

Security Awareness Roadmap

Managing Your Human Risk

Organizations and security leaders are coming to terms with the fact that cybersecurity is no longer just a technical challenge but also a human one. In fact, people are now the biggest contributors to breaches, with employees involved in 62%* of all breaches globally. In many ways security teams have become so effective at using technology to secure systems that they are driving threat actors to target people.

* Verizon 2026 Data Breach Investigations Report

The key to managing human risk is establishing a mature security awareness program. These programs take a structured approach to change and secure your workforce's behaviors. The most mature programs go beyond behavior modification and ultimately cultivate a strong security culture. A successful awareness program follows a proven roadmap that enables you to plan, communicate, and measure your efforts. The Security Awareness & Culture Maturity Model enables you to do exactly that.



- sans.org/cybersecurity-leadership
- [@secleadership](https://twitter.com/secleadership)
- [SANS Security Leadership](https://www.linkedin.com/company/sans-security-leadership)
- [sansurl.com/leadership-youtube](https://www.youtube.com/channel/UCsursurlcomleadershipyoutube)
- [sansurl.com/leadership-discord](https://discord.com/invite/sansurlcomleadershipdiscord)

Developing Your Career

SANS LDR433: Managing Human Risk™

This three-day class lays the foundation of risk management, changing organization behavior and ultimately managing and measuring human risk. Course content is based on lessons learned from hundreds of security awareness programs from around the world.

sans.org/ldr433

SANS LDR521: Security Culture for Leaders™

This advanced five-day course is designed for senior security leaders and highly experienced awareness officers. The course provides the skills, models and frameworks to build, manage, and measure a strong security culture.

sans.org/ldr521

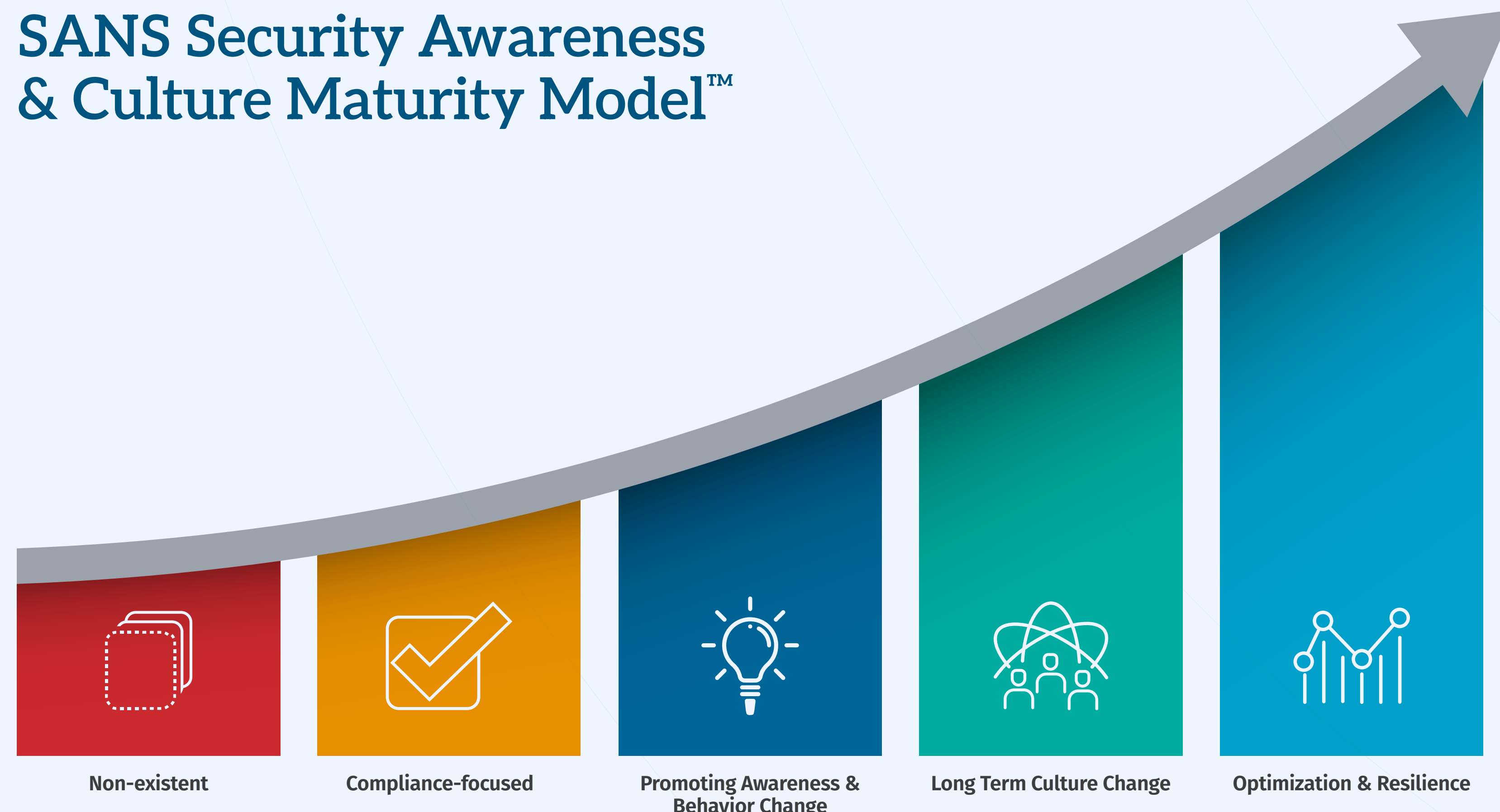
Trust SANS to Bring Security Awareness to Your Workforce

