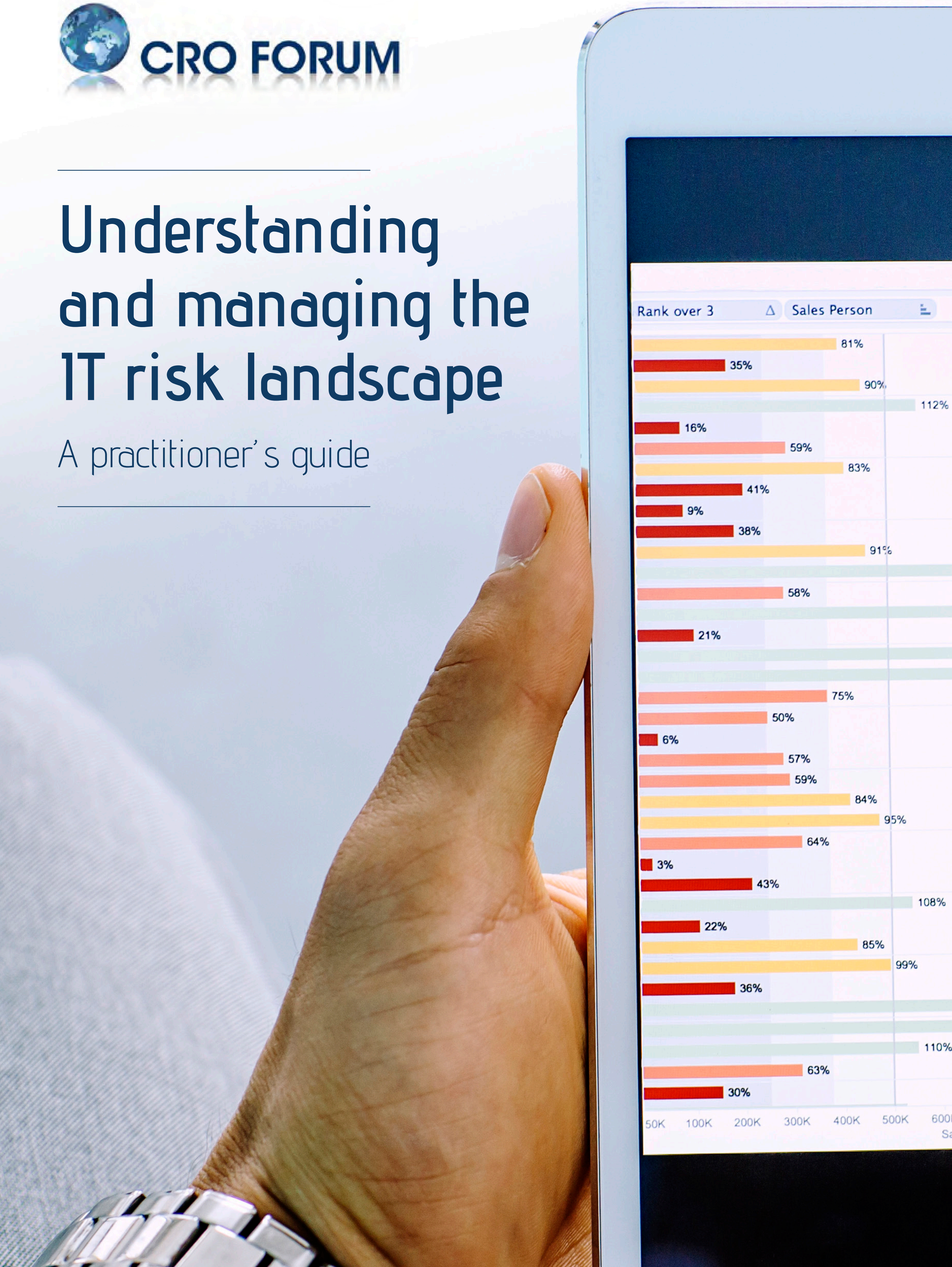
CRO FORUM

Understanding and managing the IT risk landscape

A practitioner's guide



Contents

Executive summary and context

Failure to suitably align IT and business strategies, to implement an effective IT governance, to attract and engage 'fit and proper' IT staff, or to deploy effective and resilient risk management processes, could all lead to wasted investment and an inability to adequately support the business. This could in turn result in rising costs, lower responsiveness, and a reduced ability to innovate.

