Gartner for IT Leaders

Security Program Management 101 — How to Select Your Security Frameworks, Controls and Processes

Richard Addiscott, Jeffrey Wheatman, Khushbu Pratap

8 August 2022
Security Program Management 101 — How to Select Your Security Frameworks, Controls and Processes

By Analyst(s): Richard Addiscott, Jeffrey Wheatman, Khushbu Pratap

Initiatives: Cybersecurity and IT Risk

Security and risk management leaders are faced with an array of information security frameworks, control catalogs and processes all intended to inform the design of their security programs. The issue isn’t so much which one you pick but how effectively you implement it.

Overview

Key Challenges

- There are many security frameworks, security control catalogs and security processes that security and risk management (SRM) leaders must choose from and understand when designing their security program.

- SRM leaders struggle to determine which frameworks, control catalogs and processes should be considered for their organization to execute their security programs.

- Not selecting the appropriate security framework, controls catalog and security processes can result in wasted security investment and security team burnout.

Recommendations

To help decide the appropriate security framework, control catalog and security processes, security and risk management leaders should:

- Recognize that security frameworks, control catalogs and security processes are different elements of their security program.
Strategic Planning Assumption

Through 2024, ISO 27001 and the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) will remain the predominant enterprise security frameworks complemented by localized and industry-specific standards and regulations.

Introduction

SRM leaders are faced with a confusing array of information security frameworks, control catalogs and associated processes designed to guide the establishment and execution of security and risk programs. SRM leaders and their teams’ ability to navigate the security framework and control catalog landscape will be key to:

- Designing a fit-for-purpose security program.
- Embedding effective and efficient security operations with embedded security processes.

Gartner research between 2014-2018 shows that approximately 41% of clients had either not selected a framework or had developed their own ad hoc framework (see Figure 1). Failure to select any framework and/or build one from scratch can lead to security programs being designed:

- With critical control gaps and therefore don’t address current and emerging threats in line with stakeholder expectations.
- That place undue burden on technical and security teams.
- Wastes precious funding on security controls that don’t move the needle on the organization’s risk profile.
Figure 1. Which of the Following Best Describes the Management Framework of Your Information Security Management Program?

<table>
<thead>
<tr>
<th>Description</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>We have developed our own ad hoc framework</td>
<td>20%</td>
</tr>
<tr>
<td>We have combined components from more than one standard framework</td>
<td>20%</td>
</tr>
<tr>
<td>We are using one of the standard governance frameworks and customized it</td>
<td>16%</td>
</tr>
<tr>
<td>We are using one of the standard governance frameworks</td>
<td>23%</td>
</tr>
<tr>
<td>We have no framework</td>
<td>21%</td>
</tr>
</tbody>
</table>

Source: 2014-2018 Gartner IT Score Data
ID: 380672

So, while it may seem a big challenge to select the right security framework or control catalog, security will be a much bigger challenge for SRM leaders who fail to choose any framework.

This best practice guide helps security and risk leaders:

- Differentiate between frameworks, controls catalogs, and security processes and their specific roles as part of an organization’s security program; and
- Understand the high-level contextual elements and organizational factors that inform the selection of a best-fit security frameworks and control catalog for the organization.
Analysis

Recognize That Security Frameworks, Control Catalogs and Security Processes Are Different Elements of Your Security Program

While they are interrelated, security frameworks, control catalogs and security processes perform different roles for a security and risk program. Understanding their specific roles and how they work together in support an organization’s security program is a key element in effective security program execution.

Security frameworks provide SRM leaders with a structure to organize their security controls to ensure they are complete and cohesive. Another way to think about security frameworks is that they describe “what” an organization will do to manage security risks. Leveraging security frameworks — or multiple if required — aids organizations to develop a more mature approach to security. Security frameworks serve to underpin SRM leaders to build a defensible security program by:

- Instilling confidence in internal and external stakeholders that the organization is aligning to industry best practice.
- Making it more measurable in terms of being able to assess maturity levels over time to a consistent set of control objectives.
- Increasing the likelihood that the security program is rightsized for the organization.

Control catalogs describe “how” the organization will implement its control environment. They do this by providing a menu of controls the security team can choose from based on the framework selected. Their role is to promote a systematic and consistent approach to deploying security controls to optimize the organization’s information security risk exposure.