Build a resilient workforce with SANS' Workforce Security & Risk Training. Our expert-designed solutions, including industry-leading Security Awareness training, help you measurably reduce human risk, support compliance needs, and drive cultural change. Designed to meet a range of roles, risks, and learning levels, our comprehensive approach enables you to integrate security into the fabric of your organization.



- sans.org/workforce
- [@SANSWorkforce](https://twitter.com/SANSWorkforce)
- [linkedin.com/company/sansworkforce](https://www.linkedin.com/company/sansworkforce)

SANS Security Awareness & Culture Maturity Model™



Key Elements to a Mature Program

Managing human risk is a people problem, requiring people for the solution.

Effective Engagement

Great programs start with making security personal. Show your workforce why security matters and how it safeguards them and their work. Simplify behaviors so they feel easy and natural to adopt — small steps can create big changes.

Empowered Teams with Leadership Support

Success grows from strong leadership support — backed by the right team size. Research shows you need at least 3 dedicated people to change workforce behavior, and at least 4 to embed a strong security culture. With that foundation in place, security awareness becomes a shared goal everyone can rally behind.

Integrated Awareness

Security awareness is more than compliance — it's a proactive foundation for protecting your people and your organization. Aligning awareness with the security team makes it a powerful part of your overall strategy.

Continuous Improvement

Building a security-aware culture takes real time — typically 3–5 years to shift behavior, and 5–10 years to embed lasting culture change. Through consistent communication, training, and reinforcement, your workforce becomes more resilient every year.

Security Awareness & Culture Maturity Model Indicators Matrix

This matrix details each of the stages of the maturity model, identifies which stage your organization is in, the value of the stage, and how to achieve the next stage. Leverage this matrix as a strategic planning guide for your approach to managing and measuring your organization’s human risk. For more information and free resources, visit sans.org/for-organizations/workforce.