Purpose of the paper

In a world increasingly subject to digitalisation and the use of technology, an ineffective IT strategy and failing IT are amongst the most significant risks facing the boards of most organisations. The purpose of this paper is to provide a practical guide to Chief Risk Officers (CROs) and senior risk professionals active in the insurance industry on the main threats and developments in the IT landscape in which they operate, and support them to effectively measure and manage these risks in their organisations.

Identification of these risks is necessary to have a solid understanding of the effects on an organisation. This can be done based on a business impact assessment (BIA) process[1]. The impact of a potential loss of **C**onfidentiality, **I**ntegrity, **A**vailability, **A**uthenticity of data[2] and the agility / **D**elivery of IT are some predefined categories which can be used to evaluate these potentially material risks (based on **CIA-AD criteria**), including examples such as:

- Risks of data leakage, causing loss of confidential customer data, or example of other sensitive data potentially leading to market abuse (***C****onfidentiality*);
- The accuracy of calculation rules and customer data (***I****ntegrity*);
- Fraudulent activity, potentially resulting in substantial financial losses (***I****ntegrity*);
- System outage seriously affecting operations and/or customer services (***A****vailability*);
- Based on multiple interfaces and manual input, data is collected in the golden record of customers. Inconsistent and unreliable customer data received from a non-trusted source will lead to an erroneous customer view (***A****uthenticity of data*);
- Future fit/agility: the capability of an organisation to adapt in time to changing circumstances and the flexibility of IT to support this (***D****elivery of IT*);
- Automation of IT itself has a profound impact on IT and possibly even more so on the nature of IT risk management. This will require a significantly different way of working and skillset (***D****elivery of IT*);
- Severe regulatory sanctions in case the enterprise is not able to conduct and demonstrate sound operational management or examples to comply with money laundering, customer due diligence, sanctions and anti-terrorist financing laws and regulations, which often require complex supporting monitoring systems (***D****elivery of IT*).

[1] BSI 100-4 Business Continutiy Management (2009): p.35 ff

[2] Some regulators, like BaFIN — the German supervisory authority, have identified Authentication as an additional criterion for attention

Chapter 1 examines the main trends in the internal (company) IT landscape as well as in the external environment and the primary risks arising. It covers internal developments such as company IT strategy, people and culture, resilience (business continuity) and monitoring activities focused on the IT landscape. Also, risks related to the use of external service providers, cloud providers and vendor management are discussed. In addition, we discuss the risk and regulatory concerns arising from the use of big data, complex algorithms, artificial intelligence and cyber risks. The chapter also explores technical developments in IT such as dealing with outdated legacy systems, platform hardening, network architecture and implementation, new technology developments, and risks around software and product and development.

Chapter 2 describes the organisational roles and responsibilities in operating and controlling modern, complex and fast-evolving IT environments. After a general introduction on the well-known 'three lines of defence' model, it elaborates on:

- the responsibility of the management board in understanding the risks related to the IT landscape and explores the alignment of business and IT strategy;
- the governing roles of the management board and its accountability for propagation of a proper and solid risk culture;
- the managing role of business and IT management and describes responsibilities of various C-level functions like Chief Operating Officer, Chief Technology Officer/Chief Information Officer and the Chief Information Security Officer;
- the supporting role of the CRO and information risk management, such as providing independent supervision, developing the policy house (policy, standards and guidelines), reporting on risk exposures, monitoring and challenging of first-line activities and the development and maintenance of a waiver process;
- the independent assurance role of the internal audit function is described including the most important attention areas for the annual audit plan.