Together, security frameworks and control catalogs provide the baseline standards and guidance platforms that support an organization’s approach to information security.
Security processes are the procedural actions, either mandatory or discretionary, organizations execute across operational areas in support of the organization's security policy framework. Each security process comprises a series of interdependent, linked actions executed in an orchestrated manner to achieve a specific security task or outcome. They help foster and embed a standardized approach to commonly performed security activities. In turn, this drives consistent, reliable, effective and measurable security control execution. See “The Security Processes You Must Get Right” and “Creating a Security Process Catalog” for further information.

Table 1 provides Gartner's definition for each of the key elements covered in this research note and provides examples of each.
### Table 1: Security Frameworks, Control Catalogs and Processes

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
<th>Uses and Applicability</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Framework</td>
<td>A comprehensive, structured set of processes for security and risk management.</td>
<td>Provides a structure to organize security controls to ensure they are complete and cohesive.</td>
<td>ISO27001:2017, NIST CSF, COBIT, HITRUST CSF</td>
</tr>
<tr>
<td>Security Process</td>
<td>A series of interdependent, linked actions executed in an orchestrated manner to achieve a specific security task or outcome.</td>
<td>Helps to foster a standardized, scalable approach to commonly performed security activities that helps to drive consistent, reliable, effective, and measurably security outcomes.</td>
<td>Security Governance, Security Policy Management, Security Awareness and Education, Identity and Access Management, Vulnerability Management, Incident Response</td>
</tr>
</tbody>
</table>

Source: Gartner (October 2019)

Figure 2 provides a view of the relationship between security management frameworks, control catalogs and security processes.
Figure 2. Relationship Between Security Management Frameworks, Control Catalogs and Security Processes

Identify Industry-Specific Frameworks, Control Catalogs and Security Processes Required by the Organization's Business Context

While there are several candidate frameworks and control catalogs to choose from, selecting one does not have to be an overly complex or time-consuming exercise. There is no need to reinvent the wheel and come up with your own standard. The hard work developing widely used security frameworks such as ISO/IEC 27001:2017 and the NIST CSF has already been done.

Selecting the organization's security framework and controls catalog is not rocket science. In fact, it doesn't really matter which framework or catalog you select, as long as you select something. However, SRM leaders should be mindful of their organization's unique internal and external context in the selection process. Table 2 provides some of the internal and external contextual factors to consider.
As a first step toward selecting a security framework and control catalog, determine whether there has been a security framework or controls catalog developed for your specific industry sector. Industry-specific standards such as the popular NIST CSF — originally designed for U.S. critical infrastructure providers — and others often map back to other globally accepted frameworks such as ISO27001. For government organizations, the decision is likely to have been made for you as per the examples provided below:

- **United States**: Federal government organizations are required to comply with the Federal Information Security Modernization Act of 2014 (FISMA 2014) with NIST SP800-53 providing the control catalog upon which security management must be based.

- **Australia**: Australian Commonwealth Government organization information and information systems are required to implement security measures that comply with the government’s Protective Security Policy Framework (PSPF) and Information Security Manual (ISM).

- **United Kingdom**: Organizations within Her Majesty’s Government (HMG) are required to meet a range of mandatory security outcomes contained in the United Kingdom’s Security Policy Framework published by the Cabinet Office.

---

**Table 2: Business Context Factors Influencing Security Framework and Control Catalog Selection**

<table>
<thead>
<tr>
<th>Internal Context Factors</th>
<th>External Context Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry sector</td>
<td>Regulatory and legislative requirements</td>
</tr>
<tr>
<td>IT process maturity</td>
<td>Government security requirements</td>
</tr>
<tr>
<td>Security capability maturity</td>
<td>Commercial supplier requirements</td>
</tr>
<tr>
<td></td>
<td>Access to local security talent and skills market</td>
</tr>
<tr>
<td></td>
<td>Competitive landscape</td>
</tr>
<tr>
<td></td>
<td>Customer and stakeholder expectations</td>
</tr>
</tbody>
</table>

Source: Gartner (October 2019)
SRM leaders need to also recognize not all the organization's information security requirements may be visible to the security team. SRM leaders must engage proactively with other parts of the organization such as legal, risk and front-line business units to identify discrete regulatory or legislative obligations that include information security requirements that need to be considered in control selection.

Recommendations:

- As part of the strategic planning process, scan your internal and external environment to identify the contextual factors that could influence your selection of security framework and control.
- Engage proactively with your business stakeholders to identify and document any regulatory, legislative or contractual obligations the organization has with regards to information security.

