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 program
- Develop strategic security plans that incorporate business and organizational goals
- Effectively engage and communicate with key business stakeholders
- Measure the impact of your security program
- 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**

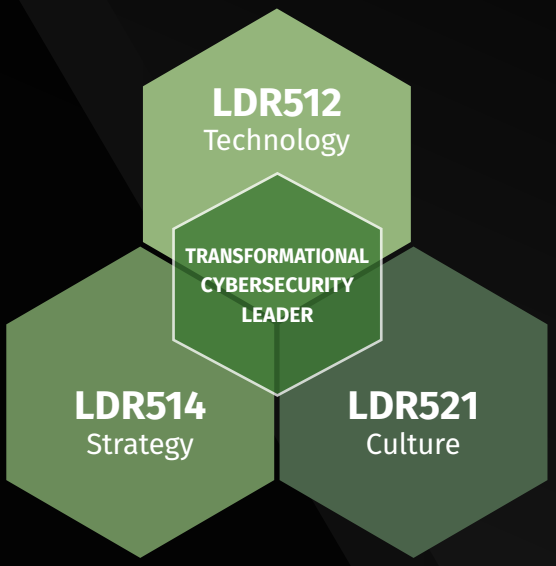
TRAINING & CERTIFICATION

sans.org/cybersecurity-leadership | SANS Security Leadership | secleadership | sansurl.com/leadership-discord

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

Transformational Cybersecurity Leader

With enterprises 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. Our Chief Information Security Officer (CISO) training paths teach how to adjust employees' and leadership's way of thinking about security in order to prioritize and act to prevent today's most common cybersecurity attacks. Organizational change is required to affect the foundational culture of the organization.



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. Complicating the matter more are a wide range of modern technologies requiring more time and knowledge to manage, more known vulnerabilities than ever before, an unprecedented migration to cloud, and ever-increasing legal and regulatory compliance standards. Information Assurance Engineers, Auditors, Security Operations Center (SOC) Analysts, Cybersecurity Managers, and CISOs need more to better defend an organization's data systems. The SANS Operational Cybersecurity Executive triad is here to provide CISO training to help you build, grow, and sharpen your cyber defense team.

Cyber Risk Officer

Modern security leaders must deal with an endless barrage of changes to the business, technology, and threat landscape. This requires a combination of technical knowledge, understanding of risk, and the ability to lead teams in times of intense pressure. Doing so requires building a comprehensive program of controls to manage information risk, enhancing cybersecurity governance while ensuring compliance, and dealing with the inevitable incidents and crises. The SANS Cyber Risk Officer triad is here to provide CISO training to help you effectively lead, govern, and manage this risk for your organization.

sans.org/cybersecurity-leadership/triads

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

- 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

Leading Security Initiatives to Manage Information Risk

Take this security management course to learn the key elements of any modern security program. LDR512 training 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, cloud security, application security, DevSecOps, generative AI (GenAI) 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

This leadership focused security training course 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 leadership simulation 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.

What Is Security Management?

Security management is all about managing information risk. This means that you need the appropriate level of technical knowledge and leadership skills to gain the respect of technical team members, understand what technical staff are actually doing, and appropriately plan and manage security projects and initiatives. This is a big and important job that requires an understanding of a wide array of security topics. Being an effective security leader requires you to get up to speed quickly on information security issues and terminology to build a modern security program. Creating a high performing security team means that you can anticipate what security capabilities need to built to enable the business and mitigate threats.