Chapter 3 describes the IT risk framework. As a CRO, one key objective is to ensure a consistent framework is selected and used throughout the organisation by all lines of defence (one consistent risk language). A high-level overview of the number of general and specific methodologies is discussed. It starts with the context, outlines the need to have specific IT risk frameworks due to the ubiquitous and interrelated nature of IT, the complexity of the IT environment and the pace of technology changes and new challenges for risk management such as cyber risk and the recently introduced data protection legislation in Europe (GDPR).

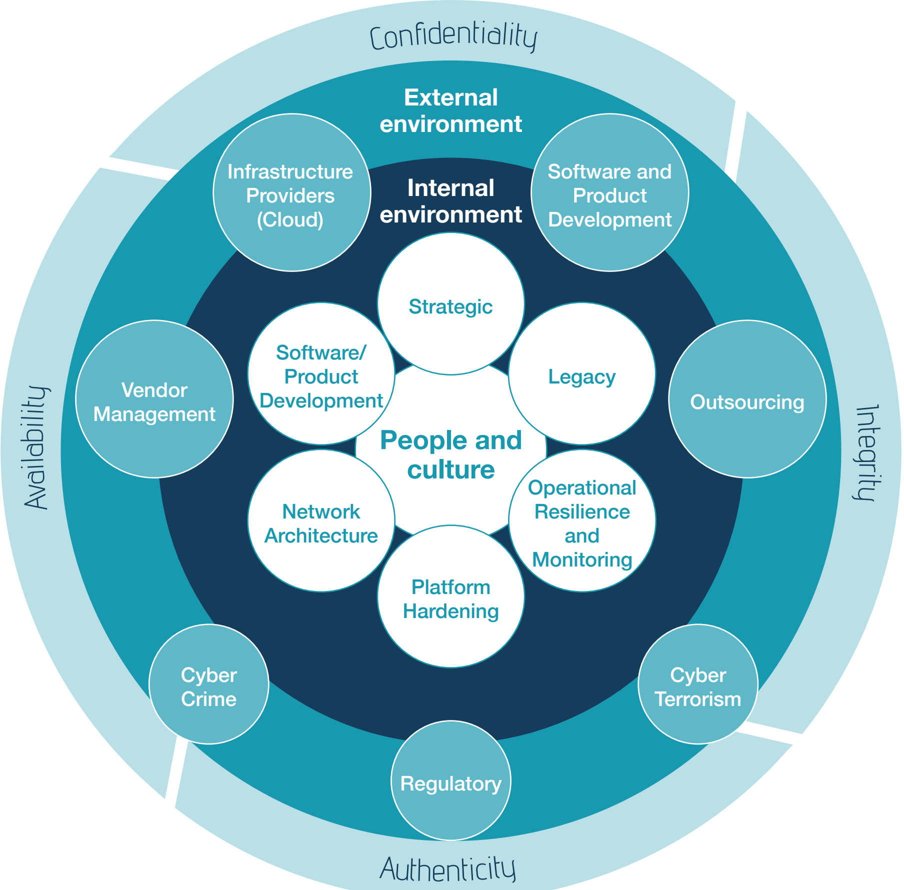
The paper describes the process of setting and maintaining risk appetite for IT risks and the benefits thereof, the process for establishing KRIs (key risk indicators) and tools and techniques in use, and breaks down the sub-steps of the IT risk management process. The paper emphasises the importance of selecting the right ('fit for purpose') IT risk framework as it should be compatible with the enterprise ERM strategy and impacts other programs, e.g., resilience, regulatory compliance and internal and external sourcing. The paper studies different frameworks commonly used in IT, describes the main purpose and focus of each framework and the main advantages and disadvantages.

1 Understanding the main trends in the IT landscape and the primary risks arising

1.1. Introduction

CROs and risk management functions are facing several potential risks arising from the IT landscape. Within an insurance company, IT is interwoven with the products we sell our customers, our front, middle and back-office processes and increasingly also our customer contact points (via portals and applications). This makes IT a core business activity for an insurance company. In this chapter, we will discuss recent developments in the IT landscape and focus on the mitigation of possible information risks. A distinction is made between internal, external and technical developments. We can evaluate the main trends in the IT landscape and the primary information risks arising based on the 'CIA-AD' framework described in the executive summary. The diagram below further elaborates on this framework and outlines, conceptually, the primary components of the IT landscape.

