A Complete Guide to Cybersecurity Risk Management

Learn the ins and outs of risk management and how it applies to compliance.

DRATA

Drata.com

DRATA

Table of Contents

DRATA

Risk Management, Defined

Cyber incidents topped the Allianz Risk Barometer for just the second time in the survey's history in 2022, listed as even more impactful than business interruptions. Considering the waves of impact from the global pandemic, this is an alarming data point. As the number of threats grows, so do the concerns that companies have and unfortunately, many of them have experienced the very real consequences of not managing these risks well.

The good news is, with the right knowledge and processes, you can mitigate the negative impacts of any potential threats. To help you implement a robust risk management plan, this guide provides an overview of IT AND cybersecurity risk management including what it is, why you need it, and how to make it work for your organization. In order to put this into context, let's define what risk management means in regards to IT and then cybersecurity.

Information Risk

Information risk is an estimate of the probability that something or someone will gain access to and maliciously or unintentionally manipulate the confidentiality, integrity, or availability of the data your organization handles. Here are some helpful terms that will help you better understand information risk:

Threat Actor: A threat actor is a human or non-human entity such as malware that exploits a vulnerability in your information systems.

Vulnerability: Some common vulnerabilities that threat actors take advantage of are a lack of data encryption, missing means of authentication, weak passwords, and more.

Outcomes: Outcomes are the result of the exploited vulnerability. This may be a threat actor gaining access to confidential information or widespread malware on company devices.

Impact: Not to be confused with outcomes, impacts are the consequences of outcomes. For example, if a threat actor gained access to confidential user information, customers may no longer trust your company with their information. It could also result in legal/regulatory issues for your organization and negative public relations.

Asset: An asset is a foundational piece of information risk. It's the data, process, or piece of technology that has been exposed to the threat actor through a vulnerability.

Cybersecurity Risk

Moving a step further than your network infrastructure, cybersecurity risk management is the process of handling cybersecurity risks which includes identifying, analyzing, evaluating, and addressing. It's a vital part of running any organization, but it can be an uphill battle to get right.

> **It's not easy to keep up with new threats that arise and it's even more challenging to keep everyone in an organization educated and proactive on security threats.**

One of the primary outputs of a risk management strategy is the risk management plan (more on that later), which more specifically is documentation that helps you to identify and prioritize your organization's cybersecurity risks, evaluate them, and respond to them. All in an effort to keep your data secure and ensure that everyone on your team sticks to the best practices that you establish.

Having this plan will help you prioritize your efforts so that those with the greatest possible impact are addressed first. It will also make sure you don't overlook anything important along the way and creates consistency in how you handle risks.

Now that you've got the context and understanding of the two kinds of risk management discussed in this guide, let's hone in on how this applies to your organization, your industry, and the role it plays in compliance and regulations.

DRATA

Applying Risk Management to Compliance and Regulations

Nearly every business needs to meet some kind of compliance requirement. You might be using your compliance posture to build customer trust or be in a heavily regulated industry like **healthcare** or **financial services**. In either case, most compliance mandates require you to understand your risk tolerance before putting controls in place to mitigate the leftover risk.

Identifying, assessing, and analyzing risk can be overwhelming for many companies. You may struggle with knowing where to start or how to set goals. However, a risk management framework enables you to create repeatable processes that allow you to define, review, and mitigate IT risks to more effectively set and monitor controls.

Understanding Risk Management Frameworks

A risk management framework (RMF) is a set of practices, processes, and technologies that enable an organization to identify, assess, and analyze risk to manage risk within your organization.

A building block for any strong compliance program, a risk management framework typically follows these steps:

- Identify
- Assess
- Analyze
- Determine risk tolerance
- Implement controls
- Monitor and update

If you are in the United States, NIST is one of the most common risk management frameworks you'll come across, so let's start there.