Maturity Level	Description	Program Indicators	People Indicators	Time to Achieve	Metrics	Steps to Next Level
STAGE 1 NO SECURITY AWARENESS PROGRAM	The program does not exist. Employees have no idea that they are a target, that their actions have a direct impact on the security of the organization, do not know or follow organizational policies, and easily fall victim to attacks. VALUE: None. Your organization is at high risk of failing to meet any compliance requirements and highly vulnerable to human-driven incidents.	- There is no security awareness program - Leadership does not discuss or care about security awareness	Employees never discuss security or exhibit secure behaviors	N/A	None	- Identify the regulations or standards that you must adhere to - Identify security awareness requirements for those standards - Identify someone to roll out the required security awareness training - Develop or purchase training that meets those requirements - Deploy security awareness training - Track and document who completes the training
STAGE 2 COMPLIANCE FOCUSED	The program is designed primarily to meet specific compliance or audit requirements. Training is limited to annual or ad hoc basis. Employees are unsure of organizational policies and/or their role in protecting their organization's information assets. VALUE: Your security program meets the legal training requirements your organization is required to adhere to. However your organization is not effectively managing its human risk. In some circumstances this stage can be the most dangerous, as leadership perceives that the organization is effectively managing its human risk, but it is not.	- Program is led by someone who is only dedicated part time to the security awareness efforts - Security awareness reports to non-cybersecurity teams such as GRC, compliance, audit, legal or Human Resources - There is no strategic plan, training topics are ad hoc and deployed at random times - Program has limited leadership support — leadership's goal is to maintain compliance at minimum costs - Security awareness is only considered during audits - There is little coordination or partnership with other departments, such as Communications and Human Resources - Leadership perceives security as purely a technical issue - Training is primarily once a year, often mandatory - There is little to no communication to the workforce about security beyond annual training	- People have a “Let’s get this over with” attitude - People perceive security as something that the IT or security team takes care of — it’s not their problem - People feel security is something they have to do - People have a negative perception of the security team, which is often perceived as arrogant, too technical or perhaps even blockers - People perceive security policies as confusing, difficult and as a blocker to their daily work responsibilities - People often ignore policies and use their own solutions to get work done	Depends on the standards, regulations, or legal requirements you are attempting to adhere to — however, the overall effort is usually minimal, often requiring nothing more than annual training	- Number/% of people that have completed training - Number/% of people that have signed Acceptable Use Policy - Number of on-site training sessions in one year - Number/frequency of awareness materials distributed (newsletters, posters, webcasts, etc.)	- Identify and gain support of key leaders and stakeholders - Create Project Charter, identifying scope, responsibilities, goals, objectives, assumptions, and constraints for the awareness program - Identify who will be responsible for the awareness program — to ensure greatest success, that person should be dedicated full time, have strong people skills, be a part of the security team, and report to the CISO - Identify the top human risks you will need to manage — Coordinate with Incident Response team, Security Operations Center, and/or Cyber Threat Intelligence team to assist with this. This may also require some type of human risk assessment - Identify the key behaviors that will mitigate and manage the top human risks - Plan how you will communicate to, engage, and train your workforce on these key behaviors - Develop, resource and/or purchase your training materials and platform, to include Learning Management System (LMS) or a Human Risk Management (HRM) platform - Create execution plan with milestones to include metrics
STAGE 3 PROMOTING AWARENESS AND BEHAVIOR CHANGE	The program identifies the top human risks to the organization and the behaviors that manage those risks. Program goes beyond just annual training and includes continual reinforcement throughout the year. More mature programs in this stage identify additional roles, departments or regions that represent unique risks that require additional or specialized role-based training. Content is communicated in an engaging and positive manner that encourages behavior change. As a result, people understand their role in cybersecurity, follow organizational policies and exhibit key behaviors to secure the organization. VALUE: Your organization is not only meeting its compliance requirements but is able to effectively identify, manage and measure its human risk.	- Program is led by someone dedicated full time to managing the security awareness program and has a team of 1-3 people to assist them — in addition, this individual often has strong communication/people skills - Security awareness reports to and is an integrated part of the cybersecurity team - Leadership understands and commits to the need for managing human risk - There is a strategic plan that has identified the scope, goals, objectives, and justification for the program - Through a risk assessment, and in partnership with different security team members (DFIR, SOC, CTI), the security team has identified and can explain the organization's top human risks and the behaviors that most effectively manage those risks - Program has sufficient leadership support to provide resources necessary and has an executive champion - Security awareness team actively partners and collaborates with various departments within the organization, including Communications, Human Resources, and Help Desk - Program goes beyond just annual training and includes continuous reinforcement throughout the year - More mature programs have identified different departments, roles or regions that represent increased or unique risks to the organization and require specialized or additional training (role-based training) - Program works to positively engage the workforce — engagement is not based on mandatory training but creating training that people want to consume	- Employees understand that technology alone cannot protect them and they have a responsibility to protect themselves and the organization - People are reporting incidents or suspected attacks - When security team pushes out information, people are asking them questions - Employees are exhibiting the behaviors they are being trained on - Employees begin to exhibit the same strong security behaviors at home and in their personal lives - Employees are asking how their family can take the training	Depending on the behaviors you are attempting to change, you can begin impacting certain behaviors within 6-12 months. However, the more behaviors you are attempting to change or the more complex those behaviors, the longer it can take to change those behaviors organization-wide. This is one of the reasons it is so important to prioritize your top human risks, and the behaviors that manage those risks. The fewer behaviors you focus on, the more likely you can change those behaviors.	This stage is all about measuring the behaviors you care about, which behaviors are the most important to managing your risk. Examples include: - Phishing simulation click rates, number of repeat clickers and reporting rates - Number of lost or stolen laptops or mobile devices - Adoption rate of password managers or MFA - Percentage of employee passwords that could be cracked - Percentage of workstations that are securely locked down at night - Percentage of mobile devices that are current and/or screenlocks enabled - Number of accidental data loss events, such as data loss due to auto-complete in email or insecure cloud accounts - In some cases, a human risk management (HRM) platform may be used to automate the collection, tracking and display of these metrics NOTE: See the interactive metrics matrix for more examples. These metrics are ultimately driven by what behaviors are the most important to managing your human risk.	