Agility/Delivery of IT



1.2. Developments in the internal environment

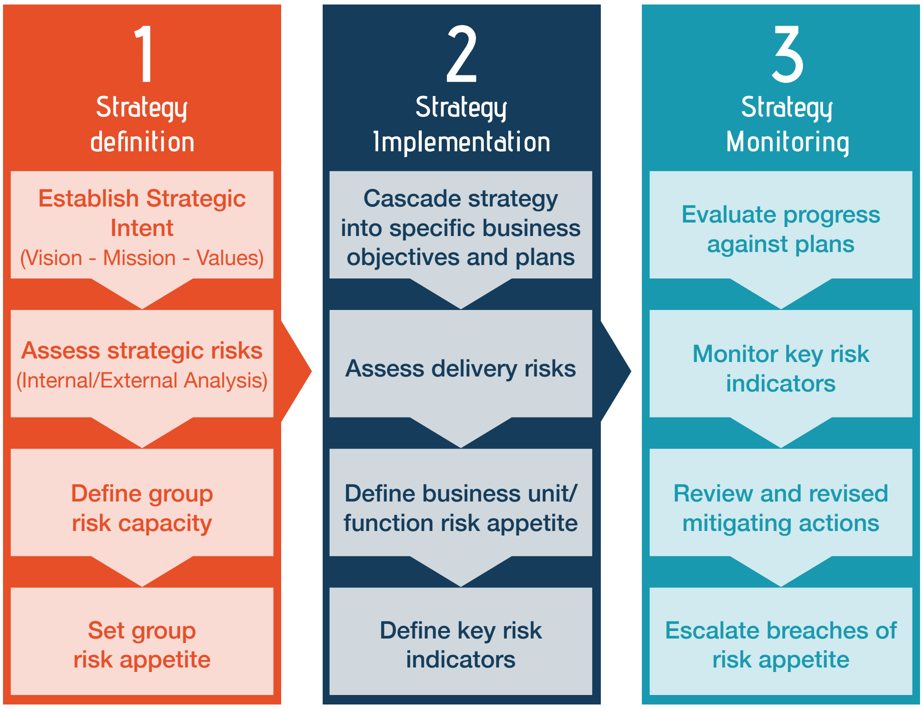
Information risk management[3] and resilience have become increasingly significant across organisations in recent years, becoming one of the recurrent key themes at board meetings. Cyber-attacks have become increasingly commonplace and the trend is an upward one. For example, according to a 2016 PwC survey[4], there were 38% more information security incidents detected in 2015 than in the previous year. The same report also highlighted the increasing costs to organisations of such incidents; the direct financial implications breaches can also have disruptive consequences on an organisation's reputation and negative impact on customers' and stakeholders'

[3] Definition of information risks: includes those risks involving IT, information security, project and program management, business continuity, data governance including data privacy, digital, and related innovation/emerging technologies

[4] PwC: Turnaround and transformation in Cybersecurity. Key findings from The Global State of Information Security® Survey 2016

trust. In addition, changes to the regulatory environment, for example, the introduction of the European Union General Data Protection Regulation (EU GDPR) are changing the way organisations must collect, manage and protect information and add a new dimension to the responsibilities of management to control cyber risks.

The importance of controlling cyber risks is also realised by globally-recognised and respected bodies such as the World Economic Forum, which has ranked cyber risks amongst its top risks for the last five years in its annual Global Risk Report[5]. This is an evidence, if further evidence is needed, of the risks posed by the changing nature of technology, the interdependencies and interconnectivity of organisations and the vast amounts of data that they collect and hold.


