Five Steps to Building a Sustainable Information Security Program

EXTEND RESOURCES

When combining the complexity of doing business in the digital world with emerging regulations, expanding cybersecurity threats, and vendor risk management strategies adopted by clients and partners, a documented, sustainable information security program is an essential element of any organization’s operation. Whether an organization plans to create its first infosec program, enhance and strengthen an existing program, or certify a program to meet industry or international standards, taking a proactive approach to information security management is more than merely smart business; it is a necessary step for protecting assets, limiting risk, and avoiding liability.

Know Where You Are.
Understand Where You Want to Be.

Taking a proactive approach to developing or enhancing an information security program begins with understanding the specific needs of the business: Which assets need to be protected -- high value and high risk -- and what is the impact if they are affected by a security incident? The starting point and foundational structure of a program will depend largely on the size of the organization, its existing information security capabilities, its appetite for risk, and specific quality-assurance, control, and audit requirements. So before diving right into the building stage, take the time to determine the scope and strategy of the program.

- First and foremost, identify the organization’s goals and specific benefits to be achieved. Are there particular areas of the business (departments, geographies, etc.) where information security is especially important? Is a holistic program required, or are there certain standards, industry requirements, or insurance considerations that could drive scope decisions? What type of information is stored, processed, and transmitted?
- An information security program should be easily maneuverable so that it adheres to the continually evolving landscape of security threats and applicable regulations. What type of organization is involved (public, private, government)? How will processes and protocols be adjusted in response to changes in security threats, industry requirements, or business initiatives? Do any internal processes have legal or regulatory implications?
- To better ensure the sustainability of an organization’s information security, having a well thought out management plan is required. Do you have executive buy-in and engagement? Which ongoing processes and tools will you use to manage the activities, tasks, and communications? How will you keep up with changing requirements?
- When crafting the components of a program, remember to focus not only on mitigating risk but also on maintaining efficient operational productivity. Often, protecting information assets requires a balance between securing information while still enabling team members to be productive via effective work processes and workflow.

The goal is to create a foundation for risk prevention and management, aligned with the strategic goals of the organization, that focuses on assessing key vulnerabilities, mitigating risks, and detecting and resolving incidents while limiting liability. Based on the overall scope of the program and outlined requirements, use the following steps as a checklist for designing the program blueprint.

Step 1: Identify the Security Team

The success of any project is mainly dependent upon collaborative planning and communication. The better aligned the team, the more productive and successful the project. Identifying the information security team, along with each team member's responsibilities, paves the path for protecting information by fostering transparency and knowledge sharing on a go-forward basis.

Defining the security team may seem an elementary exercise, but it is essential in developing the proper communication and controls throughout the enterprise. Beyond the core team, creating well-established and ongoing communications between team members and outside departments is instrumental when it comes to continual monitoring and readiness for an unexpected information security incident. A security team contains two crucial elements:

Top-Level Leadership

Involvement and buy-in by executive leadership are critical to implementing a sustainable information security program. Establishing a culture of security starts with a clear directive and "tone from the top" that flows throughout the organization. Generally, the executive team is responsible for establishing the organization's security objectives and goals, setting high-level security policies, establishing organization risk thresholds, obtaining any needed funding, and assigning responsibilities to the security management team. The CISO should report directly to the CEO or president and serve as a member of the executive team to avoid conflicts of interest.

Day-to-Day Management

Beyond the executive team, the security management team is responsible for day-to-day security operations, which include managing assets, assessing threats and vulnerabilities, managing risks, establishing policies, setting up procedures and controls, conducting internal audits, and providing training and awareness. The security management team is made up of individuals with varying roles, such as an information security analyst, a compliance administrator, or a security team leader.

Step 2: Perform a Security Gap Analysis

In this step, an organization’s existing information security program is assessed to identify areas of strengths and weaknesses. The goal here is to identify security posture gaps as compared to industry or international standards, such as ISO 27001 or NIST, and develop a detailed roadmap to achieve the desired security and compliance levels, meet compliance requirements, and accomplish business objectives.