NIST

The National Institute of Standards and Technology (NIST) Risk Management Framework sets out a risk-based approach for governing security, privacy, and cyber supply chain risk management. The NIST RMF consists of the following seven steps:

- **Prepare:** Activities that set the stage for managing security and privacy risks
- **Categorize:** Using an impact analysis to organize the systems and information they process, store, and transmit
- **Select:** Determining the controls that will protect the systems and data
- **Implement:** Deploying controls and documenting activities
- **Assess:** Determining whether the implemented controls work as intended and produce the desired results
- **Authorize:** Having a senior official authorize the system to operate
- **Monitor:** Reviewing controls to ensure they continue to mitigate risks as intended

COBIT

Established by ISACA (previously known as the Information Systems Audit and Control Association), the COBIT Framework focuses on enterprise governance and consists of these primary principles:

- **Principle 1:** Meeting stakeholder needs
- **Principle 2:** Covering the enterprise end to end
- **Principle 3:** Applying a single integrated framework
- **Principle 4:** Enabling a holistic approach
- **Principle 5:** Separating governance from management

COBIT groups the governance and management objectives into the following five domains:

Evaluate, Direct, and Monitor (EDM): Governing body evaluates strategic options, directs senior management, and monitors achievement.

Align, Plan, and Organize (APO): Management addresses organization, strategy, and supporting activities.

Build, Acquire, and Implement (BAI): Management treats the definition, acquisition, and implementation of solutions, integrating them into business processes.

Deliver, Service, and Support (DSS): Management addresses services, operational delivery, and their supports, including security.

Monitor, Evaluate, and Assess (MEA): Management monitors performance and ensures that the program meets internal targets, internal control objectives, and external requirements.

At first glance, the NIST RMF and COBIT appear different, mainly because they use different terminology. For example, NIST takes you through discrete steps based on technology assets, while COBIT focuses on leadership's responsibilities.

The difference between the two models focuses on NIST being process-oriented and COBIT being oversight-oriented. However, fundamentally, they both still require the same five components.

Governing Risk

Everyone in your organization plays a role in mitigating risk. Governance is the practice of defining and assigning responsibilities so that everyone knows what they need to do and has the skills to do it.

For example, governing risk includes:

- Assigning oversight responsibilities.
- Establishing employee policies.
- Reviewing documents proving people followed approved practices and procedures.

Identifying Risk

Before doing anything else, you need to identify your organization's risks. You can do this from a strategic level or an asset-focused level. For example, you might think in terms of the following risks:

- Compliance
- Financial
- Legal

If you're focusing on technologies, you might focus more on the following risks:

- IT
- Operational
- Data breach

However, your technology and strategic risks are interrelated in a digitally transformed business—meaning either approach will have similar results.

Measuring Risk

After identifying risks, you need to measure their impact on your organization. At a very high level, measuring risk usually involves the following equation:

> **Risk = [Likelihood of an adverse event] X [Impact to the business]**

While that might seem like simple math, the reality is more complex. The likelihood of an adverse event can depend on multiple factors, while the impact can be fines or loss of brand value and reputation.

Mitigating Risk

To protect yourself, you need to find ways to reduce the impact arising from an adverse event. Risk mitigation strategies can include:

- Implementing technical controls.
- Creating contingency plans.
- Establishing processes and procedures.

Monitoring and Reporting Risk

In an ever-changing world, your risk is going to evolve. With each change, you need to monitor your organization's risk mitigation controls to ensure they maintain the accepted level of risk.
In addition, you need to ensure that you report your monitoring outcomes to the appropriate responsible parties, like your senior leadership or board of directors.

Some things to monitor and report on might include new:

- Regulations impacting your organization.
- Internal technologies that enable business processes.
- Technologies enabling better customer experiences.

DRATA

Roles and Responsibilities in Risk Management

As part of a strong compliance posture, your leadership and board of directors needs to know that your security program functions as intended.

Most compliance mandates require that leadership and the board review IT security so that they can understand how well the organization manages risk.

In some cases, like for **SOC 2 compliance**, management and boards are required to provide evidence proving that the organization complies with internal controls. If the attestation proves false, then they can be held responsible.

When reporting your compliance posture, you need to make sure that everyone understands the identified risks, the mitigating controls, and the controls' ability to work as intended. There are several roles in a company that typically handle or touch risk management.

Individuals and their teams should have clear expectations and knowledge of their duties for when a situation arises. This will help fast track solutions, eliminate potential enduring complications, and assist in limiting the impact to the organization.

Senior Management

Senior management must ensure that necessary resources are given so an effective risk management process can be created and implemented. They review the results of the performed assessments and use it to influence their operational decisions. An effective program requires the support and involvement of senior management to be instituted company-wide.

Business and Functional Managers

The cooperation of business and other functional managers is necessary to minimize the likelihood of threats exploiting a vulnerability or from vulnerabilities arising. Actions like ensuring proper security training and that protocol is followed by their teams helps to mitigate risk throughout the organization.