"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 the fictional organizations in the course. 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 has 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 training 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**

LDR519: **Cybersecurity Risk Management and Compliance™**

5 Day Program	30 CPEs	Laptop Required

Skills Learned

- Gain practical skills in identifying and managing cybersecurity risks through structured threat modeling and assessment methodologies
- Learn to prioritize and allocate resources effectively by understanding the criticality of various cybersecurity threats and vulnerabilities.
- Develop proficiency in using industry-standard frameworks, such as NIST Risk Management Framework (RMF) and FAIR, to enhance your organization's cybersecurity posture.
- Master the process of conducting comprehensive cybersecurity risk assessments and audits to ensure compliance with regulatory standards
- Enhance your decision-making capabilities with data-driven insights and simulations, preparing you for real-world cybersecurity challenges

Business Takeaways

- Equip employees with advanced skills to identify, assess, and mitigate cybersecurity risks, enhancing organizational security
- Align cybersecurity efforts with business goals through a structured approach to risk management and compliance
- Enhance decision-making capabilities by integrating threat modeling and risk analytics into strategic planning
- Strengthen organizational resilience against evolving cyber threats through proactive risk management strategies
- Ensure compliance with industry standards and regulatory requirements, reducing the risk of legal and financial repercussions
- Implement robust cybersecurity safeguards tailored to your organization's specific risk profile
- Foster a culture of security awareness and critical thinking among team members to improve overall security posture
- Improve the effectiveness of cybersecurity governance practices, ensuring comprehensive oversight and alignment with business objectives

Who Should Attend

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

Secure Your Organization's Digital Future

Master the essentials of risk management and compliance with SANS LDR519 training. This course is designed to equip cybersecurity professionals with the skills necessary to navigate the complex landscape of cybersecurity risks. Through a systematic approach, students will delve into threat modeling, risk assessments, and safeguard implementation, ensuring their organizations remain resilient against evolving cyber threats.

LDR519 training focuses on practical methodologies and industry-best practices, providing participants with a thorough understanding of risk management and compliance frameworks. By exploring real-world case studies and engaging in hands-on simulations, students will learn to develop comprehensive threat inventories, prioritize cybersecurity defenses, and align security measures with business objectives. The curriculum integrates established frameworks such as the Cybersecurity Risk Foundation's Governance and Risk Model (CRF-GRM) and NIST Risk Management Framework (RMF), offering a structured approach to managing cybersecurity risks and ensuring regulatory adherence.

Enroll in LDR519 training to transform your cybersecurity strategy and lead your organization towards robust risk management and compliance. Gain insights from seasoned experts and leverage cutting-edge tools to enhance your decision-making capabilities. With a focus on practical applications and strategic planning, this course empowers you to implement effective cybersecurity safeguards, validate their impact, and communicate risks to stakeholders confidently. Join us at the SANS Institute and elevate your cybersecurity expertise today.

What Is Cybersecurity Risk Management and Compliance?

Cybersecurity risk management is the systematic process of identifying, assessing, and prioritizing risks, followed by the coordinated application of resources to minimize, monitor, and control the probability or impact of unfortunate events. Compliance refers to adhering to laws, regulations, guidelines, and specifications relevant to an organization's operations, ensuring ethical and legal conduct.

Hands-On Cybersecurity Risk Management and Compliance Training

LDR519 training uses a combination of case studies and Cyber42 leadership simulation game to deepen students' understanding of the concepts covered in the course. Through detailed case studies based on the fictitious company Initech Systems, students can apply theoretical knowledge to real-world scenarios. This approach allows learners to analyze vulnerabilities, develop threat models, and manage risk registers effectively. By pausing to reflect on the concepts learned, students gain practical insights into cybersecurity risk management strategies, enhancing their decision-making skills.

The SANS Cyber42 simulations offer an interactive environment where students confront realistic cybersecurity incidents. These simulations provide hands-on experiences in managing resources, responding to evolving threats, and implementing strategic initiatives. By engaging with these dynamic scenarios, students practice critical thinking, problem-solving, and collaboration techniques essential for effective cybersecurity leadership. The combination of case studies and simulations ensures that students not only understand theoretical principles but also acquire the practical skills needed to navigate complex cybersecurity challenges confidently.