Select a Framework and Controls That Are Consistent With the Security Team's Capability and the Organization's Maturity

But what happens when there is no industry-specific or government-mandated security framework and control catalog? In this case, security capability maturity and team capacity and capability become the key inputs in selecting your security control framework and control catalog. Making this decision without an understanding of these aspects can lead to unwanted consequences including:

- Controls being implemented only partially or suboptimally leaving the organization still vulnerable.
- Wasted investment in time, skills and money being unavailable for initiatives that, if pursued, would have had a more measurable impact on the organization's risk exposure levels.

Saudi Arabia: All government entities and their affiliate organizations in the kingdom are required to comply with the Nation Cybersecurity Center (NCSC)'s Essential Cybersecurity Controls (ECC).
Selecting a framework that is overly complex and/or contains controls that require capacity and/or skills not present in the security team can lead to critical gaps between the requirements of the security framework and/or control catalog. These gaps will limit the effectiveness of those controls and don’t provide any meaningful impact in relation to reducing the organization’s risk exposure levels.

Additionally, more complex security frameworks and control catalogs could see smaller and already stretched security teams feel overwhelmed by the amount of work required to meet the requirements they set out. This can lead to increased stress levels and/or security team burnout. This will impact the organization’s ability to retain security talent and sustain the required capacity and capabilities required to achieve the security outcomes expected.

Understanding the link between security capability maturity and team capacity and capability is also important. Smaller security teams with lower security capability maturity will find simpler control security frameworks like the NIST CSF and control catalogs, such as the CIS CSC, easier and faster to implement. Larger teams at a higher level of capability maturity potentially have the capacity and ability to adopt more detailed security frameworks and control catalogs. This includes ISO27001 and ISO27002, however they could also choose the NIST CSF in conjunction with NIST SP800-53 as another option.

**Recommendations:**

- Use Gartner’s “IT Score for Security & Risk Management” to gain an understanding of your current security capability maturity levels.
- Review the security team’s capacity and capability levels to ensure the decision on a security framework and controls catalog does not overstretch existing resources.
- Use the information gathered in the above steps to help identify the candidate security frameworks and control catalogs that should be considered for the organization’s adoption.
Acronym Key and Glossary Terms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Glossary Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASD</td>
<td>Australian Signals Directorate</td>
</tr>
<tr>
<td>CIS CSC</td>
<td>Center for Internet Security Critical Security Controls</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>NIST CSF</td>
<td>National Institute of Standards and Technology Cybersecurity Framework</td>
</tr>
</tbody>
</table>

**Evidence**

This research draws on over 50 open discussions on “security frameworks” in Peer Connect, more than 250 inquiries since 2017 on security frameworks and over 100 inquiries around security processes in the same period.

It also draws on findings from Gartner's IT Score for Security and Risk Management between 2014 and 2018.

Finally, it also draws on multiple industry standards as outlined in the main body of the note.

---

**Recommended by the Authors**

Some documents may not be available as part of your current Gartner subscription.

- Guide to Information Security Controls Frameworks
- Market Guide for Organization Security Certification Services
- Toolkit: Security Capabilities Framework for SMBs
- ISO/IEC 27001:2013 Shifts Focus From the Effectiveness of Controls to Risk Treatment Plans
- Best Practices in Implementing the NIST Cybersecurity Framework
Actionable, objective insight

Explore these additional complimentary resources and tools for cybersecurity leaders:

- **Research**: How to Build a Robust, Defensible Security Program That Enables Business Growth and Agility
  - Build a defensible program that meets all your business needs.
  - [Download Research](#)

- **Sample Report**: IT Score for Security & Risk Management
  - Gain perspective on your highest-priority activities.
  - [Download Report](#)

- **eBook**: 3 Must-Haves in Your Cybersecurity Incident Response Plan
  - Improve your organization’s ability to prepare for an incident.
  - [Download eBook](#)

- **Infographic**: Are you a highly effective cybersecurity leader?
  - Learn about the key characteristics of highly effective leaders.
  - [Download Infographic](#)

Already a client?
Get access to even more resources in your client portal. [Log In](#)
Connect With Us

Get actionable, objective insight to deliver on your mission-critical priorities. Our expert guidance and tools enable faster, smarter decisions and stronger performance. Contact us to become a client:

**U.S.**: 1 844 466 7915

**International**: +44 (0) 3330 603 501

Learn more about Gartner for IT Leaders
gartner.com/en/information-technology

Stay connected to the latest insights

Attend a Gartner conference
View Conference