Security Team

The security team includes: system and information owners, security officers, IT security practitioners, and other security SMEs. They are responsible for proper implementation of controls into IT systems, evaluating new risks as the environment changes using the risk management process, and much more. Together, they are the backbone of the IT risk management process and security program.

DRATA

The Business Perspective of Managing Risk

Risk management is not an island unto itself. Instead, its policies and controls are there to support your overall business objectives.

> **Every business takes risks. The only question is, how smart are the risks they take?**

Assuming the right risks at the right time requires alignment between your organizational priorities and your leadership team's risk tolerance. Security or compliance professionals need to understand both to create a risk management program that strikes the right balance and serves the business. Of course, risk management programs can never align perfectly with every business goal every time.

Sometimes you have to say no. Most of the time, you focus on the how.

For example, a new, lesser-known sales tool could increase sales by 60% but doesn't have every security control you expect in a vendor. Is that a risk worth taking? Yes, that would be an intelligent risk with the right security controls or contractual commitments in place.

Another way risk management supports business goals is by driving organizational maturity. For example, onboarding and offboarding practices that may have been appropriate in a 30-person startup make less sense in a 300-person growth company—much less a 3,000-person enterprise. A supportive risk management program evolves and strengthens these practices before they become issues in compliance audits.

When you do have to say no, compliance is usually the reason.

> **Your risk management program must align with your business's relevant compliance frameworks.**

Standards like PCI or HITRUST expect you to adopt specific security controls. On the other hand, SOC 2, HIPAA, or ISO standards offer more flexibility within their risk management expectations. General or specific, your business must do these things to avoid taking on excessive risk.

Yet, sometimes those risks may be worth taking to support your business objectives—provided you develop suitable mitigations.

Driving Organizational Accountability

Who owns the decision to accept the risk? It's not the governance, risk, and compliance (GRC) or enterprise risk management (ERM) teams.

An important concept to consider is that of risk acceptors. Neither of these roles belongs to the GRC or ERM teams.

> **The responsibility for accepting and owning risk falls on the company's leadership—the people whose decisions create that risk.**

They must own the consequences of their decisions and ensure the business only takes appropriate risks.

Without executive accountability, risk ownership falls on the GRC or ERM teams—even though they lack the authority to change the business.

GRC and ERM teams can only manage risk. They may even reject decisions that expose the business to unacceptable risks. But they do not own the risk.

Risk managers must assess a risk based on its impact on the business and present their conclusions to the executive team. Accepting a high-impact risk is not possible. Instead, the risk owner must take responsibility for transferring, mitigating, or fixing the risk.

Accepting a low-impact risk depends on the executive team's risk tolerance. But it's still an executive decision, and they are accountable if that risk causes an incident.

DRATA

Types of Risk Assessment Methodologies

An organization's sensitive information is under constant threat. Identifying those security risks is critical to protecting that information. But some risks are bigger than others. Some mitigation options are more expensive than others. How do you make the right decision?

Adopting a formal risk assessment process gives you the information you need to set priorities. There are many ways to perform a risk assessment, each with its own benefits and drawbacks. We will help you find which of these six risk assessment methodologies works best for your organization.

Organizations can take several approaches to assess risks—quantitative, qualitative, semi-quantitative, asset-based, vulnerability-based, or threat-based. Each methodology can evaluate an organization's risk posture, but they all require tradeoffs.

Quantitative

Quantitative methods bring analytical rigor to the process. **Assets and risks receive dollar values.** The resulting risk assessment can then be presented in financial terms that executives and board members easily understand. Cost-benefit analyses let decision makers prioritize mitigation options.

However, a quantitative methodology may not be appropriate. Some assets or risks are not easily quantifiable. Forcing them into this numerical approach requires judgment calls—undermining the assessment's objectivity.

Quantitative methods can also be quite complex. Communicating the results beyond the boardroom can be difficult. In addition, some organizations do not have the internal expertise that quantitative risk assessments require. Organizations often take on the added cost to bring in consultants' technical and financial skills.

Qualitative

Where quantitative methods take a scientific approach to risk assessment, qualitative methods take a more journalistic approach. Assessors meet with people throughout the organization. Employees share how, or whether, they would get their jobs done should a system go offline. Assessors use this input to categorize risks on rough scales such as High, Medium, or Low. **A qualitative risk assessment provides a general picture of how risks affect an organization's operations.**

People across the organization are more likely to understand qualitative risk assessments. On the other hand, these approaches are inherently subjective. The assessment team must develop easily-explained scenarios, develop questions and interview methodologies that avoid bias, and then interpret the results. Without a solid financial foundation for cost-benefit analysis, mitigation options can be difficult to prioritize.