LDR520: **Cloud Security for Leaders™**

5 Day Program | 30 CPEs | Laptop Required

You Will Be Able To

- Define a cloud security strategy aligned with enterprise business goals
- Build a roadmap to support rapid, secure cloud adoption
- Understand cloud security fundamentals and justify key decisions
- Mature your security posture using cloud-native tools and automation
- Communicate cloud security vision to executives and teams
- Evaluate posture against benchmarks and optimize security investments
- Implement scalable guardrails and governance across multicloud environments

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.

As cloud adoption accelerates across industries, the risks associated with evolving threat landscapes and misconfigured cloud environments grow just as rapidly. This course provides a practical, hands-on approach to building and maturing cloud security using a structured security maturity model. Participants will explore key areas such as workload protection, compliance, incident response, and visibility across cloud platforms. Through 12 interactive Cyber42 leadership simulation exercises, students gain real-world experience in making informed decisions around strategy, investment, and team capabilities, developing the leadership and technical skills essential to successfully plan, deploy, and manage secure cloud environments from day one to high maturity.

Business Takeaways

- Accelerate business transformation with architect cloud security strategies
- Evaluate your security posture against industry benchmarks to identify competitive advantages
- Optimize security investments with metrics-driven ROI frameworks
- Implement automated guardrails that protect assets while enabling innovation
- Balance security controls with cloud adoption velocity to avoid becoming a bottleneck
- Create unified governance frameworks that scale across multicloud environments

Hands-On Cloud Security Strategy Training

LDR520 training 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.

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

—Benoit Ramillon, **UEFA**

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

—Jeff Henderson

LDR521: **Security Culture for Leaders™**

5 Day Program	30 CPEs	Laptop Required

You Will Be Able To

- Explain what culture is, its importance to security, and how to map and measure both your organization's overall culture and your security culture
- Define the indicators of a strong security culture, align security with them, and embed them into your organization's existing culture
- Provide a framework and guiding principles for your security team on how to lay the foundation for a strong security culture
- Effectively communicate the business value of security to your Board of Directors and executives, gaining their support and buy-in
- Engage and motivate your workforce so they prioritize cybersecurity
- Simplify security and remove blockers, making it exponentially easier for people to embed security into their everyday actions
- Dramatically improve 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
- 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 Security Culture?

Security culture is your organization's shared attitudes, perceptions, and beliefs about cybersecurity. The more strongly your leadership and workforce believe in and buy into cybersecurity, the more likely they will prioritize security, support your initiatives, and exhibit the behaviors you want. Your organization already has a security culture. The question is, is it the culture you want?

Build and Measure a Strong Security Culture

Drawing on real-world lessons from around the world, the SANS LDR521: Security Culture for Leaders training course will teach you how to build a culture where both your leadership and workforce believe in and prioritize cybersecurity. Through hands-on instruction and a series of interactive labs and exercises, you will apply organizational change concepts to various real-world security initiatives and quickly learn how to transform your security team and 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, ADKAR change model 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 organization.

Business Takeaways

- **Security at Scale**—Make your job easier by scaling both yourself and your security team. Reduce the impact of burnout on the security team you are privileged to lead.
- **Embed Security**—Automatically bake security into the start of every business project and initiative in every business unit of your organization.
- **Executive Support**—Get the executive leadership support you need for what is most important to you.
- **Secure your Workforce**—People will exhibit the behaviors you want without telling them what they can and cannot do at work.
- **Successful Initiatives**—Make your security initiatives far more successful by gaining the buy-in of key departments, such as IT, Engineering, and the Business.
- **Advocates**—Transform your security team into security advocates who engage, motivate, and enable your workforce to be far more secure.

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.

"This content is helping bring back concepts that get forgotten when you go from a doer to a senior leadership role. It brought back good concepts and a way to utilize them in the security context as well as getting leadership to think differently."

