# Ten Cyber and IT Risk Fundamentals You Must Get Right

Published 19 October 2021 - ID G00743956 - 23 min read

By Claude Mandy, Jie Zhang

Security and risk management (SRM) leaders struggle to mature their cyber and IT risk management practices beyond conducting risk assessments. A set of fundamental risk management processes are essential to manage cyber and IT risk for their organizations.

## Strategic Planning Assumption(s)

By 2025, 60% of organizations in highly regulated industries will create a dedicated cyber risk management — or equivalent function — providing cyber risk expertise, support, monitoring on cyber risks and challenging risk-related decisions by security and risk management leaders.

## Analysis

### The Pressure Is on to Get Cyber and IT Risk Management Right

Costly ransomware attacks, data breaches and technology outages affecting major corporations have become a regular facet of the 24-hour news cycle in 2021. The View from the Board of Directors Survey 2022 [1] found that 88% of respondents viewed cybersecurity-related risk as a business risk, not just a technology risk. In addition, 51% of respondents had experienced a cyber-security risk incident in the past two years. The heightened concerns around cyber and IT risk (see Note 1) place security and risk management (SRM) leaders under constant pressure to demonstrate effective management of cyber and IT risk.

The increased concerns from stakeholders has led to increased scrutiny on cybersecurity from:

- Boards: After years of quarterly reporting on cyber risk to boards, boards are noticeably less confident in their organization's security posture and the quality of cyber and IT risk information provided to them by management. This increased scrutiny is evidenced by the creation of specific cybersecurity committees at the board level responsible for strategy and risk management, as well as 54% of respondents to the View From the Board of Directors Survey 2022, indicating that Cybersecurity is almost always on the Board Agenda.
- Regulators: Against a backdrop of a dynamic risk landscape, regulators are speeding up modification or release of regulations. This demands that organizations be more proactive in concerning areas such as cybersecurity, outsourcing and privacy. The increased regulatory

risk from these emerging regulations is creating pressure on SRM leaders to also demonstrate compliance.

- Customers: The growing reliance on technology vendors and service providers to realize an organization's strategic and operational objectives — and the steady expansion of industry and geographic regulatory requirements, as well as significant third- and fourth-party cybersecurity breaches — are forcing customers to focus their attention on their vendors. This increased scrutiny by customers is evidenced by the expansion of the IT Vendor Risk management market.

The practice of cyber and IT risk management can play a significant role in ensuring that organizations achieve their objectives and generating collective confidence across all stakeholders. However, this is made more difficult by evolving external threats, increasingly dynamic regulatory and audit requirements, and widespread adoption of modern IT delivery methods. The speed of change in these areas continues to increase. With every change, risk becomes more complex and far-reaching; and the need for prioritizing ongoing investment becomes a more immediate need.

### Fear, Uncertainty and Doubt Aren't Sustainable

Organizations that do not yet have foundational risk management capabilities in place to respond to these demands struggle to convince stakeholders of the value of risk management — let alone effectively prioritize treatment of risks based on their objectives, address known issues and create business opportunities. Instead, they are forced to resort to negative themes as the basis for investment in needed risk mitigations. The use of scare statistics, inflated risk exposures, competitor failures — and other fear, uncertainty and doubt messaging is commonplace.

These approaches may help obtain support to address immediate shortcomings, but reduce their long-term success. It is inevitable that stakeholders will either stop paying attention or question the validity of the message, where the same negative themes are used long term (i.e., the "boy who cried wolf" syndrome). The long-term success of risk management for any organization can only be measured by keeping the organization in business and out of trouble long term.

### Which Processes Are Needed for Long-Term Success?

There are multiple industry risk management frameworks that already describe the expected steps or processes for management of cyber and IT risks — and even describe the principles needed for an effective risk management program (see Note 2).

The most common are NIST 800-39 and ISO 27005. Both approaches are very comprehensive, but focused on two different decisions essential for keeping the organization out of trouble.

