LDR433: **Managing Human Risk™**

SSAP
Security Awareness Professional
giac.org/ssap

3 Day Course	18 CPEs	Laptop Required

This Course Will Prepare You to:

- Benchmark and advance your program's maturity level
- Identify and prioritize your top human risks
- Understand the sciences behind adult learning theory, cognitive biases, and behavior and organizational change
- Gain actionable strategies to motivate and drive secure behaviors
- Employ techniques to engage and build credibility with leadership and your security team
- Leverage the latest AI tools to accelerate and amplify your impact
- Implement approaches to measure and communicate your program's value

"I think the course is really engaging and works at two levels: (1) It would provide someone starting out with a solid foundational knowledge, (2) It allows an existing program to benchmark and get new ideas, to supplement the existing work."

—Brian Wright,
Student Loans Company Unlimited

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

Learn the key lessons and understand the roadmap to building a mature awareness program that will truly engage your workforce, change their behavior, and ultimately support your efforts in managing human risk. Apply models such as the BJ Fogg Behavior Model, Curse of Knowledge, the Golden Circle, and Kirkpatrick Evaluation Model, and learn about the Elephant vs. the Rider. Learn how to leverage the latest AI tools and manage the greatest AI risks facing your workforce, including vibe coding, plugins and agentic AI. Concepts include how to assess and prioritize your top human risks and the behaviors that manage those risks, how to engage and secure your workforce by changing their behaviors, how to build a strong security culture, and how to measure the impact and value of all that change.

The course content is based not only on learning theory and behavior change models, but 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, 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:

- Communicate in terms of both business and risk, building your credibility and reputation, especially with leadership and your own security team
- Identify and manage your organization's top human risks, including how AI is affecting them
- Integrate human risk management with your organization's broader risk management efforts
- Build sustainable programs that foster a strong security culture
- Demonstrate program value to leadership in business terms
- Implement effective learning and behavioral change models
- Leverage AI to maximize program impact and efficiency

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 six interactive labs.

- **Section 1:** Benchmark Your Program's Maturity Against Your Peers, Case Study: Identify and Prioritize Top Human Risks
- **Section 2:** Identify and Prioritize Key Behaviors, Create, Simplify and Communicate an AI Security Policy
- **Section 3:** Analyze and Align Security with Your Organization's Culture, Create a Comprehensive Action Plan

Section Descriptions

SECTION 1: Identifying/ Prioritizing Human Risk

Section 1 covers the fundamentals by specifically answering the question:

What is human risk, and how can you effectively manage it? We start with students defining the maturity of their existing program, then provide a strategic roadmap for how to improve their program's maturity. We then cover critical foundations for a successful program: leadership support, program charter, and partnerships. We then cover the fundamentals of risk management and how to assess and prioritize your top human risks.

TOPICS:

- How to map and benchmark your program's maturity
- The five stages of the Security Awareness Maturity Model
- The fundamentals of risk and risk management
- The definition of human risk and the three variables that define it
- Why humans are so vulnerable and the latest methods cyber attackers use to exploit these vulnerabilities
- Steps to gain and maintain leadership support for your program
- How to develop and leverage effective partnerships
- Developing a strategic plan that prioritizes your organization's human risk, the behaviors to manage those risks, and changing those behaviors
- A walk-through on how to conduct a human risk assessment and how to prioritize your organization's top human risks, including leveraging the latest in Cyber Threat Intelligence (CTI)
- How to identify and manage role-based risks

SECTION 2: Identifying and Changing Behavior

Section 2 begins with identifying the behaviors that best manage your top human risks, then covers the science of behavior change and how to engage and motivate your workforce across demographics, cultures, and regions. You will then create and customize effective training modalities, using AI to accelerate and amplify your impact.

TOPICS:

- Resources for your long-term success
- Defining learning objectives and how they apply to learning theory and risk management
- How to identify and prioritize the top behaviors that manage your key human risks
- Fundamentals of behavioral sciences, including the BJ Fogg Behavior Model, cognitive biases, the Curse of Knowledge, the Golden Circle and the importance of "why"
- How you can effectively create an engagement strategy leveraging marketing models
- Creating a training strategy leveraging the ADDIE and Kirkpatrick models
- Top tips for effective global translation and localization
- The effective use of imagery, with a focus on diverse or international environments
- Planning and documenting your training campaigns
- How to create the latest training modalities with maximum impact and minimum budget, including leveraging AI to amplify your reach and impact

SECTION 3: Security Culture and Measuring Change

Section 3 focuses on organizational culture, security culture and embedding security in your organization's overall culture. We then cover metrics, including behavior, culture and strategic metrics. Students will learn how to communicate those metrics and their value to leadership and finish the class by creating an actionable implementation plan.

TOPICS:

- Career development, a series of steps you can take to grow your credibility, position and compensation
- What organizational culture is and how to define your organization's overall culture
- What security culture is, the value of a strong security culture and the most common indicators of both a weak and strong security culture
- How to align with and embed a strong security culture into your organization's overall culture
- How to create a strong incentive program to sustain behavior change long-term
- A deep dive into Ambassador Programs
- Fundamentals of metrics, including why we collect them and how to leverage them strategically
- The difference between compliance metrics and impact metrics
- A walkthrough of the three types of impact metrics: knowledge, culture and behavior
- Identifying leadership's strategic priorities and how to align your metrics with them
- Putting an overall project plan together and executing it
- Resources for success moving forward

Who Should Attend

- Security awareness, training, engagement or culture officers
- Security management officials
- Security ambassadors or champions officers
- 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

NICE Framework Work Roles

- Cyber Instructional Curriculum Developer (OPM 711)
- Security Awareness & Communications Manager (OP 712)



SSAP
Security Awareness Professional
giac.org/ssap

SANS Security Awareness Professional

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

The first step to achieving your SSAP is taking the three-day SANS LDR433 course on building mature awareness programs.