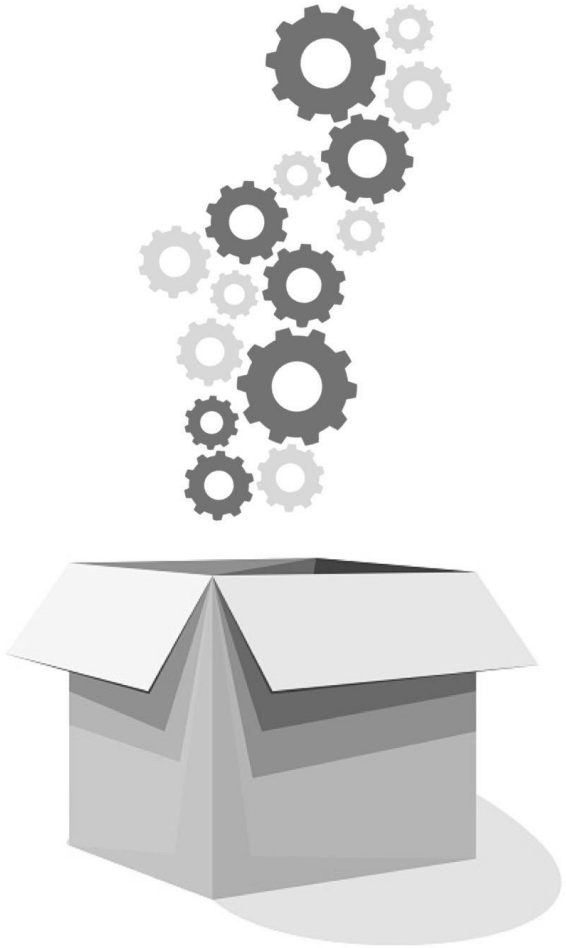
IT Risk Management

Getting Started

Author | Paula Queiroz

Last Review | January 2024

Contents



- What is risk?
- The risk management lifecycle
- NIST 800-37, 800-30, 800-53 and 800-171
- COBIT
- ISO/IEC 31000

Part 1

Understanding Risk

What is Risk?

To start understanding IT Risk Management, we are going to start with understanding what risk is.

Depending on who defines it, the definition of risk can vary considerably and, sometimes, we can even see the words “risk”, “threat” and “vulnerability” being used interchangeably. So, we’ll start by looking at the difference between the three.

Risk can be defined as “the positive or negative outcome of a particular event arising, where the outcome is dependent on an assessment of the potential likelihood and/or frequency of the event occurring within a specified period of time”.

Note the fact that a risk doesn’t necessarily need to have a negative outcome: the outcome can be negative, positive, or just a deviation from the expected.

Types of Risk

There are three types of risk which are normally always considered, We won't go into them in great detail, however, in order to understand better the concept of "corporate risk appetite", and why enterprises choose to take risks, it's important to make it clear that, again, risks aren't always a bad thing. These three risk types are:

Pure Risks

These risks are those for which the outcome will always be negative - all sorts of accidents and incidents which lead to nothing other than loss in profit, availability, reputation, etc, are pure risks.

Control/Uncertainty

These risks are those which will normally be associated with project management and give rise to uncertainty in terms of the product outcome in terms of schedule, cost and quality, mainly.

Opportunity/Speculative

These risks are those companies will choose to take, some far more aggressively than others. These will be the sort of investment risks where every risk is consciously and willfully taken in order to achieve a likely gain.

Vulnerability and Threat

Vulnerability

A vulnerability can be defined as “a weakness of an asset (resource) that can be exploited”. In other words, the vulnerability is what allows a threat to do harm. Examples of possible vulnerabilities are, ie: having outdated or non-patched systems, having hardware or software out of support, having a datacenter in an area prone to wildfires, etc.

Threat

A threat can be defined as “anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset”. Examples of threats (which can explore the examples of vulnerabilities above) are, ie: attacks against systems that target a vulnerability fixed by recent patching, hardware breaking, a wildfire occurring, etc.

Risk = Threat x Vulnerability (x Impact)

ISO 31000 (more later) defines risk as:

“The effect of uncertainty on objectives. An effect may be positive, negative, or a deviation from the expected” (note the word “uncertainty” in context), and risk management as the “coordinated activities to direct and control an organisation with regard to risk”.

The concepts of “risk”, “vulnerability” and “threat” intersect in that risk can be the potentially for loss/damage of any type of asset, resulting from any recurring or emerging threat which exploits an existing vulnerability.

To make the picture clearer and more precise, impact is most normally added to the “Risk = Threat x Vulnerability” formula, making it “Risk = Threat x Vulnerability x Impact”, as we’ll see a bit more in depth later on in this document.

Part 2

The Risk Management Lifecycle

The Risk Management Lifecycle

There are several different risk management frameworks, some of which will be discussed later which will tackle the risk management lifecycle in their own ways.

Whatever framework is chosen, however, the implementation will always be bespoke to the specific business and, here, we will be looking at the basics any risk management strategy must include.

Key Indicators (KIs)

When discussing risk management, you will constantly hear these being mentioned so, before going any further, please remember the following three basic ones:

- **KGIs - Key Goal Indicators:** these are pre-set indicators of process objectives (goals) that indicate what should be achieved by a process (they define an objective). They define the measures which will later be used to tell management whatever IT process has reached the business requirements.

- **KPIs - Key Performance Indicators:** these are measurable value that demonstrates how effectively a company is achieving key business objectives. Organizations use KPIs at multiple levels to evaluate their success at reaching targets.

- **KRIs - Key Risk Indicators:** are metrics for measuring the likelihood that the combined probability of an event and its consequence will exceed the organization's risk appetite and have a profoundly negative impact on an organization's ability to be successful.

4-Steps Risk Management Lifestyle

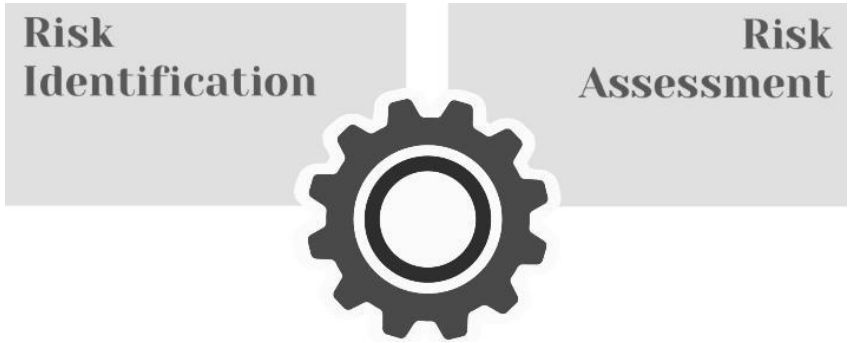
Risk Identification (or Risk Framing)

At this stage, we include and exclude items from our risk management scope and define the methods and tools to be used.
Assets, which are identified at this stage, will come in two main types:

- **Tangible assets** are anything which can be touched, that can go from a laptop, to a board-room table, to the actual building itself.
- **Intangible assets** are any assets which cannot be touched, for instance data, trade secrets, reputation, etc.

Risk acceptability criteria must also be defined at this stage, depending on the nature of the business and the will of its owners and/or stakeholders. Risk appetite will vary immensely from an enterprise to another where, for some, risks will always be perceived as threats to be avoided as much as possible and, for others, taking risks in a core part of the growth strategy (remember that risks don't always have a negative outcome!).