- ISO 27005 describes an iterative process for management of a single risk and is best suited

for an assessment of one risk at a time. It focuses on the decision-making process for how best to treat a risk.

- NIST 800-39 describes an iterative process for managing risks of a single system in the context of a system development life cycle (SDLC) process, and is best suited for managing risk when developing systems or new projects. It focuses on the decision-making process for building new systems against a defined set of control requirements.

Unfortunately, most organizations adopt only one of these frameworks when documenting their approach. This is usually sufficient to keep auditors and regulators comfortable with knowing that the organization has a risk management function. Gartner recommends that each organization adopts an approach that best fits the needs, requirements, objectives and culture of the organization, and allows risk to inform all business decisions — particularly cyber and IT risk decisions.

As illustrated in Figure 1, Gartner's Cyber and IT risk management framework provides a unified approach that is suitable for embedding risk management in both new systems and existing systems, accommodating best practices from NIST 800-39 and ISO 27005. This unified approach provides SRM leaders with the ability to synthesize and prioritize risk information to guide cyber- and IT risk-related decision making related to the development of new systems and the ongoing management of existing systems.

Figure 1: Gartner's Cyber and IT Risk Management Framework

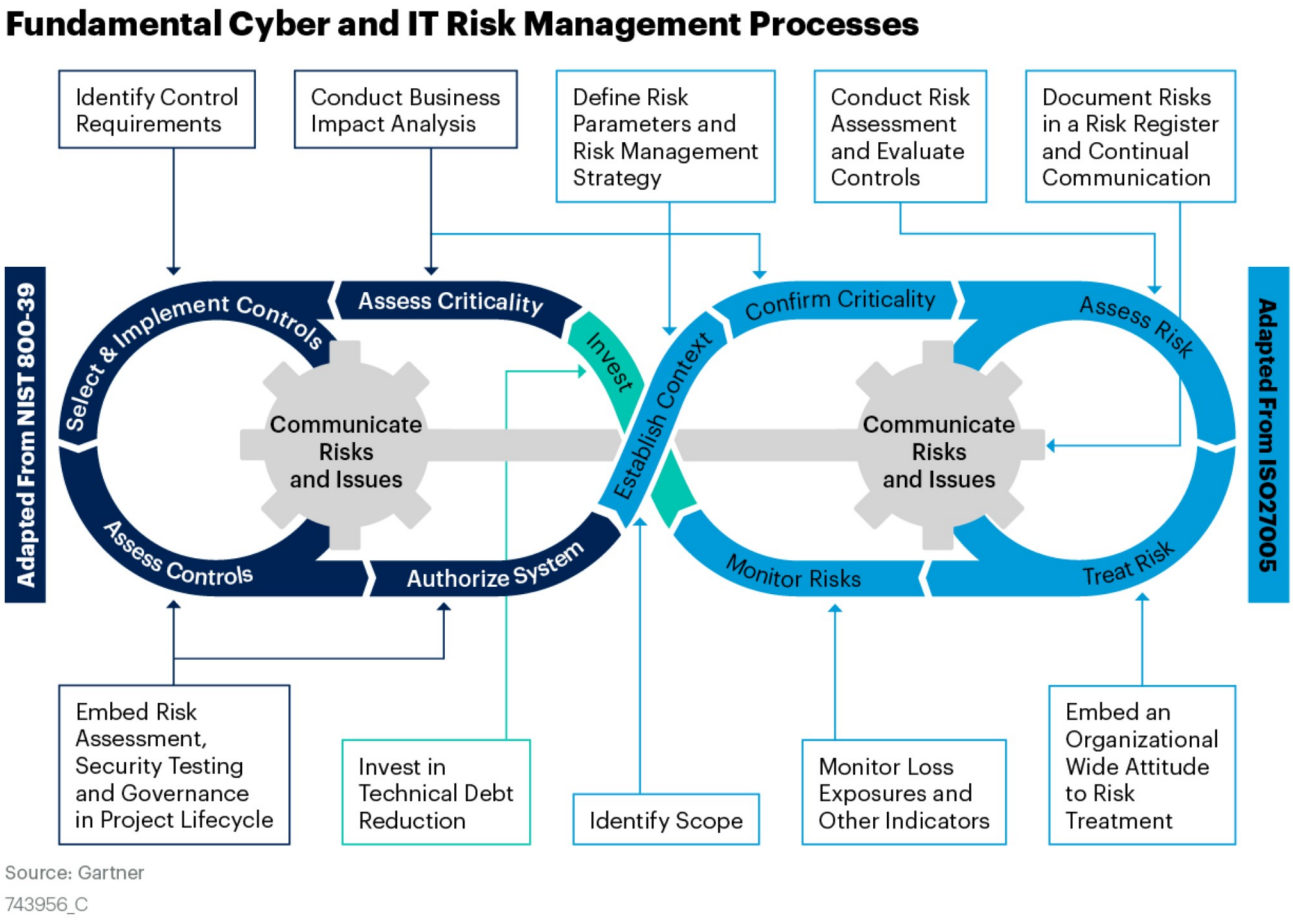

Source: Gartner
743956_C

Gartner

Within this unified framework, Gartner has identified ten specific risk management processes that are considered to be the fundamental components required to ensure success of cyber and IT risk management within your organization. This can be accomplished by embedding risk management within key decisions related to the development of new systems and the ongoing

management of existing systems.

Figure 2: Fundamental Cyber and IT Risk Management Processes




This research roundup provides a selection of recommended reading for these identified processes, but it is important to remember that the independent performance of the processes in itself is no guarantee of long-term success. Long-term success can only be achieved where risk management increases the likelihood of the organization achieving its key strategic goals and objectives. This requires risk management to be embedded in all strategic decision making, across all organizational processes.

This can only be achieved by robust governance and a decision-making culture where risk is used to improve decision quality.