—Michael Neuman

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 training 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 training 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 training 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™**

GCIL
Cyber Incident Leader
giac.org/gcil

5 Day Program | 30 CPEs | Laptop Required

You Will Be Able To

- Categorize and scope incidents correctly and the resulting incident management team's objectives
- Design, draft, proof, release and control all communications when managing a serious incident
- Manage a team under extreme pressure and to recognize the natural human responses that will emerge and what they mean
- Lead the team, win the confidence of the execs and exceed the expectations of everyone involved
- Calculate, coordinate, and execute both system and data counter compromise activities
- Strategize and respond to ransomware incidents including how to develop exercises and training around these devastating attacks
- Structure, manage, and deliver briefings to the team, execs and senior leadership or the board
- Organize the transition from active incident to business as usual and how to execute that plan
- Prepare, setup and run cyber incident management exercises

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

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

—Peter Leonhardt

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

While you can't predict when a major cyber incident will hit your organization, you can control how ready you are to face it. In the aftermath, when incident response teams are engrossed in unraveling the attacker's moves within your networks, they often find themselves overwhelmed. This is where your incident management team steps in, taking charge of managing findings, communications, regulatory notifications, and remediation. With a multitude of tasks and challenges on their plate, many are unseasoned and unprepared for the magnitude of responsibilities.

This course equips you to not just be a member of the incident management team but a leader or incident commander. It ensures a comprehensive understanding of the immediate, short, and medium-term issues an organization might encounter. Beyond familiarizing yourself with the terminology, you'll grasp preparatory actions at different stages to stay ahead of the situation. LDR553 is designed for efficient management of diverse incidents, with a primary focus on cyber, yet its methodology, concepts, and guidance are applicable to various regular major and critical incidents.

Business Takeaways

- Cultivate a workforce adept at leading or contributing to cyber incident management teams
- Streamline incident management processes for quicker resolutions
- Identify and bridge gaps in security incident plans and response strategies
- Elevate the performance of security incident teams to meet evolving challenges
- Strategically plan and navigate through high-stakes attacks, including email compromise and ransomware, fostering a resilient response frameworks
- Promote seamless collaboration between technical and non-technical teams during incident response for a more integrated approach
- Instill a culture of continuous improvement, leveraging lessons learned from incidents to refine future response strategies
- Proactively integrate threat intelligence to anticipate and mitigate potential threats before escalation

GCIL
Cyber Incident Leader
giac.org/gcil

GIAC Cyber Incident Leader

The GIAC Cyber Incident Leader (GCIL) certification validates a practitioner's ability to manage cyber incidents and lead a diverse incident management (IM) team to restore normal operations. GCIL holders demonstrate expertise in preparing for, assessing, handling, tracking, and documenting incidents; developing IM teams; managing vulnerabilities, threats, and attacks; facilitating communication; and improving IM processes.

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

What are CIS Controls?

The Center for Internet Security (CIS) 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 v8.1 training, research, and certification. Version 8.1, released in June 2024, 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 v8.1. 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 8.1, 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 training 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.

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 training 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
sans.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
- Explain the most effective ways to communicate to and engage people
- Identify high-risk roles and the required, specialized training for those roles
- 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 security into your organization's culture
- Measure the impact of your program, track reduction in human risk, and how to communicate to senior leadership the value of the program in strategic terms
- Define steps to grow your career, increase your credibility and expand your work options

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 not only learning theory and behavior change models but 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, you will have the opportunity to earn the SANS Security Awareness Professional (SSAP), the industry standard in human risk management.

What Is Human Risk Management?

Cyber threat actors have changed their attack methods, they no longer target technology but people. Human Risk Management is the structured approach in how organization's secure people, addressing for most organizations what is now their greatest vulnerability—their workforce.

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.

"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 training course on building mature awareness programs.