4-Steps Risk Management Lifestyle



Risk Assessment (and Analysis)

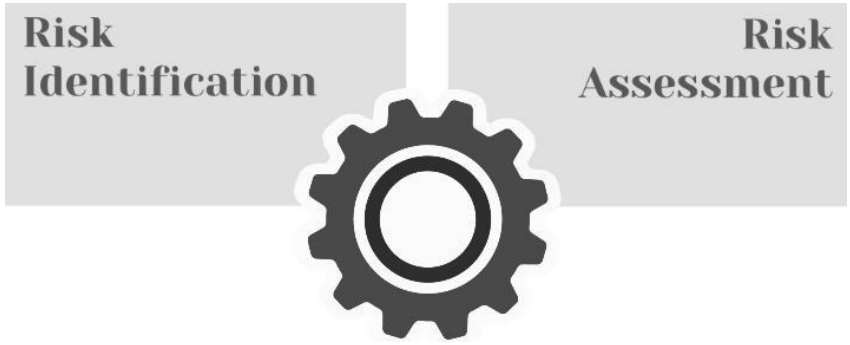
Once we know what the scope of our risk framework is, what our assets potentially at risk are, and what their context is, we will assess risks, always using a cost-benefit approach, likely in both quantitative and qualitative manners, where:

Quantitative Risk Assessment is, as the name indicates, and assessment that can be measured. Anything that we can put a precise number next to is when assessing it, is quantitative (for instance, how many hours a system will be down, how many people won't be able to connect, how much data will be lost, etc).

Here, we must be familiar with several concepts/properties which will allow us to define the value of an asset depending on how much of it is compromise, how much an incident will cost, how often incidents happen and how much that costs on an annual basis, here it comes:

AV - Asset Value defines how much an asset is worth
EF - Exposure Factor is the percentage of asset loss
SLE - Single Loss Expectancy = AV x EF tells us how much it costs us each time a loss happens
ARO - Annual Rate of Occurrence defines how often the loss happens per year
ALE - Annualised Loss Expectancy = ARO x SLE is how much money is lost yearly if the risk is ignored (which is never acceptable!)
TCO - Total Cost of Ownership is the cost of risk mitigation, upfront investment + ongoing (maintenance) cost

4-Steps Risk Management Lifestyle



Risk Assessment (and Analysis) - continued

In context, a laptop costs £10,000 (including not only the hardware, but also the value of the data it contains), whenever a laptop is lost, 100% of it is lost, and 25 laptops are lost every year, so:

AV = £10,000
EF = 100%
SLE = AV x EF = £10,000
ARO = 25
ALE = ARO x SLE = £250,000

Now let's look at securing our laptop…

Risk Assessment (and Analysis) - continued

Assume we have a 4-year refresh cycle for our laptops, and full disk encryption costs £75,000 initial investment + £5,000 per year recurring cost.

Because the AV (Asset Value) of our laptop included not only the hardware but also the data it contained, we might want to have the possibility to perform remote wipes, for which the solution will cost £20,000 upfront + £4,000 per year recurring. The staff required to manage and operate these solutions cost us £25,000 every year.

As we had seen before, our laptop annualised loss expectancy (ALE = ARO x SLE) was £250,000, so £1,000,000 per refresh cycle (£250 x 4) - this is what we'll lose every refresh cycle should we do nothing about the laptop loss threat (totally not okay!).

Encryption yearly cost = 75,000 / 4 + 5,000 = £23,750
Remote wipe yearly cost = 20,000 / 4 + 4,000 = £9,000
Support staff yearly cost = £25,000
So, total annual cost to protect us from this threat = 23,750 + 9,000 + 25,000 = £57,750.

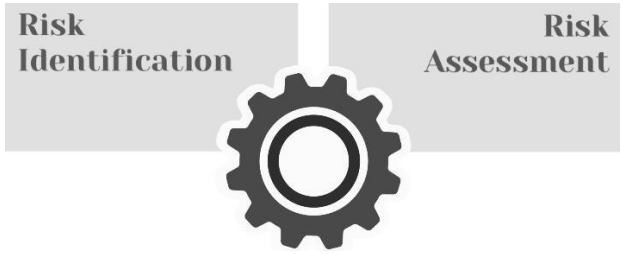
So, total annual cost to protect us from this threat = 23,750 + 9,000 + 25,000 = £57,750.

If you remember before, we were losing £375,000 per year in laptop losses (£10,000 per laptop, losing 25 laptops every year). There we were losing not only the hardware but the data it contained, where just the hardware alone for each laptop costs £1,000, and the remaining £9,000 related to data loss.
There's not much we can do about the hardware, so:

Annual data loss cost (when nothing is done) = 9,000 x 25 = £225,000
Annual cost for handling this threat = £75,750

Since we are spending way less money mitigating the data loss threat than we'd lose if we did nothing about it, our ROI (return on investment) is a clearly positive value, therefore, it makes perfect financial sense to have this solution implemented.

4-Steps Risk Management Lifecycle



Risk Assessment (and Analysis) - continued

Qualitative Risk Assessment

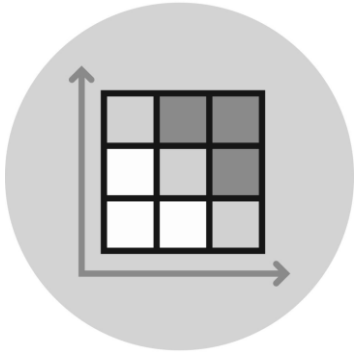
Qualitative risk assessment is that which is used for anything that is non-quantifiable. If it cannot be expressed using an actual number, then the assessment is qualitative.

For instance: how likely is it for something to happen? (notice that uncertainty makes it so that no exact number can be placed here), what will the impact be on reputation, how receptive will an audience be to a proposal, etc). Uncertainty analysis is also done here.

This is where we look at how likely an even is to occur. This likelihood will dramatically change how a risk is prioritised, as we'll see when we look at calculating risk.

When doing risk assessment and analysis, if countermeasures are already in place (they may or may not be, especially if we're talking about a new risk which has just been identified), we'll also look at the current countermeasures and assess whether they're fit for purpose, need improving or if totally new countermeasures must be put in place.

4-Steps Risk Management Lifecycle



Risk Assessment (and Analysis) - continued

Risk Matrix

A risk matrix can easily be used to perform qualitative risk analysis. This will look like a simple table correlating risk likelihood (from very probable to very probable) and impact (from very high to very low), where resulting values will range from very high to very low (this will depend on how the specific business creates their own risk matrix, ie it can be just high to low).

When qualitative analysis/the risk matrix tells us that a risk is quite serious, we are likely to want to handle that risk through a risk register (to be seen next).

The risk matrix will change depending on how things evolve and how risks are handled, where mitigation of a risk will obviously reduce its “rating” in the risk matrix.

4-Steps Risk Management Lifecycle

Risk Assessment (and Analysis) - continued

Risk Register

A risk register will be far more detailed than a risk matrix but, like a risk matrix, the format and specific information included in a risk register will depend on the specific enterprise building it.