## Research Highlights

*Some recommended content may not be available as part of your current Gartner subscription.*

### Define Risk Parameters and Risk Management Strategy

Risk parameters are the elements that outline the parameters that guide managing risk; while the risk management strategy communicates the organization's approach to risk management. Risk parameters provide documented guidance for the following:

- Estimation of the impact of specific risks (this may be quantitative or qualitative)
- Estimation of the frequency of occurrence of risks
- Evaluation of risks based on the impact and frequency
- Understanding of the scope
- Acceptable levels of risk as determined by risk appetite and risk tolerance

The development and documentation of these risk parameters are essential in helping an organization to systematically assess, treat and accept risks consistently in a structured way across the organization. Without well-documented and understood parameters, organizations will struggle to consistently make risk-based decisions. They also struggle demonstrating to auditors, regulators and other stakeholders that they are serious about risk management without documented parameters for risk management and a clear strategy for managing cyber and IT risk.

The parameters and strategy are usually documented in an overarching risk management framework and should be periodically updated.

**Suggested Reading**

7 Critical Elements of a Security Risk Management Framework

Case Study: Risk Response Decision Matrix (FirstSeed*)

Action-Oriented Risk Matrix (Power Co.)

### Identify Scope

Cyber and IT risks are pervasive. The scope can include potential risk events caused by any number of cyber or technology root causes — including threats or technology failures (i.e., cyber and IT risk exposures). These exposures can be existing or new exposures that are delivered into the business as a result of IT or business projects that leverage IT assets.

---

*Cyber and IT risk exposures can include, but are not limited, to:*

- *Cybercrime (including ransomware, business email compromises, phishing and denial of service attacks)*
- *Online brand and reputational damage (including social media misinformation and fraudulent mobile apps)*

- *Theft, loss or improper access to data*
- *Technology failures (including software, network, cloud infrastructure)*

---

The scope can also consider other operational risk events that may impact cybersecurity and IT functions themselves (i.e., operational risk exposures to cybersecurity and IT functions). The operational risk exposures may be further caused by cyber and IT risk exposures.

