McKinsey & Company

Cybersecurity Practice

Creating a technology risk and cyber risk appetite framework

Here's how to build a comprehensive, measurable, and objective end-to-end risk appetite framework as a foundation for managing technology risk and cyber risk.

This article is a collaborative effort by James Kaplan, Charlie Lewis, Lucy Shenton, Daniel Wallance, and Zoe Zwiebelmann, representing views from McKinsey's Cybersecurity Practice.

August 2022

When it comes to technology risk and cyber risk, financial institutions are increasingly shifting toward a risk-based approach to determine their priorities for controls. Those controls should be based on their current security capabilities, the likelihood of threats, and the impact of any potential cyber breach. However, the question remains: can organizations really make strategic, objective decisions about which controls they should and should not implement, given their appetite for technology risk and cyber risk?

Risk-based management measures risk against an organization's risk appetite to determine where further technology and cyber controls are needed. The goal is to reduce the remaining technology and cyber risks to a point the business can tolerate. To succeed, it must have clear, measurable statements on its technology risk and cyber risk appetite, defined in business terms, with clear ownership.

In addition, regulators are now pressuring organizations to better articulate their risk appetite. A clear risk appetite statement is the cornerstone of successful risk-based management. Major regulators—for instance, the Office of the Comptroller of the Currency—have recently issued findings to major US banks about how to define and structure their technology risk and cyber risk appetites. It is believed that this trend will also be seen in Europe, as the European Banking Authority has already set out guidelines for managing cyber risk and continues to see it as an emerging concern. However, though regulators have described the characteristics of an optimal cyber risk appetite framework, there is no consistent picture of what the risk appetite should actually be or how to implement it across an organization.

Because of this lack of direction, financial institutions often struggle to understand how they should build a risk appetite framework that meets regulatory expectations and provides real value as a basis for decisions.

Clarifying the risk appetite framework

Many organizations find that they already have components of an optimal risk appetite framework (such as thresholds for key risk indicators) or overarching, enterprise-wide statements that present the overall appetite for risk as high, medium, or low. These organizations, however, struggle to measure their risk appetite against real-world business events and to agree on risk appetite–based thresholds for metrics.

For example, it is easy for organizations to say that they have a low appetite for cyber risk. But debate begins when they ask what constitutes such a low appetite in terms of control implementation and when the first and second lines of defense ask whether residual risk falls within or outside of that overall appetite. To manage technology risk and cyber risk effectively, organizations must lay out an objective risk appetite framework that supports business decisions on risk and uses objective metrics and reporting to achieve alignment with the risk appetite.

Financial organizations need a systematic, impact-driven structure that communicates their technology risk and cyber risk appetites, from the board level down to control objectives and metric thresholds. Determining the risk appetite should be a team activity that takes into account the needs of various stakeholders, including the board, the business, the technology function, and the second line.

The technology risk and cyber risk appetite framework

Risk appetite frameworks, structured against the technology risk and cyber risk taxonomies, should cascade from the risk taxonomy to control objectives and support metric thresholds.

The technology risk and cyber risk taxonomies should encompass all current and emerging technology risks and cyber risks. Organizations commonly structure taxonomies according to the

possibility that different impacts of technology risk or cyber risk will be realized. For example, the tech and cyber taxonomy may be structured by availability loss of systems, confidentiality compromise, data integrity compromise, project management risks, or any combination of those possibilities.

Once the key risks are understood, organizations should define their appetite for them. Such an enterprise risk appetite statement should not only be business oriented and quantitative but also correspond to the technology risk and cyber risk taxonomies. In addition, these quantitative statements should be stratified by importance to the business. For example, enterprise risk appetite statements for the unavailability of systems might be "no more than X minutes of unplanned downtime for systems associated with critical business services" and "no more than Y minutes of unplanned downtime for systems associated with noncritical business services."

The organization should then design control standards and control patterns based on these risk appetite statements. The control objectives should cover all types of technology and cyber controls (which would ideally map to industry standards) and should be ranked by importance to the business. They should also be measurable, so that organizations can track adherence to their control objectives through metrics (see sidebar, "Case in point").

Finally, organizations should create thresholds for key risk indicators (KRIs) to measure if risk is within tolerance, as well as key control indicators (KCIs) to compare the performance of controls with the control objectives. For example, a KCI for multifactor authentication control could be the percentage of applications handling business-critical data with multifactor authentication. A KRI could be the number of instances of unauthorized access to business-critical data as a result of breached access controls.