1
Strategy definition
Establish Strategic Intent
(Vision - Mission - Values)
Assess strategic risks
(Internal/External Analysis)
Define group risk capacity
Set group risk appetite
2
Strategy Implementation
Cascade strategy into specific business objectives and plans
Assess delivery risks
Define business unit/ function risk appetite
Define key risk indicators
3
Strategy Monitoring
Evaluate progress against plans
Monitor key risk indicators
Review and revised mitigating actions
Escalate breaches of risk appetite

Information risk, whilst not unique amongst other operational risk types, does, to some extent, stand out and warrant special attention because of the:

- ubiquitous and interrelated nature of IT in our society;
- complexity of IT environments within organisations;
- pace of technological change;
- volume and attractive nature of the data being processed and stored within IT systems;
- level of threat from cyber criminals seeking to exploit data and systems for malicious purposes.

Moreover, some organisations actively aspire to be more innovative and advanced in terms of their information risk management capabilities, recognising that it can be a differentiator in their marketplace, providing a competitive advantage and thus preserving profitability and managing stakeholders' expectations, as well as being a marketing opportunity to expand their service offerings.

However, whilst these challenges and opportunities may require a specific IT risk management framework to be adopted by organisations, in essence, IT risk management remains the application of standard risk management methods to IT resources. As such, it should be an integrated component of an organisation's wider strategic and enterprise risk management framework, processes and tools.

Generally speaking, an IT risk management framework should have a number of touchpoints with a general risk management framework. These are outlined further below.

1. **Strategy definition:** As part of an organisation's overall strategy development, it will assess strategic risks both internally and externally. For most organisations, this will include a high-level examination of IT from both an organisational and technical perspective to ensure alignment of the organisation's overall aspirations and the high-level plan for IT, and to identify any associated risks or uncertainty that may arise.
2. **Strategy implementation:** As with any other business or functional area, IT will be required to develop a set of objectives and plans to support the implementation of the strategy. To support these, IT departments need to implement standard risk management processes including a detailed risk assessment, followed by an appropriate risk response (treat; tolerate; terminate; transfer), establishment of a risk appetite and key risk indicators.
3. **Strategy monitoring:** The implementation of the IT-strategy objectives and plans needs to be monitored throughout the strategy-planning cycle. This includes evaluation of progress, monitoring of key risks and mitigations and escalation of any breaches (or potential breaches) of risk appetite.

1.2.1. Strategic

The company IT strategy should provide a holistic view of the current business and IT environment, the future direction, and the initiatives required to migrate to the desired future environment.
The main objective to be taken into account is the alignment between the business objectives and business models indicating the medium- and long-term IT demands for the company.

[5] World Economic Forum: The Global Risks Report 2018

A specific part of the IT strategy deals with the application of emerging technology trends that will influence and potentially disrupt the business. This is a very specific consideration to be made in the Board, but requires linkage to specialised technology experts who have sufficient experience. For example, the latest technology trends and developments in companies like Fintech and Insurtech.

The IT strategy should describe how IT-related goals contribute to the company strategic goals, and should be communicated to the business owners in the organisation, where further translation into business objectives should take place. We distinguish three major types of threats:

(i) Misalignment between the IT strategy and the business strategy in the organisation: As a consequence, the IT landscape/architecture and IT services may not reflect the enterprise needs, leading into:

- inflexible and/or complex IT architecture;
- costly implementation of IT solutions;
- missing or poor functionalities;
- unreliable execution of IT.

(ii) Incomplete or simplistic description of the IT strategy: As a consequence, the IT risk profile is not consistent or does not reflect the objectives of the IT strategy, leading into:

- poor internal control procedures;
- missing controls, or controls with design or effectiveness deficiencies;
- erroneous risk assessment;
- wrong implementation of security measures.

(iii) Unclear strategic alliances with business partners: As a consequence, the IT organisation may not deliver the expected IT service, resulting in:

- growing/developing limitations;
- missing competencies and faulty ‘solutions’;
- poor value chain for the organisation;
- a disadvantage relative to competitors.