---

*The operational risk exposures to the Cyber and IT functions can include, but are not limited to, the following risk exposures:*

- *Data management (including data quality, inadequate data retention)*
- *Third-party risk (including third-party IT and security control failures)*
- *Disaster recovery (including IT outages as a result of natural disasters)*
- *Physical security for IT assets*
- *Safety of IT staff*
- *Legal noncompliance*
- *Transaction processing and execution failure*
- *Regulatory compliance*
- *Internal and external fraud*

---

These can impact not only the organization and its IT systems, but also its customers and suppliers too. It is important to understand the scope to:

- Further tailor the risk management processes to different elements of the scope. For example, approaches to assess risk for traditional on-premises systems managed in-house will differ compared to use of a cloud service, where it is more reliant on the cloud service provider.
- Tailor the depth and approach to the breadth of the scope. For example, a broad scope in a complex organization will require a significant amount of resourcing or compromises on the quality of the assessment. Conversely, a narrow scope may exclude risks that can

significantly impact the organization.

An accurate and up-to-date inventory of the systems, vendors, etc., in scope is essential at the risk assessment stage to provide SRM leaders with an increased understanding of the business value, the dependency of business processes on them and risks associated with technology aspects. The growth of digital business and its plethora of component assets (e.g., Internet of Things [IoT]), emerging technologies (e.g., artificial intelligence [AI], automated tools) and delivery models (cloud, as-a-service) are forcing organizations to more effectively and proactively manage dynamic, hybrid technology environments and their rapidly expanding volumes and types of technology assets.

Where an accurate and up-to-date inventory isn't maintained already, SRM leaders can develop their initial scope by determining the most relevant sources for information on the systems, vendors and applications used by the organization. This could be from an IT Asset discovery tool or directly from the people within the organization.

**Suggested Reading**

Reduce Audit Costs and Risks With a Comprehensive IT Asset Management Strategy

How to Successfully Choose an IT Asset Discovery Tool for Service Dependency Mapping

Break the CMDB Failure Cycle With a Service Asset and Configuration Management Program

### Conduct Business Impact Analysis

Organizations are made up of a complex web of activities and supporting infrastructure — including business partners, internal dependencies and IT partners in the delivery of its services. Unexpected disruptions can result in a failure to deliver services to customers with the resultant impact on revenue, reputation, life/safety and strategic objectives.

A well-conducted BIA is the most effective way of measuring the impact of disruptions to the business. The BIA will help the business determine critical activities, their recovery time objectives (RTOs) and maximum acceptable outages (MAOs). In addition to helping organizations develop recovery strategies, solutions and plans for critical activities, these insights are useful for classifying IT assets, prioritizing remediation activities of risks and informing the risk appetite for extended outages. The BIA is essential with helping SRM leaders prioritize based on the criticality of systems and vendors to the business.

**Suggested Reading**

Fundamental Elements of Business Continuity Management — Governance and Program Management

The Business Impact Analysis: A Digital Business Essential

2021 ERM Risk Response Accelerator: Business Continuity and Organizational Resilience —

Topic Guide

2021 ERM Risk Response Accelerator: Business Continuity and Organizational Resilience — Toolkit

### Identify Control Requirements

SRM leaders are fortunate that as an industry, significant investment in developing a set of control catalogs has already been completed. Control catalogs describe “how” the organization could implement its control environment. They do this by providing a menu of controls the security team can choose from based on the catalog or 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. The variety of overlapping control catalogs can be confusing, particularly when overlaid against existing internal policies.

Gartner recommends developing a rationalized set of control requirements mapped to the organization’s internal policies, external industry standards, other regulatory requirements and even contractual requirements.