This process involves interviewing and collaborating with all stakeholders to assess the organization’s current adherence to the information security program goals and internal standards. You can’t protect what you don’t know. So, a thorough inventory of all assets must be conducted during this step, as assets reveal vulnerabilities and weaknesses. Once the inventory is complete, each asset must be assigned an owner and categorized according to the value of the information contained within and the cost to the company if it is compromised. To ensure effectiveness, this process should be performed on an annual basis, at a minimum.

Tasks in the Security Gap Analysis phase should include:

Identify threats, vulnerabilities, and risks for each asset

Inspect and evaluate the current structure, assets, policies, practices, and controls

Develop a framework diagram illustrating security gaps and resolutions

Develop a project plan with a schedule of activities to implement gap resolutions

Create a customized project plan to meet any compliance required objectives

Step 3: Assess Information Security Processes and Protocols

While there is no way to eliminate risks completely, identifying and understanding an organization's vulnerabilities and risks help support the longevity of a successful security management plan. To do so, identify and list all the definitive and potential risks associated with an organization and categorize them based on their level of importance and impact on the organization. Listing all definitive and potential risks, along with the protocols and processes involved in addressing them, is highly advisable.

Definitive Risks	Potential Risks
Sources of real threats. For example, a situation where an outside source gained access to confidential data causing a privacy breach.	Vulnerabilities or flaws in systems or processes that can be initiated accidentally or even intentionally, causing a security breach. For example, a potential risk may an employee inadvertently clicking a link in a phishing email that contains a virus.

Risks are not always internal. Organizations frequently interact with third parties such as vendors and suppliers who may have unstable network security or poorly managed security practices, which can create a substantial risk. Third parties often have access to confidential information. Take the time to identify these third parties and establish a process to evaluate their security measures and communicate any required controls at least once per year.

Upon completion of the assessment process, an organization should develop an assessment report which provides insight into the organization's infosec infrastructure. The assessment report should document areas in which security risks exist, define detailed steps to resolution, and outline areas in which the information security program aligns with any current or forthcoming regulatory legislation, like GDPR or ISO 27001. Depending on the industry and client base, an organization may need to incorporate a variety of standards and regulatory requirements into an information security program.

Components in the information security assessment phase include:

Map regulatory and legal controls to current requirements

Research forthcoming regulatory requirements

Identify threats, vulnerabilities, and risks for each asset

Document policy improvements, enhancements, and risk treatment options

Define and execute a risk treatment plan

Develop metrics to maintain your information security scorecard

Develop a documented action plan that defines a transparent track to eliminating gaps

Step 4: Internal Audit and Performance Check

Once an organization has established security processes and protocols and has aligned them with specific business requirements, an internal audit of the program ensures the integrity of the security management process.

An internal audit is a performance check conducted by an external, competent auditor, designed to provide visibility into the reliability of the security infrastructure, validate that team members are following security processes and protocols, illustrate areas in which security risks exist, and verify the resolution of those risks.

The internal audit generally includes the development of a report for the security and executive teams. Recommended tasks for the internal audit phase include:

- Validate the scope of Information Security Management Program security assurances
- Perform a detailed review of security policy documents, practices, and procedures
- Document the results of the audit mapped to any regulatory requirements (current or future)
- Recommend policy improvements, enhancements, and risk treatment options
- Develop metrics to maintain an information security scorecard
- Develop a documented action plan that defines a transparent track to eliminating gaps

Step 5: Ongoing Management and Incident Response

Developing a strong infrastructure and performing internal audits supports and validates the quality of an information security program. Maintaining a healthy security posture requires an ongoing management program that continuously monitors the maturity and effectiveness of an organization's security processes.

