influence or communications program

People have become the primary attack vector. Manage your human risk.

Learn the key lessons and the roadmap to build a mature awareness program that will truly engage your workforce, change their behavior and ultimately manage your human risk. Apply models such as the BJ Fogg Behavior Model, AIDA Marketing funnel, and Golden Circle, and learn about the Elephant vs. the Rider. Concepts include how to assess and prioritize your top human risks and the behaviors that manage those risks, how to engage, train and secure your workforce by changing their behaviors and culture, and how to measure the impact and value of that change.

The course content is based on lessons learned from hundreds of 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'soverall risk management efforts.
- Make the most of your investment by sustaining your program long term, going beyond changing behavior to embedding a strong security culture
- Communicate and demonstrate the value of the change to your senior leadership in business terms

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 three section course has eight interactive labs. Each lab is approximately 30 minutes to complete as a team, with another 20–30 minutes of group discussion.

- **Section 1:** Determine Your Program's Maturity Level, Creating an Advisory Board, Identify and Prioritize the Top Human Risks to Your Organization
- **Section 2:** Identify and Prioritize the Key Behaviors that Manage Your Top Human Risks, Leverage the AIDA Model to Sell MFA, Putting it All Together, Creating an Engagement Plan
- **Section 3:** Define Your Organization's Culture, Measuring a Key Human Risk and Behaviors that Manage that Risk

"The labs presented an effective way to grasp the material and present to others for good feedback."

—Michael U., **U.S. Government**

SSAP
Security Awareness Professional
sans.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 three-day SANS LDR433 course on building mature awareness programs.

LDR525: **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 LDR525: 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. LDR525 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

LDR419: **Performing A Cybersecurity Risk Assessment**

2 Day Course | 12 CPEs | Laptop Required

You Will Be Able To

- Understand the business context for a risk management program
- Create a cybersecurity program charter
- Understand foundational elements of risk
- Choose appropriate cybersecurity safeguards
- Perform third-party risk assessments
- Perform a cybersecurity risk assessment
- Evaluate cybersecurity documentation
- Examine the implementation of cybersecurity safeguards
- Thoroughly report risk to business stakeholders
- Effectively report risk to technical stakeholders
- Productively respond to risks identified during an assessment

Who Should Attend

- Risk management professionals
- Governance, risk, and compliance professionals
- IT auditors
- Directors of security compliance
- Information assurance management
- System administrators/engineers

"The Cyber42 exercises were a great way to demonstrate the realistic circumstance of having to weigh imperfect options against each other and make the best of what we have."

—Stephanie Martin, **Federal Reserve**

"The content is very relevant and can be directly applied to my work. It helped me get an overview on risk management frameworks before diving into how we do a risk assessment."

—Sammie Pless, **Premera**

Every organization should be performing risk assessments as a part of their cybersecurity program. Regular risk assessments allow organizations to create practical strategies for defense and evaluate where there are weaknesses in their cybersecurity program that could keep them from achieving their goals. Most cybersecurity risk courses are theoretical and academic, often leaving students unsure how to prepare for and do the actual assessment work. This cybersecurity risk assessment training teaches students the foundational knowledge and practical, hands-on skills they need to perform risk assessments.

The course uses the Cyber42 leadership simulation game to put students into real-world scenarios that spur discussion and critical thinking of situations that they will encounter at work. Throughout the class students will participate in multiple Cyber42 activities to help them practice what they learn and ensure that they will be able to take these skills immediately back to the office.

Business Takeaways

- Establish the business case for a cybersecurity risk assessment
- Prepare for a risk assessment that matters to the business
- Meet and exceed regulatory requirements
- Effectively export the results of a risk assessment to key stakeholders
- Create a strategy for how to respond to identified cybersecurity risks

Hands-on Cybersecurity Risk-Assessment Training

Each of the case studies in this course will be based on a fictitious technology company, Initech Systems, and its quest towards maintaining a more mature cybersecurity program. Students will have an opportunity to explore Initech's specific cybersecurity strategies and tactical plans, which are based on real-world examples. To facilitate these case studies, students will use the Cyber42 tabletop simulation game to put students in real-world scenarios that spur discussion and critical thinking of situations that they will encounter at their offices.

- Evaluating an organization's governance model
- Evaluating a cybersecurity program's goals to create a safeguard inventory
- Creating a comprehensive risk assessment plan for internal and third parties
- Evaluating a cybersecurity policy
- Evaluating cybersecurity technical safeguards
- Creating an executive risk briefing
- Writing a personal action plan

Section 1: Learn the practical, foundational skills necessary to prepare for and plan for performing a risk assessment.

Section 2: Learning the practical skills for how to perform a cybersecurity risk assessment and present risks to leadership.

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 LDR551: 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.

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 LDR553: 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 LDR521 and SEC405 courses for SANS.

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 LDR520.

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—LDR414.

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 LDR525, 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 LDR516.

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 cybersecurity for both the government and commercial sectors.

Mark Orlando

Certified Instructor | @markaorlando

Mark Orlando is a co-author of LDR551 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 LDR516.

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.

John Scott

Certified Instructor

John Scott is the Lead Cybersecurity Researcher for Culture AI, a comprehensive human risk management platform that empowers organizations to effectively measure employee security behaviors and reduce cyber risks.

SANS

CYBERSECURITY LEADERSHIP

Landing Page – sans.org/cybersecurity-leadership

Twitter – @secleadership

LinkedIn – SANS Security Leadership

Discord – sansurl.com/leadership-discord

YouTube – sansurl.com/leadership-youtube