**Suggested Reading**

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

Information Security Controls Mapping Tool

Rationalized Compliance Framework (Pfizer)

### Conduct Risk Assessment & Evaluate Controls

A risk assessment may be one of the most overused terms within risk management — mainly as it is the basis for all decision making around risk. SRM leaders know that they should do some form of risk assessment, but struggle to determine what type of risk assessment is needed and what risk assessment methodology is best suited. The three types of risk assessments are:

- One-time assessment: These are ad hoc, one-off or special-purpose assessments often performed in “new territory” that may be requested following a specific trigger.
- Tollgate assessment: These go/no-go, approval or quality assurance assessments are performed in support of larger processes with governance and risk, or project management objectives.
- Portfolio assessment: These are scheduled assessments that are usually identified during periodic (i.e., annual, quarterly) or just-in-time risk management planning in support of an enterprise risk management or compliance objective.

Performing a risk assessment can be also based on either a qualitative, quantitative or hybrid risk assessment methodology. Furthermore, risk assessments can be performed on an inherent risk basis or residual risk basis. Organizations looking for greater assurance conduct not only an evaluation of the design of the controls, but further testing on the effectiveness of the controls as well.

Regardless of the type and methodology, SRM leaders should tailor the risk assessment to the decisions expected as a result of the risk assessment.

**Suggested Reading**

Best Practices for a Successful Security Risk Assessment

A Data Risk Assessment Is the Foundation of Data Security Governance

6 Principles for Digital Business Risk Assessment

4 Steps to Optimize Your RCSA

**Document Risks in a Risk Register and Continual Communication**

SRM leaders are adept at identifying the numerous technical causes of cyber and IT risk, but can be overwhelmed by the volume of technical issues identified. Using a strictly technical and granular summary of issues identified to assess and express these risks is useful for tracking remediation, but does not resonate with business leaders. The inability to communicate effectively to the business severely limits the usefulness of risk assessments and the influence of security and IT risk management teams. A risk register is critical to help the SRM leader provide a high-level overview of cyber and IT-related risks stated from a business perspective. The use of an enterprise risk register is encouraged. A well-designed risk register can be used to:

- Guide the risk assessment process and methodology
- Consistently record, prioritize and organize the outputs of the risk assessments
- Track treatment of risks and remediation of granular technical issues related to the risks
- Continually communicate on status of risks

The ability to communicate risk is essential with helping an organization prioritize and make decisions to increase the likelihood of the organization achieving its key strategic goals and objectives. There are several situations in which such communication is essential:

- Sharing or exchanging risk-relevant information with stakeholders
- Supporting a risk treatment decision-making process

- Identifying risks with the help of cross-functional teams
- Consulting others about risks and consequences
- Making employees aware of risks and appropriate behavior
- Helping to report risks to authorities
- Conveying a sense of responsibility for risks

The communication of risks should focus not on providing more risk information for business decision makers to sift through, which increases risk consideration, but does not actually improve decision quality. Rather, SRM leaders should focus their communication on helping decision makers make sense of the risk information available to them. For decisions to be adequately risk-informed, decision makers must be aware of, and fully understand, all risks that could:

- Result from the decision
- Threaten the objectives of the decision
- Hinder the decision maker's role or function
- Affect the broader enterprise

Synthesizing and prioritizing risk information, and preparing and guiding decision makers, can help the organization take advantage of opportunities that may have been perceived to have been too risky due to a lack of clarity.

At a minimum, effective risk communications must be objective, pragmatic and clearly focused on the best interests of the organization to ensure that activities are aligned with business requirements. They must clearly state why a certain risk is relevant to the organization to enable the business to prioritize and make decisions.

**Suggested Reading**

Toolkit: Document Your Cyber and IT Risks in a Risk Register

Methods to Ensure Continuous Risk Identification in Your Organization

Toolkit: A Practical Risk Heat Map That Drives Change and Growth

Effective Risk Communication for the Technical Professional

The Risk-Enabled Enterprise: ERM's Role in Risk-Informed Decision Making

**Embed Risk Assessment, Security Testing and Governance in Project Life Cycle**

Enterprises can benefit from having a standard project life cycle (see Note 3) in place to guide projects on the path to completion. Tollgate risk assessments can be effective in validating that projects manage risks to the project and to the organization appropriately.