To mitigate these risks, the following measures/controls are recommended:

- Ensure that a document describing the overall business strategy and strategic goals of the different activities carried out by the company is developed and maintained;
- Assess and identify gaps between current business and IT capabilities and IT services;
- Define the required and desired business process, IT capabilities and IT services, and describe the high-level changes in the enterprise architecture (business, information, data, applications and technology domains);
- Conduct a gap analysis between the current and target environments;
- Identify and adequately address risk, costs and implications of organisational changes, technology evolution, regulatory requirements, business process re-engineering, staffing, insourcing and outsourcing opportunities, etc.;
- Define the initiatives that will be required to close the gaps, the sourcing strategy and the measurements to be used to monitor achievement of goals, then prioritise the initiatives;
- Determine dependencies, overlaps, synergies and impacts of the strategic alliances with business partners.

Your risk culture will become stronger and more effective if you repeat the main company values again and again using different communication channels and with support from your management board members. The tone on the top is very important and should be consistent with daily practices; walk the talk.

1.2.2. People/Culture

The primary objective of the ‘people and culture’ dimension is to increase the **awareness of information risks and urgency of IT** as the main enabler in the day-to-day processes and to ensure that a solid and embedded risk culture is established and maintained throughout the enterprise. Knowing the competences needed for all the tasks and activities within your lines of business is necessary to achieve this.

Attention is needed for ongoing training, education, coaching and tailor-made engagement programmes. Technology continues to develop rapidly, requiring relatively high investments in trainings and to keep organisational IT knowledge and experience up to date. Regular staff rotation could be considered to prevent blind spots development as those could evolve into serious limitations in knowledge and skill gaps.

Increased regulatory requirements and expectations of the societies within which companies operate, are expected to lead to an increase of demand for specific expertise in customer conduct, for example to develop monitoring systems.

New ways to develop software, such as agile development, will bring important necessary changes in habits and behaviour and in skills, capabilities and amounts of resources needed. Self-organising and cross-functional teams require a different way of management than teams developing software in the traditional way (see chapter 1.4.8. Agile development).

Outsourcing IT services to third-party vendors, requires sufficient remaining capabilities and knowledge and development of new skillsets to stay in control over the outsourced service. An often occurring risk is that such knowledge gradually disappears over time because the related tasks shrink in size and importance, or are no longer attractive to IT professionals. Sometimes specialised staff is ‘following work’ and is transferred to outsourcing partners. Furthermore, a clear understanding is required of key man exposure in an organisation's IT Function and the possible consequence if this risk materialises.

It is important to consider how performance goals, remuneration packages including variable reward and the outcomes of risk tracking and testing are linked and balanced. It is recommended to explain to your employees what you expect from them based on the company values. It is important to promote a culture where people are encouraged to report mistakes and deficiencies without delay, enabling the IT organisation to address them quickly, instead of not being transparent about such failures and trying to hide the bad news and hoping that problems will be solved before they explode.

Measure the level of risk awareness and risk culture of your staff, and evaluate the changes needed in people knowledge and culture at least once a year.

Suitable awareness and culture are also key components in helping to defend against cyber-attacks. While people are often seen as the weak link in a technology-driven organisation, they can, through appropriate awareness, become the best defence. Furthermore, good HR practices in ensuring appropriate employment vetting as well as good ongoing tracking of joiners, leavers and transfers are vital in maintaining a healthy access management process.

1.2.3. Operational resilience and monitoring

Operational resilience can be defined as 'the capability of an organisation to continue the delivery of products or services at acceptable predefined levels following a disruption' [6]. This should be considered as 'a holistic management process that identifies potential threats to an organisation and the impacts those threats, if realised, might cause to business operations, , and which provides a framework for resilience that safeguards the interests of key stakeholders, reputation, brand and value-creating activities'[7].