Semi-quantitative

Some organizations will combine the previous methodologies to create semi-quantitative risk assessments. Using this approach, organizations will use a numerical scale, such as 1-10 or 1-100, to assign a numerical risk value. Risk items that score in the lower third are grouped as low risk, the middle third as medium risk, and the higher third as high risk.

Blending quantitative and qualitative methodologies avoids the intense probability and asset-value calculations of the former while producing more analytical assessments than the latter. Semi-quantitative methodologies can be more objective and provide a sound basis for prioritizing risk items.

Asset-based

Traditionally, organizations take an asset-based approach to assessing IT risk. Assets are composed of the hardware, software, and networks that handle an organization's information—plus the information itself. An asset-based assessment generally follows a four-step process:

- Inventory all assets.
- Evaluate the effectiveness of existing controls.
- Identify the threats and vulnerabilities of each asset.
- Assess each risk's potential impact.

> **Asset-based approaches are popular because they align with an IT department's structure, operations, and culture.**

A firewall's risks and controls are easy to understand. However, asset-based approaches cannot produce complete risk assessments. Some risks are not part of the information infrastructure. Policies, processes, and other soft factors can expose the organization to as much danger as an unpatched firewall.

Vulnerability-based

Vulnerability-based methodologies expand the scope of risk assessments beyond an organization's assets. This process starts with an examination of the known weaknesses and deficiencies within organizational systems or the environments those systems operate within. From there, assessors identify the possible threats that could exploit these vulnerabilities, along with the exploits' potential consequences.

> **Tying vulnerability-based risk assessments with an organization's vulnerability management process demonstrates effective risk management and vulnerability management processes.**

Although this approach captures more of the risks than a purely asset-based assessment, it is based on known vulnerabilities and may not capture the full range of threats an organization faces.

DRATA

Threat-Based

Threat-based methods can supply a more complete assessment of an organization's overall risk posture. This approach evaluates the conditions that create risk. An asset audit will be part of the assessment since assets and their controls contribute to these conditions.

> **Threat-based approaches look beyond the physical infrastructure. By evaluating the techniques threat actors use, for example, assessments may re-prioritize mitigation options.**

For instance, cybersecurity training mitigates social engineering attacks. An asset-based assessment may prioritize systemic controls over employee training. A threat-based assessment, on the other hand, may find that increasing the frequency of cybersecurity training reduces risk at a lower cost.

DRATA

Choosing the Right Risk Assessment Methodology

None of these methodologies are perfect. Each has strengths and weaknesses. Fortunately, none of them are mutually exclusive. Whether intentionally or by circumstance, organizations often perform risk assessments that combine these approaches.

When designing your risk assessment process, the methodologies you use will depend on what you need to achieve and the nature of your organization.

If board-level and executive approvals are the most important criteria, then your approach will lean towards quantitative methods. More qualitative approaches might be better if you need support from employees and other stakeholders. Asset-based assessments align naturally with your IT organization while threat-based assessments address today's complex cybersecurity landscape.

> **Constantly assessing your organization's risk exposure is the only way to protect sensitive information from today's cyber threats.**

Identify Your Cybersecurity Risks

Identify the risks associated with your business. You can ask yourself these questions to help you through this process:

What are my organization's assets?
Your assets are anything that has value to your business. This includes intellectual property, customer data, financial records, and anything that would make it difficult for your company to function if it were lost or stolen.

If there were any way someone could compromise these assets, how would they do it?
Look at how different parties in your organization gain authorization to information, as well as what devices and processes they use to access it.

What information is sensitive?
Some types of information may be more valuable than others—like credit card numbers or social security numbers. Other information may not be as valuable but still needs protection because it could be used as leverage in a future attack (such as information about the operating systems being used).

What technology do you use?
The technology you use will determine how vulnerable your organization is to certain types of attacks. You may also need to take additional steps to keep information secure if you are using legacy or outdated systems.

Also, review any recent security issues that came up for your organization. You'll want to ensure that any measures you put in place to resolve them are working as intended.

Analyze Cybersecurity Risks

Next, it's time to look at what you uncover during the first step and get more details on the risks you face. There are two components that are critical at this stage.