There is no “one size fits all” but, nonetheless, there are some things which will normally be seen in most risk registers…

4-Steps Risk Management Lifecycle

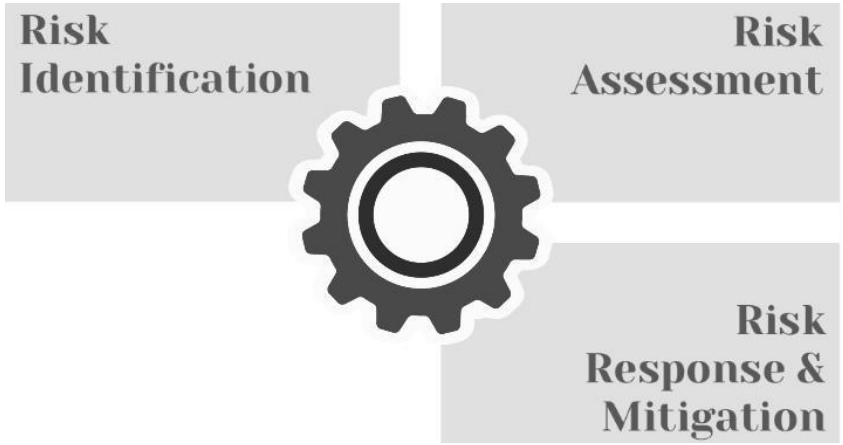
The following bare minimums will normally always be present:

- Risks will be assigned number, and they will be grouped in categories that group them depending on their nature.
- Besides the risk name, every risk will normally have a quick description.
- There will be a column for risk impact, and another for probably, which will correspond to numbers (integers) within the range defined by the business (ie 1 to 5).
- A risk score/rating column will also be found which, again, will be an integer obtained by multiplying impact x probability. Ie, if the probability is 2 and the impact is 3, the score will be 6.
- The risk score/rating is often used to determine which risks should be addressed first where, the higher the score, the most urgent it is to address them.

Many other columns can be added to the risk register, again, depending on the specific format used by the business. Personally, I will also include:

- Risk owner
- Date identified
- Possible effects
- Contingency measures
- Action
- Action owner
- Action date
- Etc.

4-Steps Risk Management Lifecycle



Risk response and mitigation

There are four main types of acceptable risk response, which are:

- **Risk acceptance**
- **Risk mitigation**
- **Risk transfer**
- **Risk avoidance**

We will check the above in more detail next. However, very importantly, please remember:

Risk rejection is never an acceptable response to risk!

- **This is purely ignoring a risk which we know exists. This can never be done as it equates to not performing due care, which translates to negligence!**

4-Steps Risk Management Lifecycle

Risk response and mitigation

Risk acceptance

When the risk is low and doesn't result in serious losses, quantitatively or qualitatively, and, looking at the cost of mitigation vs loss, we may choose to accept the risk. This is not the same as ignoring it, here we are analysing the risk and making a conscious, cost-benefit based decision.

Risk transfer

Here, we insure ourselves against the risk - ie we buy insurance that will cover us financially in case of losses.

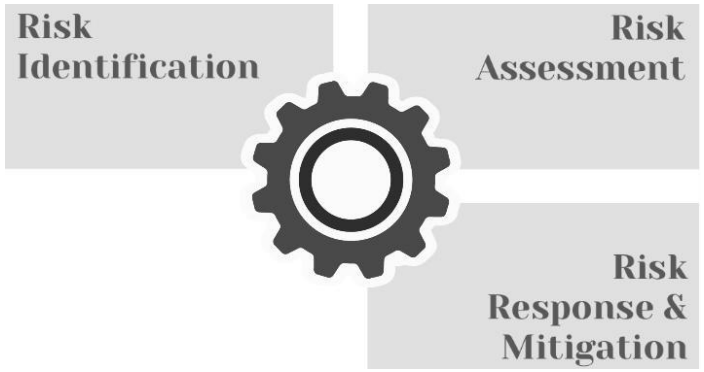
Risk mitigation

This means risk reduction, where we implement measures to make sure we minimise losses resulting from this risk. This doesn't mean we get rid of all possible negative consequences, but we make sure we minimise them, where how far we do so will have to make financial sense.

Risk avoidance

This approach simply eradicates the risk - whatever we were doing which introduced the risk, we simply stop doing it. In most real-life situations, this isn't doable. For instance issuing laptops introduces a risk. Risk avoidance would be stopping issuing them but, in practical terms, in most cases, this isn't really an option.

4-Steps Risk Management Lifecycle



When doing something about a risk, we may end up with…

Secondary risk(s):

Acting against a risk may result in the introduction of new one(s). Here we're basically looking at how far we are increasing our exposure surface.

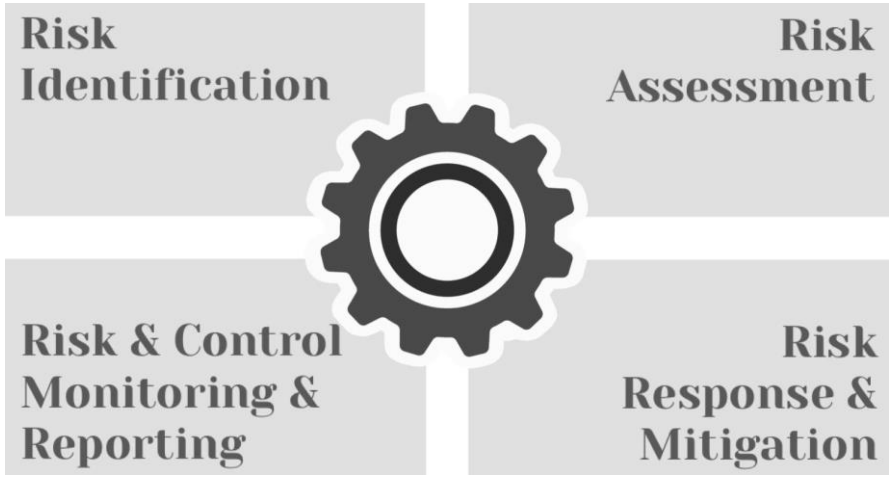
For instance, when we implement a solution to secure us against a risk, the solution itself may have weak points which have a certain probability to fail or be exploited - these will be secondary risks we are introducing to our environment, and these risks will need to be taken into consideration too.

Risk response and mitigation is always performed in the context of the choices made by senior management, based the information we provided/our recommendations during the assessment phase.

Risk response will probably rely partially on the information contained in the risk register, where risks with the highest score (remember, probability x impact) are likely to be addressed first.

As risks are addressed, this will reflect on the risk register (and matrix) where, as risks are addressed, their score will diminish, and this will happen in a fully iterative fashion which is never really over, as new risks that need addressing will keep being identified, and the score of known risks will change.

4-Steps Risk Management Lifecycle



Risk and control monitoring and reporting

The monitoring and reporting of both risks and the controls we implement to tackle them is also an ongoing process, and KRIs and KPIs will be useful for doing this effectively.

During this phase, efficient communication between IT and the senior management is required, where IT needs to be able to explain the state of the affairs in a way that, very likely non-technical, senior management will understand.

Without this sort of clear, engaged communication, senior management's ability to make decisions that will dictate what needs to be done next will be compromised.

The execution of the actions relating to this phase will lead us straight back to the start (remember that risk management is an iterative lifecycle) as, depending on the results obtained (and reported to senior management) during the monitoring of the risks and controls put in place, risk identification will start again, including these existing risks and any new risks identified.

Part 3

Risk Management Frameworks

NIST 800-37, 800-30, 800-53 and 800-171

The American National Institute of Standards and Technology (NIST), in partnership with the Department of Defense (DoD) have provided us with an integrated and very practical Risk Management Framework.

NIST SP 800-37 is the actual RMF.

NIST SP 800-30 provides the methodology for conducting risk assessment.

NIST SP 800-53 (American federal systems) and **800-171** provide the security requirements and controls.