The monitoring should be part of the resilience. It consists of ongoing monitoring of IT infrastructure, facilities, environment, internal and outsourced IT services such as applications, systems, and their related events, as well as a robust incident and problem management process. Furthermore, monitoring should support the swift agility and continuity of main processes. Recent developments have enhanced the requirement for robust resilience and monitoring, specifically:

- recent high-profile technology failures in the financial sector with resultant reputational impact;
- rapid technological and business changes, such as increasing use of cloud processing and outsourcing/ utilisation of third parties, both from a technical and business service perspective (thereby placing reliance on a widening service value chain);
- digitalisation and the reliance on it for enhanced customer distribution and communication channels;
- the increasing cyber threats;
- non-capturing/non-maintaining the correct or needed monitoring information will complicate the resilience to provide timely and effective response;
- in addition, regulatory principles often highlight that an organisation 'must establish, implement and maintain an adequate business continuity policy aimed at ensuring, in the case of an interruption to its systems and procedures, that any

> In the near future, there will be increasing deployment of machine learning, artificial intelligence and robotic processing automation within financial services. As these are integrated within the organisation's IT architecture, the importance of resilience will be key, as will the ability to fully understand their impact on the processing landscape.

[6] ISO 22300: 2018 Security & Resilience

[7] ISO 22301: 2012

losses are limited, the preservation of essential data and functions, and the maintenance of its regulated activities, or, where that is not possible, the timely recovery'.

To assure a robust resilience and effective monitoring, the following measures/controls are recommended:

- Procedures and rules to identify and record threshold breaches are defined, implemented and communicated;
- Recovery time objective (RTO), which is the acceptable amount of time to restore the service, and recovery point objective (RPO), which is the maximum time difference between last backup and breakdown of a system including loss of all recently entered data, are defined;
- Event logs, including security events, are produced and retained to assist in future investigations;
- Event logs are monitored and reviewed regularly for potential incidents and incident tickets are created in a timely manner;
- Relevant information is traceable to support root-cause analysis in case of any issue;
- An incident and problem management process are defined and implemented and should cover the entire chain including activities or services performed through intra-group servicing and/or through external third-party outsourcing;
- Classification and prioritisation schemes are in place and incidents are categorised, recorded and tracked;
- Rules and procedures for root-cause analysis, resolving, recovery and closing are defined;
- Escalation rules as well as communication paths are defined;
- Breach trend analysis is in place to detect trends, assess root causes and take lessons learned. As an outcome of the lessons learned, a catalogue of problems is maintained including known error records and sustainable solutions addressing the root cause;
- Status reports are produced according to the stakeholder's need.

1.3. Developments in the external environment

1.3.1. Outsourcing/Vendor management

Outsourcing of IT, either in full or in part, to external service providers (ESPs) has enabled organisations to realise cost efficiencies, increase flexibility, improve security and gain access to external technical expertise that they may not otherwise have had.

Although an organisation can outsource IT services, it cannot outsource or delegate accountability, which means that an organisation must stay in control over outsourced activities and has to identify and manage the risks associated with its use of ESPs. This includes the undertaking of appropriate due diligence prior to committing to a decision on outsourcing, as well as ongoing vendor management.

The growing use of ESPs and the potential impact on an organisation's operational resilience, especially given the increased targeting of smaller, more vulnerable ESPs by criminals in an attempt to steal the sensitive data or compromise the networks of larger organisations, means that management of ESPs has grown in significance.

A holistic and consistent risk mitigation process needs to be in place to identify and assess the risks of all the parties providing goods or services (e.g., even after termination of a contract, sensitive information might reside on the infrastructure of an ESP).

> **To mitigate the External Service Providers risk a risk-based approach including mitigating actions should be followed that covers the whole life-cycle of an engagement with an ESP.**

Some key IT outsourcing and vendor management risks and measures are explained below.