The first is prioritizing risks. This involves examining the threats and vulnerabilities associated with a system, and determining which poses the most risk to your organization. At this stage, you need to figure out what risks to deal with first.

The second is identifying and assessing the impact of potential risks. Once you figure out what risks you're focusing on, you need to work to understand the likelihood that a risk will occur and the impact it would have if those risks become a real threat. This will empower you to create better processes.

Treat Cybersecurity Risks

You can take steps to reduce the likelihood of a successful cyberattack, and you can recover from an attack if it happens. First, think about what you can do to prevent security issues.

For example, to treat the risk of unauthorized access to an account, you might choose to use two-factor authentication (2FA) every time you log in to your system so that attackers cannot access your account even if they steal your password. If someone gains access without permission, 2FA will stop them from going any further.

Then, consider the processes you can put in place to respond to any threats you may need to contend with. Can you improve any measures you may have in place to notify you of a breach and improve response time? Can you put a process in place to stop any unauthorized users in their tracks? Consider all options.

Monitor and Update Your Risk Management Plan

As a cybersecurity risk management plan rolls out, it will need updates and revisions. It's important that you monitor the way your organization uses the plan, as well as how effective it is at addressing potential threats. The following are some steps you should take to ensure that your plan stays up to date:

- Check that all processes and procedures listed in the risk management plan are being used properly by employees.
- Consider gaps in coverage that may be introduced by new business practices or technology changes.
- Ensure that your processes will address any new threats that may have come into play after the initial plan.

Remember, as you make updates, you need to ensure that all employees in your organization are aware of them. A cybersecurity risk management plan can be good, but it will only be effective if people are following it.

DRATA

Building Your First Risk Register

In 2021, the average number of cyberattacks and data breaches increased by 15.1% from the previous year. Many organizations know they need to take risks seriously, but they may not have awareness about what they're most likely to face and how to handle a threat.

A risk register is a list of all the risks that you identify and your organization's plans to respond. The purpose of the risk register is to help you get a complete picture of your threat landscape and ensure that you have risk management processes in place.

A risk register is a documented way to understand risks, their likelihood and impact, and the actions you intend to take to address those risks. It's an essential tool for leaders and stakeholders to track and communicate security concerns before problems arise.

Simply put, it benefits your company by making it easier to:

- Identify and track risks that might derail your organization.
- Decide which risks are worth acting on (and which ones aren't).
- Determine how to react if something goes wrong—whether it's the best way to recover from an unexpected delay or ensuring that a critical change doesn't wreak havoc.

Leaders and cybersecurity professionals within your organization will typically use the risk register as a reference to make sense of cybersecurity threats and make moves towards proactive security.

> **A well-managed risk register can also be used as part of an audit trail within your organization if you are required to keep records of risk management activities.**

The most important thing about creating a risk register is setting aside time to do it. If you're working with a team, make sure everyone agrees on who will be responsible for making sure things get done.

The next step is deciding how detailed to get on your list. The more details you include, the better equipped you'll be when something goes wrong. However, as your list gets more complex, it becomes even more important to keep things organized and consider automation.

A risk register should include a description of each risk and the probability and impact it could have. It should also include responses to risks or plans for how you will deal with them.

Including responses in your register will help you demonstrate an awareness of not just the threats themselves, but that you've put thought into how you can manage them. Failing to include them can be seen as risk blindness, since there was no real consideration given towards how those threats might happen or what would be done if they did occur.

When you're ready to try out this process for yourself and create a risk register for your organization, the National Institute of Standards and Technology (NIST) Framework acts as a good guideline.

You can put the NIST Cybersecurity Framework to work in your business in these five areas:

- Identify
- Protect
- Detect
- Respond
- Recover

Here's what that looks like in the context of a risk register.

First, do some digging to think about all of your potential risks. This may include problems that your organization has dealt with in the past, upcoming threats, or risks that are most common in your particular industry. What actions can you take to protect your organization from risks right now?

Next, ask yourself: How serious is each risk? At this stage, you'll want to create a risk rating. There are several factors that may go into that rating. Those may include how likely the risk is to have an impact and what level of impact it would have. From there, you can organize the risks based on how serious they are to you.

Then, start taking a closer look at the impact. How will the risks on your list influence operations if they become an issue? What can you do to lessen that impact and respond to the threat? This is one of the most critical parts of your risk register—it's the starting point for your plan of action.

Finally, what will you do after an attack? How will you recover in the event that information does get compromised? You'll also have to think through ways to keep everyone informed both internally and externally.