- Establish a process to give leadership regular updates on the awareness program - Identify a specific date when the security awareness program is reviewed and updated every year - During annual review and update, identify any new risks or behaviors required to manage human risk, and new ways to communicate to, engage and train your workforce - Security awareness team should partner with audit, compliance or GRC and actively assist with policy development to help ensure they are simple as possible for the workforce - Security awareness team should be actively assisting the security team in any outreach, communication and engagement efforts to include any new tool rollouts - Some type of formal incentive program to recognize individuals, groups or departments excelling in cybersecurity and/or exhibiting key behavior - Senior leadership creates a compensation or bonus program dependent on leaders or managers achieving certain cybersecurity-related KPIs - Establish a security ambassador/champion program to help engage and promote security throughout the workforce - Partner with or establish a training program for mid-level managers, often the biggest blockers in any culture change initiatives
STAGE 4 LONG-TERM CULTURE CHANGE	The program has the processes, resources, and leadership support in place for a long-term sustainment. In addition, the security team has moved beyond just continuous training and is focusing on additional human-related drivers, such as simplifying security policies and workforce communications, supporting incentive programs or improving how the security team partners with and enables other departments. As a result, security is an established part of the organization's culture, people believe in, support and prioritize security in their daily actions and processes. VALUE: Your program has gone beyond impacting behavior and has started building a strong security culture. By security culture, we mean your workforce's shared attitudes, perceptions and beliefs about cybersecurity. A strong security culture, not only creates an environment where people are far more likely to exhibit secure behaviors, but, promotes and helps ensure security is prioritized and built into almost all operational aspects of the organization, exponentially increasing the overall security of your organization.	- Program is led by someone dedicated full-time to managing the security awareness and culture efforts and has a team of at least three people, more often five or more - Security awareness reports directly to the Chief Information Security Officer (CISO) - Leadership believes in and has invested in long-term support of the program — program is actively reviewed and updated on an annual basis — program lead is regularly updating leadership on a monthly or quarterly basis - Security team is actively invested in supporting and enabling other departments — they perceive their role not as an enforcer but customer service, enabling other departments to achieve their business goals safely and securely - Security ambassador or BISO program ran by a dedicated program manager - Security team actively works to simplify security for their organization, to include simplifying policies, automating processes and providing tools to other departments - Incentive program for the workforce on leadership compensation is tied to security-related KPIs - Security awareness team is assisting the security team with all organization-wide security communications or security tool roll-outs ensuring that expectations are simple to understand and tools are easy to use	- Good security practices are baked into who we are and what we do - Employees educate their peers on good security behaviors - Employees start providing ideas or suggestions on how to improve security in the organization - Employees or departments actively reach out to and request assistance or briefings by the security team - Department leads and teams request security reviews/audits and involvement of the security team in new products or projects - The security team and their security efforts are perceived as approachable, collaborative and helpful by the workforce (e.g., people feel safe reporting an incident, even when they know they caused it)	Impacting your organizational culture takes much longer than impacting behavior. Impacting culture organization-wide can take 3-10 years depending on the size, complexity and age of your organization and its culture (John Kotter, Leading Change). For this stage, you are focusing on embedding security into the overall culture. The biggest drivers of security culture are: - Security training - Security team - Security policies - Leadership support and buy-in	- Survey people's attitudes, perceptions and beliefs towards information security (this can be broken down by what people think about your security policies, your security team and your security training) - Conduct focus groups or interviews for deep dives into the “why” of people's attitudes, perceptions and beliefs - Number of people/departments requesting security briefings or updates - Employee satisfaction working with the security team (think Net Promoter Score for security) - Number of people engaging the security team with questions or submitting ideas on how to improve security	- Identify and align with leadership's strategic priorities - Identify and align security behaviors and culture with any key strategic security frameworks or models used by the organization
STAGE 5 OPTIMIZATION AND RESILIENCE	The program has a robust metrics framework aligned with and supporting the organization's mission and business goals. It is no longer just measuring and reporting on changes in behavior and culture, but ultimately how these changes are reducing risk and enabling leadership to achieve their strategic priorities. As a result, the program is continuously improving and able to demonstrate return on investment. VALUE: Your program is aligned with and actively supporting your leadership's strategic priorities and your organization's business goals/mission.	- Security team works with business leaders to identify and align with their strategic business priorities - Metrics are collected on a regular basis, often automated — these metrics are continuously used to improve and optimize the program and ultimately the security culture of the organization - Metrics are provided to senior leadership demonstrating value at a business level and showing alignment with strategic business priorities - Metrics are aligned with the security framework(s) that your leadership has committed to (e.g., NIST Cybersecurity Framework or CIS Critical Controls) - Different types of metrics are delivered to different target audiences - You have the ability to benchmark your program's maturity against peer organizations in your industry	- Leadership actively requests and uses security awareness and culture metrics to measure their organizational progress and/or compare departments across the organization - Security becomes a business enabler and competitive differentiator	Stage 5 is maintained through continuous improvement rather than completed as a final milestone. Ongoing leadership engagement, measurement, and adaptation are required to sustain this level of maturity.	How these changes are impacting and reducing overall risk to the organization, which can be measured in strategic metrics, such as: - Overall number of security incidents - Average time to detect an incident (i.e., attacker dwell time) - Average time to recover from an incident - Number of policy, audit or compliance violations In addition, show leadership how the awareness program is aligned with and enabling strategic goals in strategic security frameworks (e.g., NIST CSF, ISO 27001, Critical Controls).	