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**

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

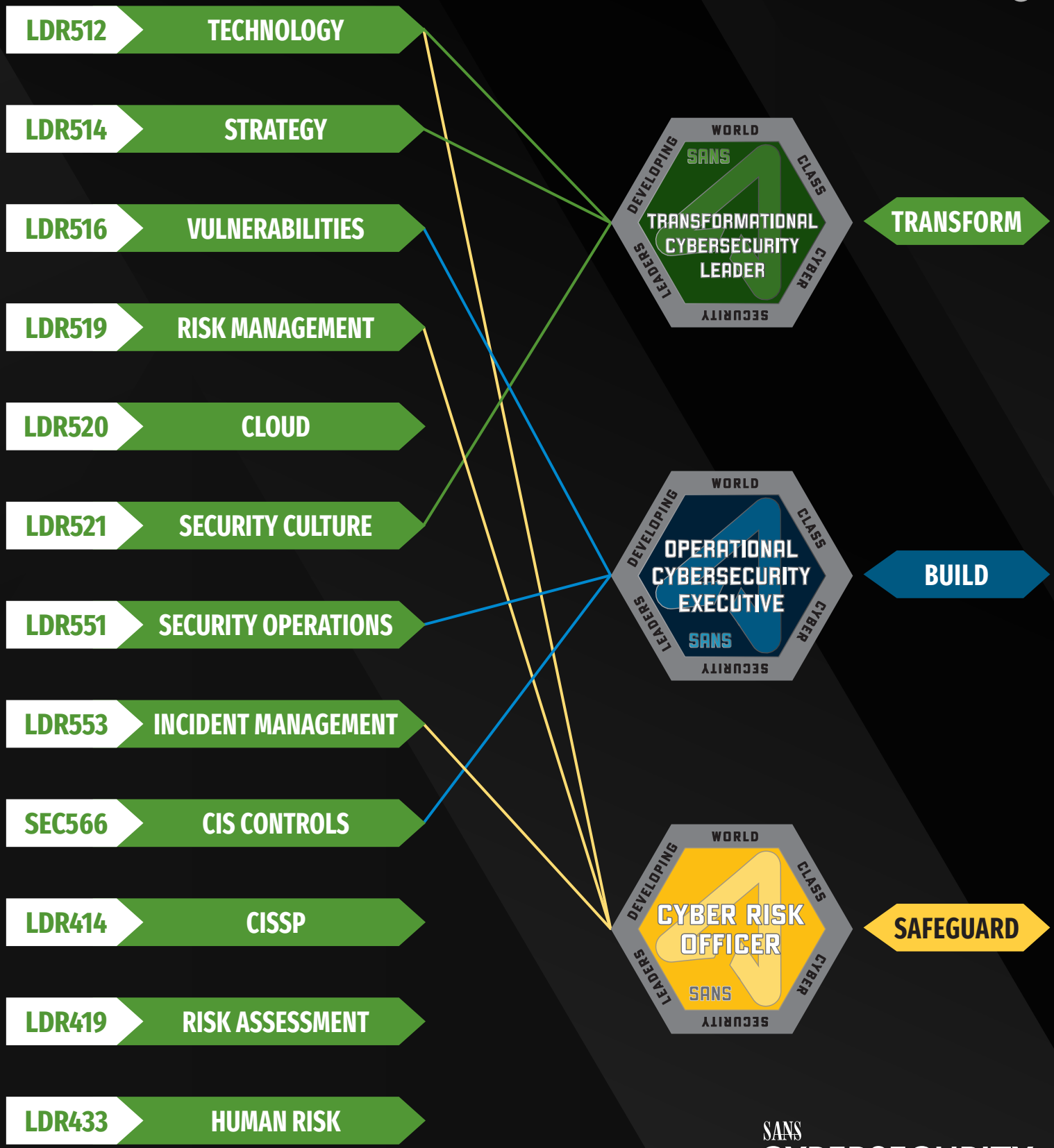
Section 1: Learn the practical, foundational skills necessary to prepare for and plan for performing a risk assessment.

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

"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**

CYBERSECURITY LEADERSHIP WIREFRAME



SANS
CYBERSECURITY 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.

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.

Steve Armstrong-Godwin

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.

Jason Lam

Principal 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 SEC566™ 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

Principal 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

X – @secleadership

LinkedIn – SANS Security Leadership

Discord – sansurl.com/leadership-discord

YouTube – sansurl.com/leadership-youtube