NIST 800-30

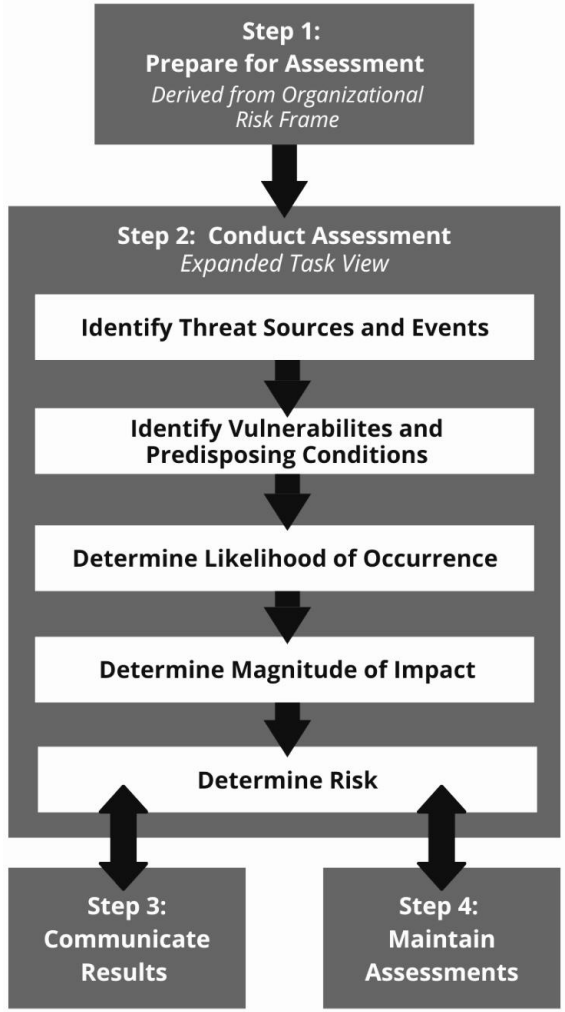


Image source: cyvatar.ai

NIST SP 800-30, named "Guide for Conducting Risk Assessments", defines how risk management fits into the system development life cycle (SDLC) and describes how to conduct risk assessments and mitigate risks.

It covers:

- Both internal and external vulnerabilities
- Relevant threats to the organization
- Impact on their organization
- Likelihood of harm to occur

This eventually results in the determination of risks.

In particular, SP 800-30 guides execute the following steps of the risk assessment process.

- Preparing for the risk assessment
- Conducting the assessment
- Communicating the results of the assessment
- And maintaining it

NIST 800-37

NIST SP 800-37, named "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy" provides the RFM itself. It is made of 7 steps:

1. Prepare

Tasks in the Prepare step are meant to support the rest of the steps of the framework. The purpose of this step was to "reduce complexity as organizations implement the Risk Management Framework, promote IT modernization objectives, conserve security and privacy resources, prioritize security activities to focus protection strategies on the most critical assets and systems, and promote privacy protections for individuals."

2. Categorize Information Systems

This step is all administrative and involves gaining an understanding of the organization. Prior to categorizing a system, the system boundary should be defined. Based on that system boundary, all information types associated with the system can and should be identified.

3. Select Security Controls

Security Controls are the management, operational and technical safeguards or countermeasures employed within an organizational information system that protect the confidentiality, integrity and availability of the system and its information.

NIST 800-37

4. Implement Security Controls

Step 3 requires an organization to implement security controls and describe how the controls are employed within the information system and its environment of operation. Policies should be tailored to each device to align with the required security documentation.

5. Assess Security Controls

Assessing the security controls requires using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security requirements for the system.

6. Authorise Information System

The authorise information system operation is based on a determination of the risk to organizational operations and individuals, assets, other organisations and the nation resulting from the operation of the information system and the decision that this risk is acceptable.

7. Monitor Security Controls

Continuous monitoring programs allow an organization to maintain the security authorization of an information system over time in a highly dynamic operating environment where systems adapt to changing threats, vulnerabilities, technologies and mission/business processes. While the use of automated support tools is not required, risk management can become near real-time through the use of automated tools.

NIST 800-53

The NIST 800-53, named "Security and Privacy Controls for Information Systems and organisations", is a cybersecurity standard and compliance framework developed by the National Institute of Standards in Technology.

It's a continuously updated framework that tries to flexibly, based on risk, cost-effectiveness, and capabilities, define standards, controls and assessments.

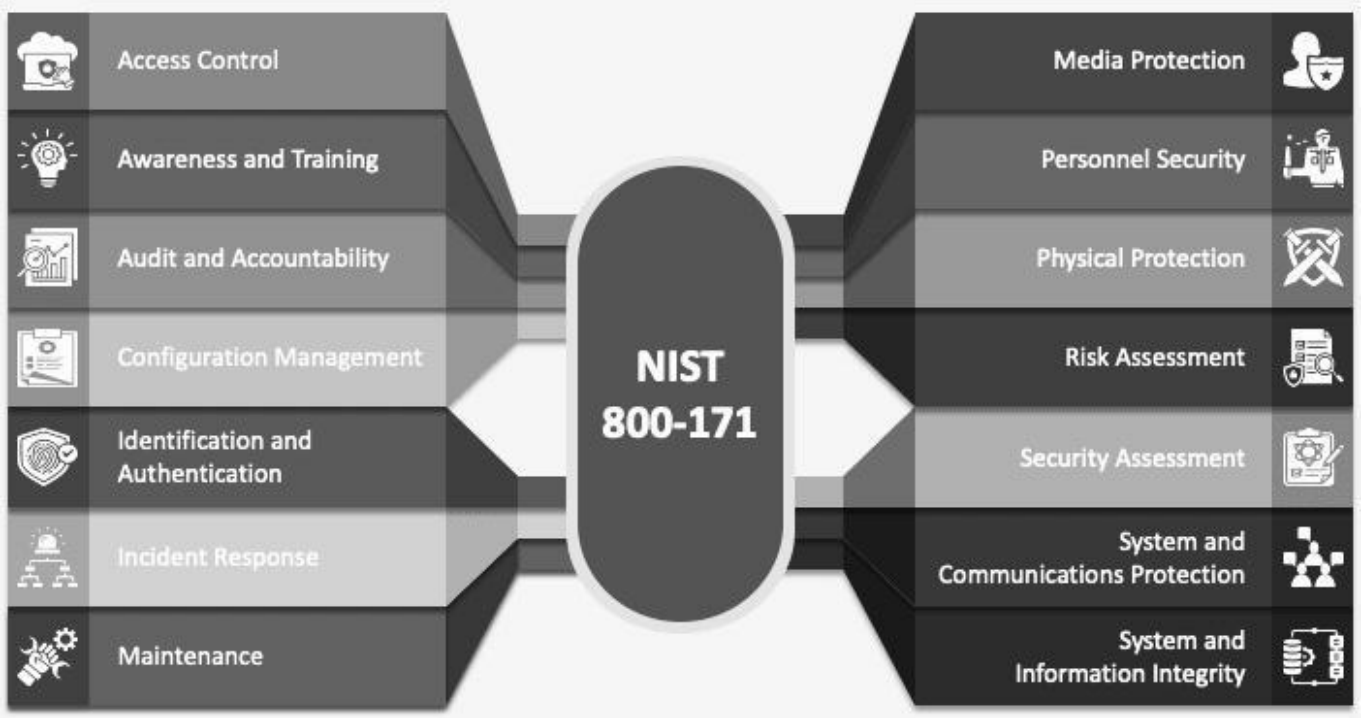
It is designed to provide a foundation of guiding elements, strategies, systems, and controls, that can agnostically support any organization's cybersecurity needs and priorities.

By establishing a framework available to all, it improves communication and allows organizations to speak using a shared language.

Because it doesn't specifically support or suggest specific tools, companies, or vendors (intentionally so), it's designed to be used as new technologies, systems, environments, and organizational changes arise, shifting cybersecurity needs.