Case in point

The following is a scenario for the appetite statements and thresholds of each component in a bank's threshold framework. It uses data leakage as an example.

This is an enterprise appetite statement for data leakage risk:
The organization does not tolerate any loss of more than *X* megabytes of high-sensitivity data a year. It does not tolerate any loss of nonsensitive data that leads to significant reputational damage or to regulatory fines and reviews.

This cascades down to control objectives:

— All vulnerabilities on critical systems must be patched within *Y* hours of patch release.

— All vulnerabilities on noncritical systems must be patched within *Z* hours of patch release.

Then the organization determines key control indicators and key risk indicators to track enterprise data leakage:

— For the percentage of applications processing critical data with open vulnerabilities, the metric threshold is *A* percent.

— For the percentage of severity-one, -two, and -three security incidents of data leakage identified through data loss prevention, the metric threshold is *B*.

The enterprise appetite statement now cascades down to a statement for the business units, such as a retail bank:
The retail bank does not tolerate any loss of more than *Y* megabytes of high-sensitivity data a year. For nonsensitive data, the retail bank does not tolerate any loss of data that leads to significant reputational damage or regulatory fines and reviews.

An organization should set the risk appetite together with the technology teams, basing it on how much technology and data impact they would accept to achieve business objectives.

Risk appetite statements at the business unit level should reflect risks and key drivers relevant to specific units. Such statements should generally cascade down from enterprise-level risk appetite statements, but business units with unique needs and value propositions can have independent ones.

Why develop a risk appetite framework?

Risk-based management succeeds only if measured against the business-oriented risk appetite. Implementing a structured, comprehensive risk appetite statement aligned across the business, the technology function, and the second line has multiple benefits, including these:

1. supporting transparent communication with the board on the level of technology risk and cyber risk, to enable business-oriented discussions on investments and priorities

2. creating an objective platform for discussion between the first and second lines of defense about the level of residual risk

3. helping both the first and second line to give regulators objective evidence that the organization is effectively managing tech risk and cyber risk against the risk appetite

Designing and implementing a risk appetite framework

There are three key considerations for designing and implementing a risk appetite framework: understanding what's currently in place, aligning with the business, and leveraging automation where possible.

Understand what's currently in place. Many organizations already have components of a risk appetite framework but lack an end-to-end structure fully linked to control objectives. To determine how to advance further, they should understand which capabilities they already have.

Align with the business. An organization's risk appetite should be measurable and aligned with business objectives. The business should set the risk appetite together with the technology teams, basing it on how much technology and data impact they would accept to achieve business objectives. Those technology teams should ask the business questions, such as how many minutes of unplanned downtime it is willing to accept for a specific business service, how much sensitive data it would accept losing to achieve its objectives, and what combination of cyber investment, cyber control, and business enablement it needs to manage cyber risk during day-to-day operations. These insights should determine the organization's risk appetite and the associated control objectives.

Leverage automation where possible. Advances in technology make it easier to enforce and apply controls for different systems automatically—for example, through policy-as-code[1]—based on levels of residual risk. Identifying opportunities for using automation to apply controls in line with the risk appetite and to measure the degree of overall alignment with it will ensure a more sustainable environment for risk management.

Developing, understanding, enforcing, and executing an appetite framework for tech risk and cyber risk is a complex challenge that requires good data, extensive monitoring, and coordination among the business, the technology function, and the second line. There is plenty of difficult up-front work to get the tech risk and cyber risk appetite right, but organizations will reap strong dividends from enabling their business objectives by knowing and understanding just where their technology and cyber strengths lie.

Regulatory requirements in highly regulated industries, such as financial services, often force the creation of strong risk appetite frameworks. However, establishing a solid technology risk and cyber risk appetite has benefits not only for regulated industries but also for organizations across all industries, which would gain by managing technology risk and cyber risk against a business-impact-oriented risk appetite.

James Kaplan is a partner in McKinsey's New York office, where **Daniel Wallance** is an associate partner; **Charlie Lewis** is an associate partner in the Stamford, Connecticut, office; **Lucy Shenton** is an associate partner in the Berlin office; and **Zoe Zwiebelmann** is a consultant in the Hamburg office.

Designed by McKinsey Global Publishing

[1] Managing rules and conditions with code.