The Authority to Operate methodology prescribed by NIST 800-39 is a suitable approach to verify that security requirements have been met before operationalizing a system. This approach is commonly adopted by organizations seeking FedRAMP and other system-focused certifications.

These go/no-go decisions are the final opportunity to avoid introducing serious, expensive and possibly immutable security risks into the enterprise, and it is critical to ensure that risk is a key component of the governance. Organizations should note that too much reliance on such toll gates can be perceived to slow down projects and programs. In contrast, agile teams prefer to use frequent feedback, automated and received at regular intervals, to recalibrate teams and products.

To avoid introducing serious, expensive and possibly immutable security risks into the enterprise through the project, it is critical to ensure that security tools (including application security testing tools and vulnerability management) are integrated where possible. Additionally, security resources must be embedded in the project methodology adopted by your organization based on the project's risk and criticality.

**Suggested Reading**

Structuring Application Security Tools and Practices for DevOps and DevSecOps

Integrating Security Into the DevSecOps Toolchain

Ignition Guide to Establishing and Conducting Project Risk Assessments

Risk and Control Resources for IT Project Management and Governance

FedRAMP Demystified

### Embed an Organizational Wide Attitude to Risk Treatment

Ensuring that risks are treated appropriately is arguably the single most important risk management process within an organization. Organizations should ensure that the relevant governance body formalizes the organization's risk acceptance and risk treatment procedures to ensure that it is apparent for clearly defined risk exposures:

- How much risk is acceptable in pursuit of business objectives
- Who can the risk be accepted by
- How long can it be accepted for
- How best to deal with the unacceptable risk

- When treatment should be completed

A risk treatment plan may not only need to address risks to individual parts of the organization, but also other functions and the organization as a whole. This requires individuals within the organization to be willing to look beyond their areas of responsibility to focus on the best interests of the organization. This may require risk management training or risk management to be embedded in existing training programs.

The attitude toward treatment of risks plays a significant role in the overall culture toward risk management. Where the attitude toward risk treatment is inconsistent between senior management and operational teams, this leads to misleading perceptions of the organization's risk. For instance, a management team who attempts to eliminate risk completely and, as a result creates unrealistic time frames for remediation, may create an organization unwilling to identify risks for fear of repercussions. Organizations should instill an approach to risk treatment that emphasizes determining the optimal treatment in a given situation to increase the likelihood of the organization achieving its key strategic goals and objectives. The achievement of the organization's strategic goals and objectives should always be prioritized over a quick fix, or the reduction of risk in its own right.

**Suggested Reading**

Institute Cybersecurity and Risk Governance Practices to Improve Information Security

Toolkit: Document Your Cyber and IT Risks in a Risk Register

Measure and Motivate a Risk-Smart Culture

### Monitor Loss Exposures and Other Indicators

Plenty of idioms and memes encourage individuals to learn from mistakes. A robust risk management program not only learns from its own mistakes — improving the processes of risk management — but learns from mistakes both internal and external to the organization. If it happened to another organization, it could happen to yours.

A retrospective review of incidents and root cause analysis are powerful tools to help validate the:

- Organization's assessment of risk (frequency and impact)
- Adequacy of controls needed
- Effectiveness of your risk management program

However, relying solely on incidents can result in a very reactive risk function. Analyzing the primary root causes of the risk exposure can help identify leading indicators — which can help make course corrections and avoid (or mitigate the impact of) incidents. Leading organizations

develop key performance indicators to track performance of the risk management function and organization, key risk indicators to monitor specific risks and key control indicators to measure the effectiveness of existing controls.

**Suggested Reading**

Methods to Ensure Continuous Risk Identification in Your Organization

Define the Root Causes of Risk Events— Vanguard

Tool: Root Cause Analysis Template

Post-Mortem Review

Metrics to Prove You CARE About Cybersecurity

How to Develop Key Control Indicators to Improve Security Risk Monitoring

**Invest in Technical Debt Reduction**

Overtime organizations accumulate substantial technical debt that limits the ability of the organization to address risk without significant investment or replacement. This increasing technical debt not only increases risk from obsolete technology, unpatched vulnerabilities and lack of vendor support, but greatly impacts the long-term performance of resources, workflows, capabilities and mindsets around it — and the organization's ability to achieve its long-term objectives.