Needless to say, the information it contains isn't applicable to American federal systems alone, and every enterprise has a lot to gain from embedding it's contents into their risk management frameworks.

NIST 800-171



The NIST 800-171, named "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations", is a companion to NIST 800-53 and dictates how contractors and sub-contractors of Federal agencies should manage Controlled Unclassified Information (CUI).

It supplies the list of 14 control families illustrated.

Again, although the document targets American federal agencies' contractors and subcontractors, its contents can (and I would say should) be applied to any other enterprise and figure in their RMF.

More information about these control families next…

NIST 800-171

1. Access controls

Make sure to limit access to CUI so only authorized individuals and devices can view that data. This covers core IT security aspects such as routers, firewalls, computers, servers, and any devices on your network.

2. Awareness and training

Staff should be educated on cybersecurity risks and best practices. NIST-compliant training also ensures that every individual can fulfill security responsibilities in alignment with their role. They should understand insider threats and how to identify them.

3. Auditing and accountability

All systems in use need to have an audit trail. Implementing an audit trail makes it possible to hold individual actors accountable for data access, viewing, storage, and handling. You'll therefore know exactly who has accessed CUI, when, and by what means.

4. Configuration management

Any software and hardware should have configurations that focus on creating the most robust cybersecurity measures possible in alignment with NIST requirements. Make sure to maintain this baseline security configuration even as new updates and firmware are released.

5. Identification and authentication

You need to identify every user, device, and process that attempts access to your systems at any given time. Make sure that you have the right technologies and safeguards in place to accurately authenticate identities via methods like biometrics or multi-factor authentication (MFA).

6. Incident response

Make an incident response plan that adequately prepares your teams for incidents. Your organization should detect any intrusions, analyze what's going on, contain the problem, and bring your systems back up. Also, have documentation and reporting processes that enable collaboration with relevant authorities.

7. Maintenance

The entirety of your information systems and data storage ecosystem should receive ongoing and proper maintenance. This keeps your cybersecurity posture and NIST compliance up to date and properly protected.

8. Media protection

Organizations handle CUI in a variety of ways, including storage on various media devices like external drives, CDs, and thumb drives. Any media systems or devices containing CUI need NIST-compliant protection, including access controls and processes by which media is sanitized or destroyed.

9. Personnel security

Anyone who accesses CUI must complete a thorough, NIST-compliant screening process. In addition, have procedures in place that protect every individual's CUI and private data if and when they are discharged or decide to leave on their own volition.

10. Physical protection

Cybersecurity itself isn't sufficient to comply with NIST 800-171. The physical location of systems or devices needs to be safeguarded in a way that prevents unauthorized on-site access. Rooms with devices or paper files should have access control measures like PIN codes and fingerprint scanners that allow only authorized individuals.

NIST 800-171

11. Risk assessment

Implement a risk assessment procedure and use it regularly to gauge the specific risk factors that your organization faces from a cybersecurity standpoint. Your CUI may be more susceptible to phishing attacks than ransomware, for instance, so a risk assessment will help point out these vulnerabilities and allow you to better mitigate them for NIST compliance.

12. Security assessment

Evaluate whether or not your current cybersecurity measures are doing their job adequately. A security assessment for NIST will help you understand how robust your current measures are, and if you need to update them based on the current threat environment.

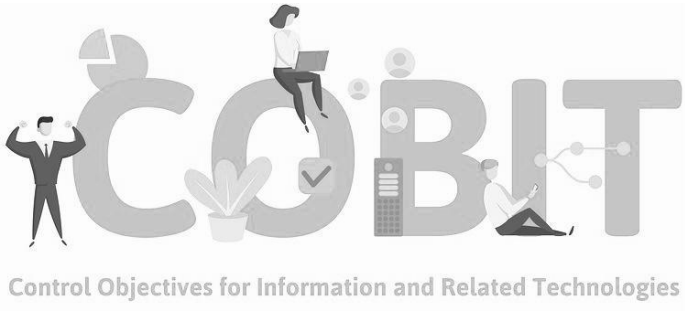
13. System and communications protection

Both external and internal boundaries of your information systems should be properly controlled, monitored, and protected. Things like email and SMS communications on the boundaries are at higher risk, so make sure anytime CUI is transmitted from one person to another, it's adequately protected or encrypted.

14. System and information integrity

The final NIST requirement centers around protecting your systems from malicious code and malware. You need to find, report, and fix all flaws in your information systems at all times. Monitor security alerts and take swift actions to ensure system and information integrity of CUI.

COBIT



COBIT (Control Objectives for Information and Related Technology) helps organisations meet business challenges in regulatory compliance, risk management and aligning IT strategy with organisational goals.

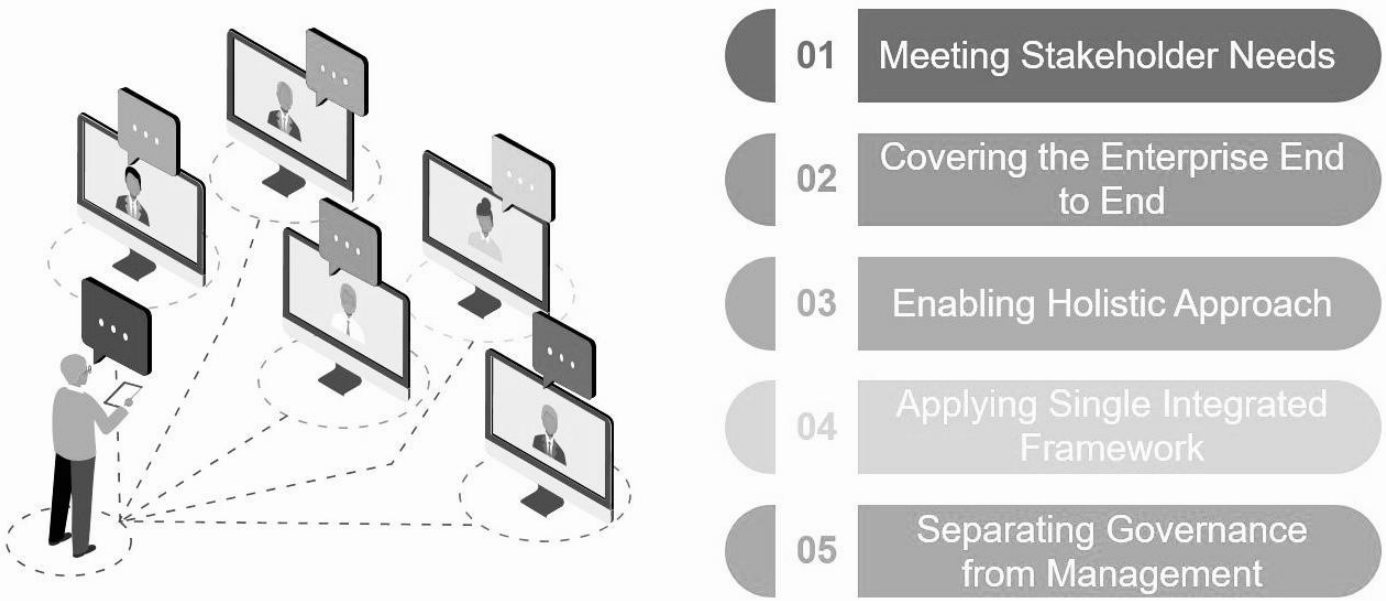
In other words, COBIT is a business framework for the governance and management of enterprise IT.