Ongoing management should include conducting regular compliance evaluations to ensure the sustainability of an information security program and implementing a more extensive array of protocols, reviews, and reporting to improve the program continuously. To maintain ongoing compliance, security, and sustainability, it is also vital to confirm regularly that your people, processes, and infrastructure are in alignment with your security policies.

Consistent with human nature, it is fair to say that one of the most significant security risks within an organization is its people. Human error is the reason why training is an integral part of the long-term management of a successful information security program. Employees need sufficient education and knowledge to help combat security threats and maintain continual security awareness.

Intentional or otherwise, security incidents happen. There is simply no way to eliminate risk completely. A comprehensive incident response plan, which systematically identifies each step required to manage a security incident, is an integral part of an infosec program. Communication within and across different internal and external teams is essential in both detecting and responding to an incident.

For successful ongoing management and proper incident response:

- Track changes to relevant legislation and regulations and update your program when appropriate
- Track new required practices and changes to procedures and update your program when appropriate
- Monitor the effectiveness and maturity of the program's controls
- Conduct risk assessments and update the treatment of assets on a regular basis
- Conduct table-top exercises to test security procedures and playbooks
- Maintain training records, access control, and a scorecard to measure program effectiveness

Step 6: Sustaining the Success of an Information Security Program

It is almost impossible to maintain the integrity of your information security management program without an information security compliance software platform that enables you to document and maintain policies, identify risks and mitigation plans, track infosec activities across teams, provide compliance guidance through supported by a variety of best practices, and report on results -- all in one place.

To give your information security program the best chance for long-term success, choose the right technology solution will help you manage it efficiently and enable your security team to:

- Manage your overall information security projects and program
- Easily interpret compliance requirements and identify organizational gaps
- Develop regulatory-compliant information security management
- Identify opportunities for improvement in environment, processes, and protocols
- Update controls and other documentation to meet regulatory standards
- Conduct risk assessments and treatment of the enterprise's assets
- Measure information security objectives
- Maintain training records, access control, and a scorecard to measure program effectiveness
- Manage third-party vendor security risks

In Conclusion

The benefits are evident; a strong, sustainable security program can help reduce risk and avoid liability as well as improve brand reputation, increase financial controls, and simplifying regulatory compliance. Businesses that continuously invest in ways to promote information security and embed security in day-to-day processes often have a competitive advantage.

Ready to Take the Next Step?

Many organizations have limited resources for establishing and improving information security. At EXTEND Resources, our team of experts can provide the clarity needed to determine the most advantageous path forward for a sustainable information security program. Using OnTrack™ 27001, EXTEND's intuitive and configurable compliance management tool, our teams help organizations develop, implement, and manage world-class infosec programs.

Interested in learning more?

Contact us at info@extendresources.com or (203) 479-9408 to speak with one of our security experts and find out how EXTEND can help your organization build a sustainable information security program.

About EXTEND Resources

EXTEND Resources solves a fundamental problem many organizations face: How to do more with less. As a professional services and solutions company specializing in business and legal process optimization, contract management, and cybersecurity, clients rely on EXTEND to help them increase productivity, enhance efficiency, and generate valuable results. EXTEND's executives have many decades of combined expertise in business management, legal technology, and global outsourcing. To learn how EXTEND can help you power performance, visit ExtendResources.com and follow the company on Twitter at @ThinkExtend.

The information contained in this EXTEND Resources article is provided for informational purposes only and should not be construed as legal advice on any subject matter. No recipients of content from this article, clients or otherwise, should act or refrain from acting on the basis of any content included in this article without seeking the appropriate legal or other professional advice on the particular facts and circumstances at issue from an attorney licensed in the recipient's state. The content of this article contains general information and may not reflect current legal developments, verdicts or settlements. EXTEND Resources expressly disclaims all liability in respect to actions taken or not taken based on any or all the contents of this article.

EXTEND
RESOURCES

T/F (203) 479-9408
info@extendresources.com

1127 High Ridge Road, Suite 170
Stamford, CT 06905
V181026