Once you put in the work to create your risk register, you need to have it in a place that's accessible for review. The right choice here will depend on your team. You can use a spreadsheet, a project management system, or an internal database.

No matter what you decide, be sure to review this information regularly. This isn't something you should set and forget. Instead, you'll need to make updates and changes as risks continue to evolve.

DRATA

Assessing Risk

Adopting the right risk assessment methodology is necessary for companies to be aware of potential threats and create mitigation strategies in the face of these threats. Below we outline the steps mentioned in NIST SP 800-30 to help inform your assessment.

System Characterization

System characterization involves characterizing the IT system through an intense review of the company's information systems and infrastructure. System-related information is collected through questionnaires, on-site interviews, document review, and use of automated scanning tools.

Threat Identification

When determining a threat, you must consider potential threat sources and their motivations. **Threats come when a vulnerability in a system is exploited or accidentally triggered.** For example, a malicious actor could be trying to access confidential information and a poorly trained employee may accidentally trigger a threat through a successful phishing attempt.

Vulnerability Identification

A vulnerability is typically paired with a threat during a risk assessment to understand how they may be exploited. Such as a disgruntled former employee (a threat-actor) accessing proprietary data if their information has not been immediately removed from the system upon termination (the vulnerability). A method for identifying system vulnerabilities might be the development of a security requirements checklist.

Control Analysis

Controls must be put in place to lower or eliminate the chance of a threat-source exploiting a system vulnerability. These security controls may be technical, like an authentication and authorization mechanism for company software, or non-technical, such as a security policy.

Likelihood Determination

As it sounds, **likelihood determination is the probability that a vulnerability may be abused by a threat-source.** This is usually characterized by ratings from low to high. A low rating means that controls have been put in place and the malicious actor has low motivation or capability to act. A high rating may be considered that the actor has high motivation and capability to act and the controls in place are rendered ineffective.

Impact Analysis

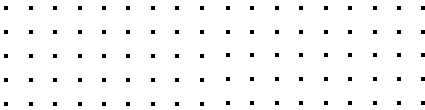
Impact analysis determines the harmful impact that would result from a successful threat exercising a vulnerability. The impacts are described in terms of failing the following security goals:

- Loss of integrity
- Loss of availability
- Loss of confidentiality

Impacts may be measured in quantifiable means such as a monetary value or how many hours it takes to restore a system's functionality. Other impacts such as a loss of public confidence or credibility are qualitative and harder to assign a number to.

Risk Determination

Risk determination means quantifying the level of risk a particular threat may be to the IT system. To determine this, you may deploy a risk scale—ranging from low to high—and a risk-level matrix. These ratings are subjective as different threats have higher or lower levels of risk and impact depending on the company. Risk scales help organizations prioritize the risks they've identified.



Controls Recommendations

During this part of the process, **controls that could mitigate or eradicate the prior identified risks that are a threat to the company's operations are recommended.** By this step, these controls have already been determined feasible and justified in a cost-benefit analysis during the risk mitigation process.

Results Documentation

Once the assessment has been completed, **a risk assessment report should document results** to inform future updates or changes to protocol.

DRATA

Implementing Risk Management

There is a lot that goes into raising awareness of risks, creating an action plan, and implementing an effective process. With the potential for varying degrees of impact, it's crucial to get your program up and running quickly and efficiently to be well equipped against liabilities.
Implementing your IT risk management plan and executing a risk mitigation strategy based on your risk assessment report are the last steps in the process.

Senior management uses the risk assessment report to influence the methodology they use to mitigate the identified risks with these options:

Assumption/Acceptance

The assumption option means to accept a potential risk that may occur and continuing with the current system in place. Or instead, implementing a control to lower the risk to what senior management deems acceptable. Your risk assessment policy will define which risk scores must be mitigated versus which can be accepted.

Avoidance

Risk avoidance is defined as eliminating the risk caused altogether by no longer using certain aspects of the IT system or shutting it down when risks are discovered.

Limitation/Mitigation/Treatment

You can limit risk by adding controls that reduce the detrimental effects when impact occurs.

Planning

Risk planning is putting a risk mitigation plan in place that prioritizes, implements, and maintains controls.

Research and Acknowledgement

Through research and acknowledgement, you can reduce the risk of loss by noting the flaw in the system and researching controls to fix it.

Transference

Transferring a risk can be done by using other options to compensate for the loss, like purchasing cybersecurity insurance.