The COBIT 5 framework can help organisations of all sizes achieving the following:

- Improve and maintain high-quality information to support business decisions.
- Use IT effectively to achieve business goals.
- Use technology to promote operational excellence.
- Ensure IT risk is managed effectively.
- Ensure organisations realise the value of their investments in IT; and
- Achieve compliance with laws, regulations and contractual agreements.

COBIT

COBIT 5 is based on five principles that are essential for the effective management and governance of enterprise IT, as per the image:



These five principles enable an organisation to build a holistic framework for the governance and management of IT that is built on seven 'enablers':

1. **People, policies and frameworks**
2. **Processes**
3. **Organisational structures**
4. **Culture, ethics and behaviour**
5. **Information**
6. **Services, infrastructure and applications**
7. **People, skills and competencies**

Together, the principles and enablers allow an organisation to align its IT investments with its objectives to realise the value of those investments.

COBIT

Principles

Meeting Stakeholder Needs

The priority for all organizations is to fulfill stakeholder needs while maintaining optimal security for their data. COBIT enables this transformation and helps companies create strategies that will help them meet their goal.

There are three parts to this process. Organizations need to manage their resources optimally, and they also need to reap benefits from their resources. At the same time, the third factor involved in this scenario is the risks that come along with it.

COBIT creates a balance between all three factors for organizations. This process involves managing all the needs of the stakeholders, even the conflicting ones, by proper governance, decision-making, and negotiation so that the end result delivers value.

Taking a Holistic Approach to Governance

IT governance is more than just for the IT department. It needs to cover the entire organization, and COBIT does that.

One of the main principles of COBIT is to take a holistic approach to governance and work with IT, auditing, and management to create effective and enterprise-wide governance using certain ‘enablers’.

These enablers can be applied to all departments within an organization and are divided into five main categories:

- Principles and Policies
- Structures within the company
- All the information and data
- Processes of the company
- Competencies and skills of the employees

Covering the Entire Project

COBIT is also focused on covering the entire project as a whole when it comes to governance.

It integrates IT and enterprise governance into one platform by combining the IT services and processes along with the business processes.

COBIT has four main objectives here, which are to create value using governance, using the enablers effectively, assign roles and responsibilities, and deciding the scope of each project.

COBIT

Principles

Single Integrated Framework

COBIT is a single integrated framework to tackle all the changes in the technologies, manage risks, and govern information, all in one. It consistently covers the entire organization.

COBIT can also be customized to suit the needs of each and every organization and maintain regulatory standards for the company.

Creating a Difference Between Governance and Management

Since governance and management have different objectives, responsibilities, and different activities, they need different structures to manage them. COBIT integrates them and also separates the two by using different frameworks.

For governance purposes, COBIT uses the EDM method, which is to:

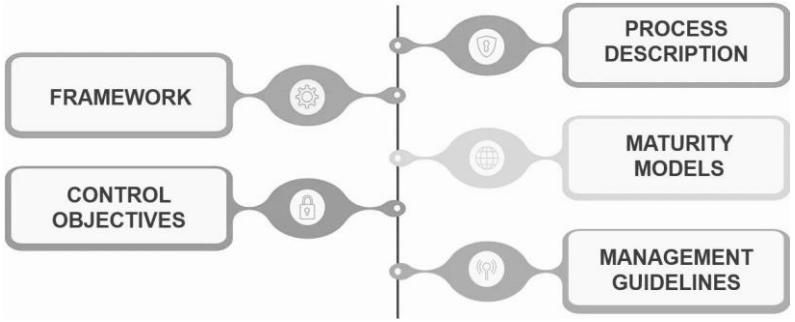
- Evaluate
- Direct
- Monitor

For management purposes, COBIT uses the PBRM method, which is:

- Plan
- Build
- Run
- Monitor

COBIT

COBIT has five components as illustrated:



1. COBIT framework

The COBIT framework is designed to help organizations organize and categorize all their objectives when it comes to IT governance. It also helps companies follow good practices in the IT domain and integrates it with the business requirements as a whole

2. Process descriptions

These descriptions provide organizations with a process model and create a common language for all departments across the enterprise.

3. Management guidelines

These management guidelines are used to assign job roles and responsibilities for IT governance. This helps in creating a uniform structure across the company and helps departments work together and agree on their business objectives as well as measure overall performance. The guidelines also showcase the relationship COBIT has with all other processes in the organization.

4. Maturity models

Maturity models in COBIT are used to better understand the capability and maturity level of each process and work on any gaps found in the same.

5. Control objectives

The control objectives created in the COBIT framework give organizations certain requirements they need to meet so that they can manage their control of IT processes effectively in the company.

ISO/IEC 31000

The ISO 31000 Risk Management framework is an international standard that provides organizations with guidelines and principles for the design and implementation of a risk management framework.

The standard enables organizations to apply risk management to all strategic, management and operational tasks as well as to projects, functions and processes.

ISO 31000 is designed to be used in organizations of any size. Its concepts work equally well in the public and the private sector, or in large and small businesses and nonprofit organizations.

It provides a universal standard for practitioners and companies employing risk management processes.

The ISO 31000 standard is based on three main components: principles, framework, and risk management process. These components are interconnected and reinforce each other to provide a coherent and effective approach to risk management.

ISO/IEC 31000

ISO 31000 carries a significance number of benefits to an enterprise adopting it, not exclusive to but including:

Effectiveness

- Because ISO 31000 is an internationally recognized standard, it's used by countless organizations. This means that ISO 31000 has been thoroughly vetted and proved to be effective.

Addresses risks in a standardized way

- When properly implemented, ISO 31000 acts as a template to help organizations identify key drivers of risk. It establishes risk criteria and risk treatments in a standardized way.

Creates a culture of risk mitigation

- By incorporating risk mitigation into nearly all business processes, employees become used to the idea of identifying and potentially mitigating risks.

Increases the organization's profitability

- When an organization mitigates unnecessary risks, it also reduces the potential for financial damage stemming from events tied to that risk.

Utilizes what is already in place

- ISO 31000 is just one of many ISO standards. The various standards are designed to work together, which means that organizations should be able to incorporate the ISO 31000 strategy within their existing management systems without much additional work.

Compels an organization to be more preemptive

- A good ISO 31000 implementation can help an organization shift from being reactive to taking a more proactive approach to risk mitigation.

Helps the organization acquire funding more easily

- Banks and investors tend to be risk-adverse. If an investor is convinced that an organization is serious about identifying and mitigating risks, it might be more likely to approve an investment.

ISO/IEC 31000

ISO 31000 relies on 8 main principles:

1. Integration: Risk management should be integrated at all levels of the organization and in all processes.

2. Structured: Risk management should have a structured approach in the organization's governance.

3. Personalization: Risk management should be tailored to the specific needs and characteristics of each organization.

4. Inclusion: All relevant stakeholders must participate in the risk management process.

5. Dynamism: Risk management should be proactive and capable of adapting to changes in the internal and external environment.