The risk of technical debt would be identified as risk by other risk management processes, however, current risk management approaches fall short in proactively planning and driving technical debt reduction. Technical debt reduction through these approaches is impossible to justify when focusing solely on the short-term losses and consequences versus cost of significant upgrades, which encourages organizations to identify lower cost compensating controls.

The creation of a specific formal planning process within Gartner's cyber and IT risk management framework is intended to highlight that addressing the risk of technical debt long term should be based on the assessment of risk in achieving the organization's long-term business objectives and not only short-term losses and consequences. SRM leaders should consider technical debt reduction as a key driver and requirement for new IT projects.

**Suggested Reading**

How to Assess Infrastructure Technical Debt to Prioritize Legacy Modernization Investments

Address Technical Debt With Gartner's PAID Model and Avoid Bankrupting Your Application's Future

Manage Technology Debt to Create Technology Wealth

The Essential Elements of Effective Vulnerability Management

## Evidence

[1] Gartner View From the Board of Directors 2022 Survey: This study was conducted to understand how BoDs will address the risk from economic and political volatility and a multipolar world, and their intent to convert digital acceleration to digital momentum. The survey also helps understand the impact of the key societal issues that took center stage during the pandemic on BoDs' strategy and investment approaches.

The survey was conducted online from May through June 2021 among 273 respondents from the U.S., Europe and Asia/Pacific. Companies were screened to be midsize, large or global enterprises. Respondents were required to be a board director or a member of a corporate board of directors. If respondents serve on multiple boards, they answered for the largest company, defined by its annual revenue, for which they are a board member.

The survey was developed collaboratively by Gartner analysts and the Research Data and Analytics team.

*Disclaimer: Results of this study do not represent global findings or the market as a whole but reflect sentiments of the respondents and companies surveyed.*

In preparing this research, Gartner also used a combination of information from interactions with clients, real-life case studies and the following industry standards:

- ISO 31000:2018, "Risk management — Guidelines"
- ISO/IEC 27005:2018, "Information Technology — Security Techniques — Information SRM"
- NIST Special Publication 800-37 R2, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy"

## Note 1: Definition of Cyber and IT Risk

Cyber and IT risk refers to internal and external exposures that impact the goals and values of the organization due to operating in interconnected digital environments. Such exposures are linked to digitization, technology adoption and adoption patterns, and the pace of modernization. IT risk exposures are generally associated with core IT systems ranging from endpoints, networks, applications and platforms to data and information flow. Cyber risk extends IT risk to include the external risks that an organization exposes itself to when connecting to the outside digital world. These risks are normally associated with third parties, supply chains, customers and prospects.

## Note 2: Analysis of current industry standards

The 11 guiding principles defined within ISO 31000 are explicit statements of intent that should

form the basis of an effective cyber and IT risk management program.

> **For risk management to be effective, an organization should at all levels comply with the principles below. Risk management creates and protects value Risk management is an integral part of all organizational processes Risk management is part of decision making Risk management explicitly addresses uncertainty Risk management is systematic, structured and timely Risk management is based on the best available information Risk management is tailored Risk management takes human and cultural factors into account Risk management is transparent and inclusive Risk management is dynamic, iterative and responsive to change Risk management facilitates continual improvement of the organization**
>
> *— Extract from ISO 31000:2018, "Risk management — Guideline"*

## Note 3: Project Life Cycle

The use of the term "project life cycle" is deliberate in this context. For developers, this term can be interpreted more narrowly to refer to specific forms of this concept (e.g., "software development life cycle" or "solution development life cycle"). However, the accountability of the goes beyond this — for example, the secure design to support a physical location in a new country. For "project life cycle."