A combination of these options will likely be chosen to handle the risk associated with the company's mission and objectives.

Risk Mitigation Strategy

A risk mitigation strategy is then executed to put controls in place as needed and implement a safeguard plan when threats arise. The steps are described below.

1. Prioritize control implementation actions based on risk levels.
2. Evaluate recommended controls on feasibility and effectiveness for your organization's operations and IT system.
3. Conduct cost-benefit analysis that describes the cost and benefits of implementing or not implementing the controls.
4. Have management select the most cost-effective control(s) for reducing risk to the organization's mission.
5. Assign the responsibility of implementing controls to the appropriate parties (employees or contracted vendors).
6. Develop a control implementation plan to outline the prior information as well as start date, targeted completion date, and necessary maintenance requirements.
7. Implement selected controls, execute the safeguard implementation plan, and evaluate residual risk.

DRATA

Applying Risk Management to ISO 27001

As your organization grows and adds new technologies, your IT risks evolve. Malicious actors increasingly use supply chain attacks to cause as much damage and disruption as possible. In response, legislative bodies and regulatory agencies implement more rigorous compliance requirements. Meanwhile, customers often require companies to prove that they understand their risk and have mitigating controls in place.

Many compliance mandates integrate the controls and processes defined within the International Organization for Standardization (ISO) 27000-series—in particular, ISO 27001.

> **ISO 27001 describes best practices for building an information security management system (ISMS).**

As you start your ISO certification journey, you need to understand how to conduct an ISO 27001 Risk Assessment because it's the foundation for everything else.

Clause 6.1.2 of ISO 27001 outlines the requirements for an information security risk assessment, requiring that organizations:

- Establish and maintain information security risk criteria.
- Implement repeatable processes that produce consistent, valid, and comparable results.
- Identify information security risks.
- Analyze information security risks.
- Evaluate information security risks.

The ISO 27001 risk assessment guides every other activity that the organization takes to protect sensitive data.

Embedded within ISO 27001's general risk assessment requirements, the standard also includes several actions to take and documents to collect.

> **It's important to remember that a risk assessment requirement, like ISO's, is intended to provide a flexible framework rather than a prescriptive set of steps.**

When you dig into the risk assessment clause a little further, you start to get a better sense of what ISO expects from you. Some key requirements include:

- Defining the risk acceptance criteria in the policy.
- Defining the assessment criteria in the policy.
- Identifying information confidentiality, integrity, and availability risks .
- Identifying risk owners.
- Assessing the potential consequences if the identified risks materialize.
- Realistically assessing the likelihood that the risks will occur.
- Determining risk level.
- Comparing risk analysis with risk criteria.
- Prioritizing risk treatment.

As part of the planning process, your risk assessment provides a map that helps you outline everything from how you design your architecture to how you measure your security program's effectiveness.

Since everything about compliance and audit relies on documentation, your risk assessment will generate reports used during the audit.

Risk Assessment Table

The risk assessment table lists the organization's:

- Assets and information resources.
- Identified vulnerabilities and threats.
- Risk level.

DRATA

Risk Assessment Table

This report outlines how you measure risk and incorporates your company's context. For example, you should consider including:

- Legal, regulatory, and compliance requirements.
- Business objectives.
- Information security objectives.
- Stakeholder expectations.

Once you define how you plan to assess risk, you can create consistent processes for how to treat risks. This means knowing what risks you plan to:

- Accept
- Avoid
- Transfer
- Mitigate

Not every risk is equally important, and you might decide to accept something with a low risk of adversely affecting your company because mitigating it is cost-prohibitive. On the other hand, you might choose to mitigate a risk that could negatively impact your company because it provides an equally important benefit and cost-effective mitigations exist.

Statement of Applicability (SoA)

> **The SoA documents which ISO 27001 Annex A controls you implemented, how you implemented them, and your reasoning for implementing them.**

In addition, if you chose not to implement controls, you must also document why you felt they weren't necessary within your unique environment.

For each control, you want to explain which of the following requirements it fulfills:

- Legal obligations
- Contractual obligations
- Business requirements
- Results of risk assessment

Risk Treatment Plan

While your risk treatment methodology explains how you make risk tolerance decisions, your risk treatment plan outlines the actions that you plan to take for each identified risk. Basically, the document proves you appropriately applied the methodology in practice.