6. Continual improvement: The organization should constantly seek opportunities to enhance its risk management approach.

7. Evidence-based: Decision-making in risk management should be based on accurate and up-to-date information.

8. Human and cultural factors: Human behavior and culture influence risk management.

ISO/IEC 31000

As a framework, ISO 31000 includes:

0. Leadership and commitment

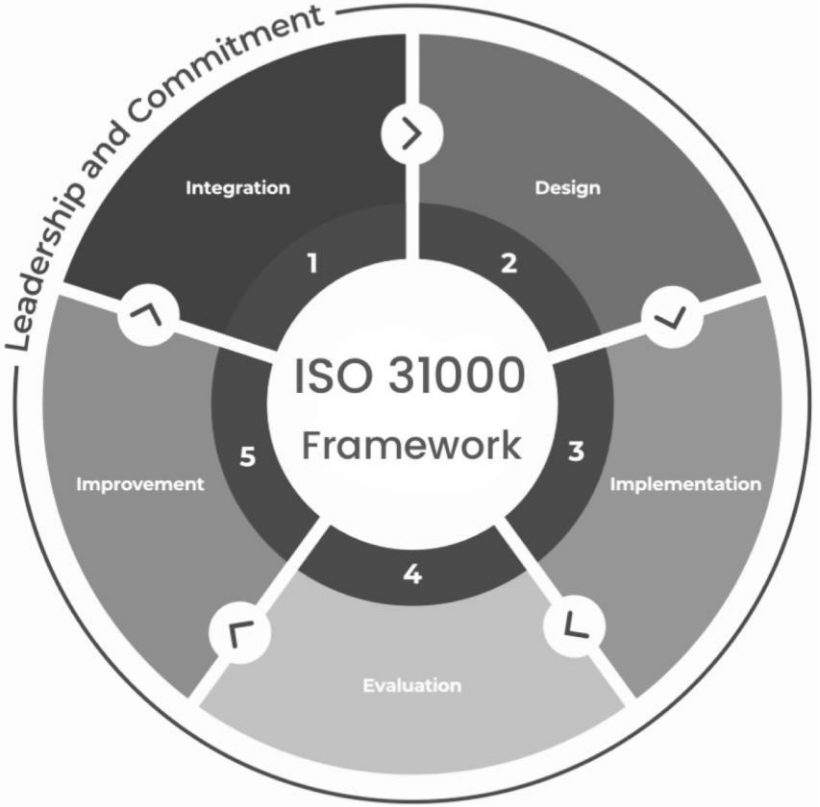
- Required from top management and crucial to aligning risk management with the objectives, strategy, and culture of the organization. Oversight committees are responsible for overseeing risk management and ensuring that risks are considered when establishing the organization's objectives.

1. Integration

- The integration of risk management depends on understanding the structures and context of the organization. Governance and management structures translate strategic guidance into concrete actions to achieve sustainable performance. All members of the organization have the responsibility to manage risk.

2. Design

- The design of the framework involves understanding the organization's internal and external context, establishing commitment to risk management, assigning roles and responsibilities, allocating adequate resources, and establishing effective communication and consultation with stakeholders.



ISO/IEC 31000

Framework (continued)

3. Implementation

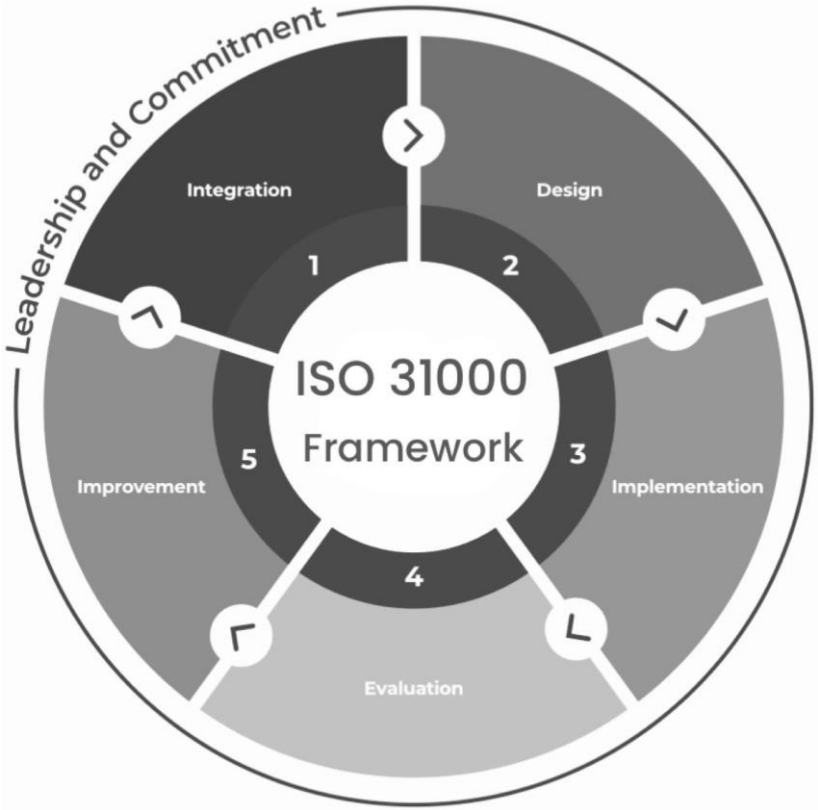
- The successful implementation of the framework requires a proper plan, identifying decision-makers, and modifying relevant processes. Periodic performance assessment and continuous improvement are essential to ensure the effectiveness and adequacy of the framework.

4. Evaluation

- Establishing a continuous monitoring process to oversee the implementation of risk management strategies is necessary. Enterprises must periodically evaluate the performance of the risk management process and its effectiveness in relation to established objectives.

5. Improvement

- The organization should continuously adapt and improve the risk management framework based on internal and external changes, using the identified gaps and improvement opportunities, and assigning responsibilities for its implementation.



ISO/IEC 31000

The Risk Management Process

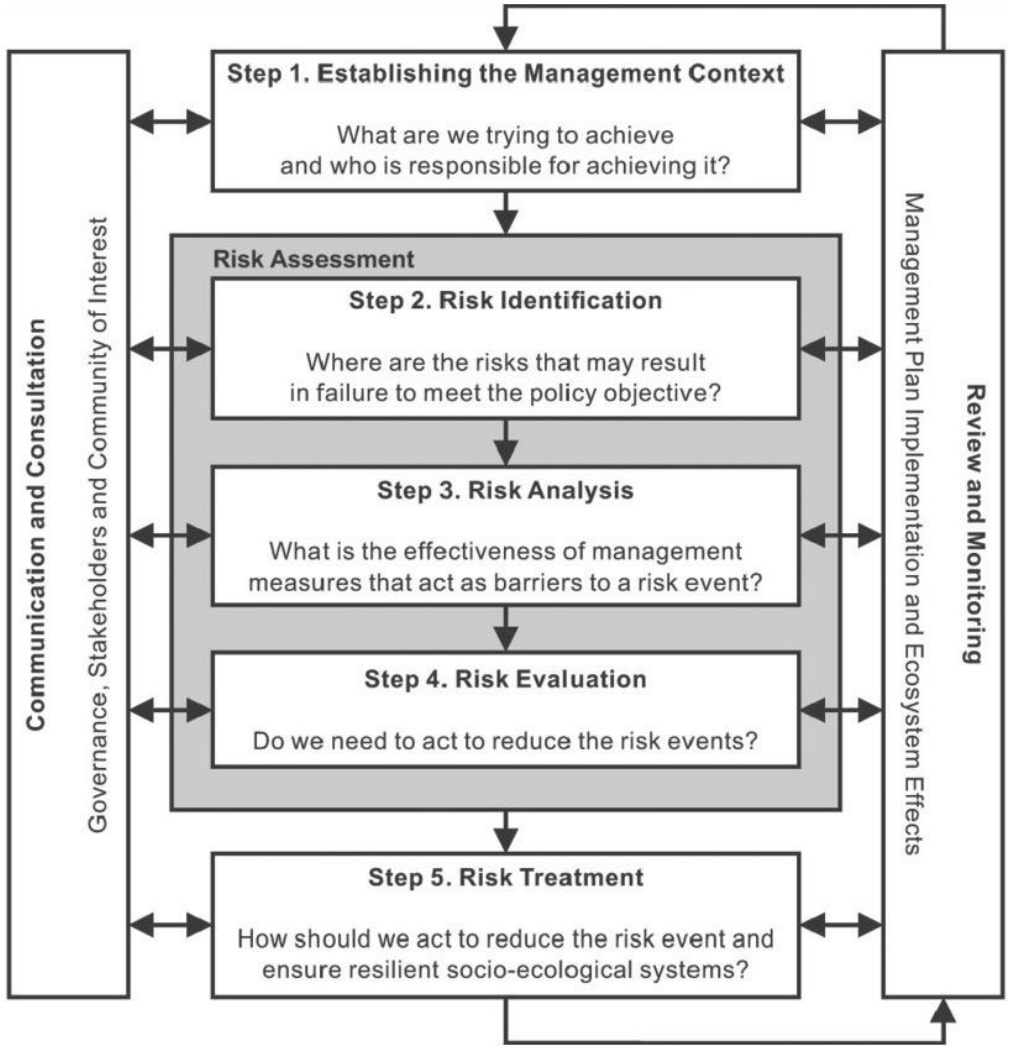
The diagram explains how the above comes together in an iterative risk management process consisting on several stages:

1. General:

- Establishing the framework and principles for risk management in the organization.
- Defining the roles and responsibilities of the parties involved in the risk management process.

2. Communication and consultation:

- Establishing a communication and consultation approach to support risk management.
- Sharing relevant information with stakeholders and gathering their feedback.
- Ensuring that communication and consultation are timely and effective.



ISO/IEC 31000

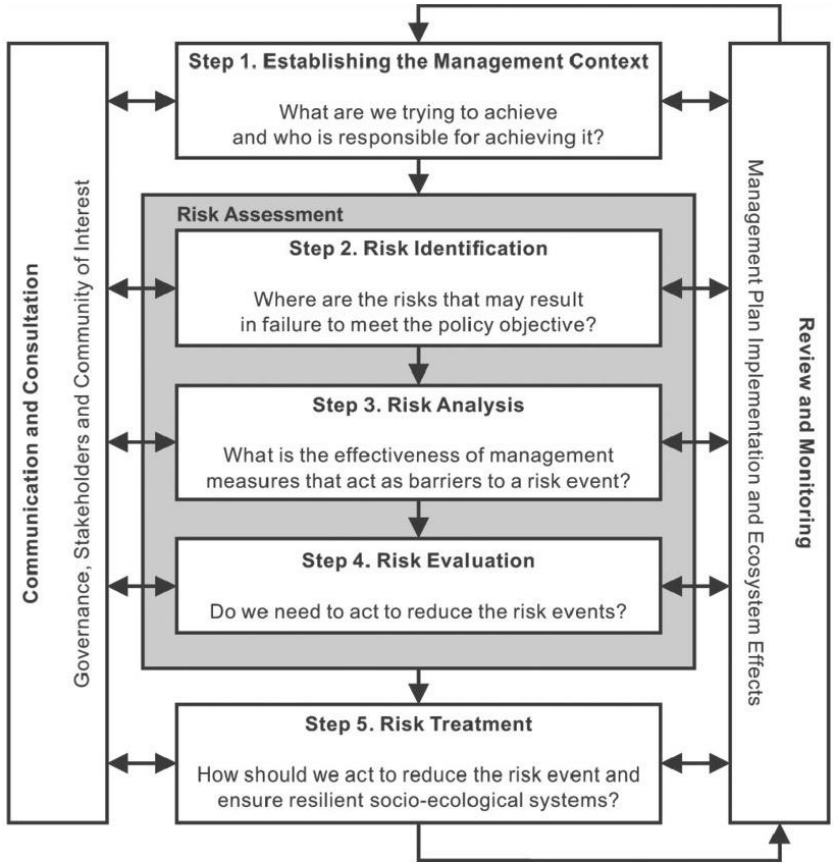
The Risk Management Process (continued)

3. Risk assessment:

- Identifying the relevant risks for the organization.
- Assessing the probability of the risks occurring and their potential impact.
- Analyzing the interrelation between risks and their potential accumulation.
- Prioritizing the risks based on their importance and establishing the basis for informed decision-making.

4. Risk treatment:

- Developing and implementing strategies and actions to address the identified risks.
- Selecting the most suitable options to address the risks, which may include avoiding, transferring, mitigating, or accepting the risks.
- Establishing controls and measures to reduce the probability of risks occurring and minimize their impact.
- Continuously monitoring and reviewing risk treatment strategies to ensure their effectiveness.



ISO/IEC 31000

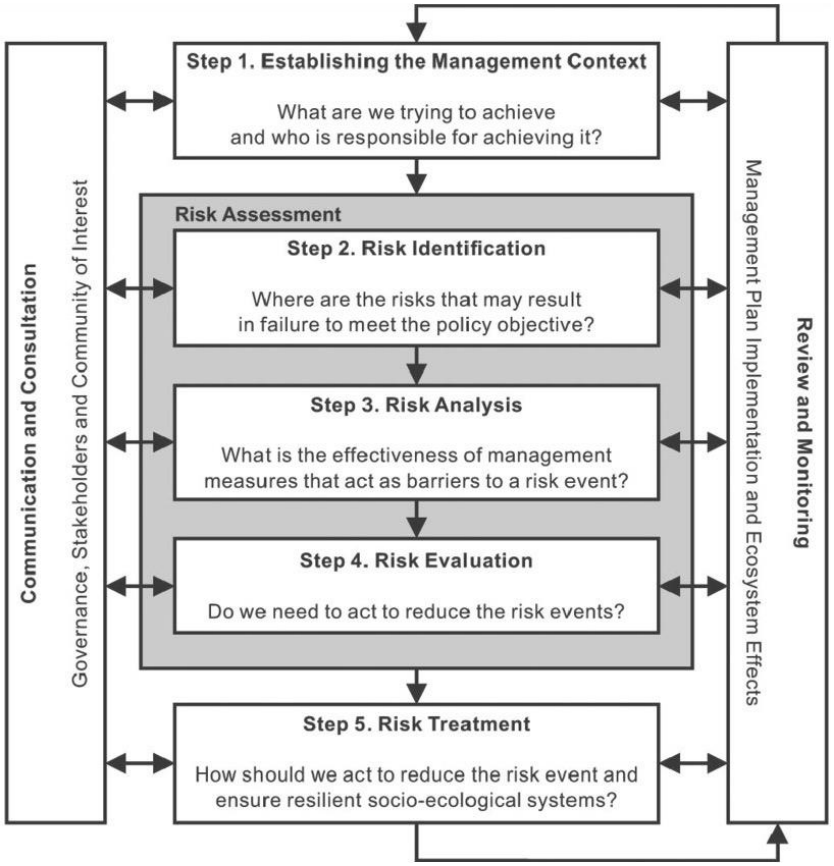
The Risk Management Process (continued)

5. Monitoring and review:

- Establishing a continuous monitoring process to oversee the implementation of risk management strategies.
- Periodically evaluating the performance of the risk management process and its effectiveness in relation to established objectives.
- Conducting regular reviews to adapt and improve the risk management process based on internal and external changes.

6. Registration and reporting:

- Maintaining proper records of identified risks, actions taken, and outcomes obtained.
- Generating reports on the status of risks and risk management activities to inform stakeholders.
- Communicating the results of the risk management process and any relevant changes to stakeholders in a clear and effective manner.



Once again, do remember that the risk management process is iterative and continuous, and must adapt according to the organisation's context and requirements, in order to constantly improve the ability to identify, assess, and effectively treat risks.