In many ways, the risk treatment plan is similar to the risk treatment methodology. You're documenting a list of assets, threats, and risk-based choices. In addition to those, your risk treatment plan will include:

- A person responsible for the asset.
- The security control(s) that mitigate risk.
- The person responsible for implementing and maintaining the control(s).
- Deadlines associated with implementing, monitoring, and reviewing control(s).
- Resources needed to implement the control(s), including staffing and budgets.
- Method of evaluating control implementation.

How to Conduct an Asset-based Risk Assessment

ISO 27001 recommends an asset-based risk assessment, here's how to do it:

Create a Cross-functional Team

No one person in your company knows everything about your technology stack or the risks you need to consider. When you build out a team, you want to include stakeholders from across the organization, including:

- IT
- Senior leadership
- Department managers
- Legal
- Compliance/Audit

Establish an Asset Inventory

You can't protect what you don't know you have. Include the following in your asset inventory:

- Data
- Devices, including Internet of Things (IoT) devices, network devices, and mobile devices
- Users
- Storage locations
- Networks
- Applications/Software

You need to create an asset inventory that's as complete as possible, so you should be monitoring for new assets regularly—especially in cloud environments.

Assign Each Asset a Risk Level

For each asset, you want to consider whether it poses a high, medium, or low risk to the organization. This is where you look at your organization's context, like legal or compliance risks. For example, privacy laws regulate how you need to handle personally identifiable information (PII), so that data poses a high compliance risk.

Define Threats and Vulnerabilities

Once you know all your assets, you can outline threats and vulnerabilities for each one. For technologies, you want to consider things like:

- Common vulnerabilities and exposures.
- Availability of security updates.
- Potential downtime.
- Known attacks targeting them.

You also want to consider administrative and procedural threats and vulnerabilities like:

- An employee leaving the organization.
- Lack of process documentation.
- Employee security awareness.

Analyze Risk

When you analyze risk, you consider the likelihood that an event will happen and compare it to the damage it causes. A high-risk asset with a low likelihood of experiencing a risky event might be a moderate risk overall.

Document Risk Assessment and Risk Treatment Methodology

Once you have analyzed all your assets, threats, vulnerabilities, and risks, you can write your risk assessment and treatment methodology. This aggregates all the activities you've engaged in and allows you to outline your reasons for accepting, refusing, mitigating, or transferring the risks.

Choose and Document ISO 27001 Controls

Once you've determined which risks you want to mitigate, you start working through the different ISO 27001 Annex A controls listed in ISO 27002. For each asset, you define the threat/vulnerability and document which control(s) apply, including your reasoning for implementing them.

Implement and Test Chosen Controls

When it comes to compliance, your actions speak louder than your words. For each control, you need to use either a technology or a process for implementing it. You should be documenting how you implemented the control, who's responsible for the implementation, and when you completed the implementation.

Monitor Controls

Security changes continuously, so you need to make sure that you monitor whether your controls are working as intended. For example, security researchers continue to find new vulnerabilities in operating systems and software.

To ensure continued control effectiveness, you should run vulnerability scanners and update software or operating systems with security patches. To monitor whether your vulnerability and patch management controls are working, you need a way to make sure that all devices connected to the network are securely configured.

Report Program Effectiveness to Leadership

ISO 27001 certification requires oversight from senior management and the board of directors. With everything documented and monitored, you need to give everyone the information that allows them to make informed decisions when risks change. Your reports should include key performance indicators that show whether controls work as intended to mitigate risk or whether you need to update the risk treatment plan with additional controls.

Automating the Risk Management Process

For most companies, maturing their risk management processes is challenging.

Many organizations start with spreadsheets that document their risk and controls. However, as the organization grows and matures, its compliance program also needs to mature.

With so many people and moving parts involved, manually managing the risk assessment process can quickly become inefficient. As you move toward certification, you need to have a single source of information for audits, but shared spreadsheets may not always be up to date. With Drata, everyone involved in the risk management process can collaborate without worrying about multiple copies of documents or making unauthorized changes.

Our library of pre-mapped risks and ability to create custom risks streamlines the identification, assessment, and analysis process. Our platform automatically populates a custom score that allows you to assign responsible parties and track their activities to prove compliance. As we continuously monitor your security, we also monitor your compliance, providing alerts and suggesting treatment plans so that you can proactively mitigate risks.

To learn more about how you can automate your risk management process and integrate it into your existing compliance effort, set up a time to chat with Drata.

DRATA

Drata.com