- Potentially, outsourcing increases the number of relationships, and also increases the system's complexity. Delineation of responsibilities becomes more important, as does establishing and maintaining an overview of how business processes flow across ESPs so that their impact, should a failure occur, is fully appreciated and possibly mitigated;
- When IT processes are split among IT infrastructure provider, application provider and business companies, it is necessary to build a strong cooperation and information sharing between the involved companies' risk management functions. This is required to allow a comprehensive evaluation and management of these shared risks;
- The responsibilities of the provider as business partner of its customers should be:
  1. to deliver the agreed IT services
  2. to ensure that the services delivered minimise the following risks in a cost-effective way:
     - Compliance risk: considering regulatory and legal requirements delivering the services (e.g., GDPR);
     - Security/Cyber risk: considering security measures by design;
     - Shared risk: considering the services and technologies shared among customers;
     - Technology risks: considering the available technology options.
- Outsourcing and vendor risk management, often lead to transfer of staff to the ESP and thus of the knowledge needed to monitor that these activities and services are performed in a controlled way;
- An ESP may have thousands of clients it serves and so may not be supportive in contractually agreeing an RTO/RPO (Recovery Time

Objective/Recovery Point Objective) and a sequence of bringing-up services that meets the service recipient's requirements. They may also not be prepared to agree penalties for non-fulfilment of agreed requirements;

- Economic power can be hugely distributed disproportionately. An organisation may have a hard time to obtain more than the ESP's standard contract conditions, or push through a meaningful monetary penalty that covers an amount anywhere close to the real costs of a business interruption;
- ESPs servicing a relatively large part of the financial industry, may form a kind of concentration risk in which many insurers rely on the same ESP;
- While the use of a single ESP may result in reducing costs, increasing dependence and reliance upon a single supplier can also represent an increasing business continuity risk should that supplier fail;
- Failure to identify all costs during the original business case may result in cost efficiencies not being realised;
- Failure to develop an adequate exit strategy, should an ESP go out of business, could put the organisation at risk;
- ESPs, themselves, might use sub-service providers for providing essential parts of the service (e.g., fourth party, fifth party, etc.). With the specialisation of service providers to specific pieces of the value chain, dependencies are not transparent anymore. For instance, a cyber incident at one of the ESPs might impact several, independent ESPs at the same time. While ESPs themselves are responsible for the sub-service providers they use, poor due diligence by them may leave their service recipients vulnerable.

It should be noted that there are many risks associated with outsourcing that are not directly related to IT, including contractual risk, HR (resourcing/skills), the outsourcing of core competences (like development of the business core system), data protection or other regulatory risks.

> **Cloud computing is arguably revolutionising the IT industry and the organisations that they support by transforming computing into a utility proposition.**

While much emphasis is placed on the initial due diligence and ongoing reviews of ESPs, the fact is that the reviews and associated review process are also a source of risk. These include:

- Identifying risks within ESPs which are often subjective and difficult due to limitations in access, real oversight and rights to audit;
- Organisations that use a large number of ESPs may struggle to scale their assurance program to cover the volume and depth of review required;
- Inappropriate targetting of reviews (to address the volume/depth challenge) may incorrectly discount the impact from seemingly low-risk ESPs;
- Over reliance on industry certifications and generalist questionnaires may hide underlying risks;
- Failure to implement an annual due diligence review invalidates past conclusions and assumptions;
- Failure to define and agree adequate key performance indicators (KPIs) and undertake meaningful regular service-review meetings to identify issues.

1.3.2. Infrastructure providers (cloud)

In many aspects, the risks associated with typical IT outsourcing and vendor management also apply to the cloud. However, there are some that are either cloud-specific or increased due to the limitations and restrictions that arise with a cloud engagement.

For some, the term cloud is an evocative label meaning a loss of control and increased risks, but generally most believe the cloud is not necessarily better or worse from a risk and control perspective than traditional on-premises solutions.

Cloud computing includes many different service models, typically, but not exclusively, Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS), and equally varied deployment models (Public, Private, Community, and Hybrid). Which cloud solution is appropriate will depend upon the type of data processed, and the provider's ability to address the business need, as well as an organisation's governance and security requirements.

With cloud, traditional management control and audit procedures have to be adapted. Especially in shared environments, where data of different customers is processed in the same datacentre, system or business applications, it is not possible to exercise a right to audit. Major cloud providers are addressing this need by regularly releasing assurance reports (SOC reports) or are compliant with international regulations and frameworks. Nevertheless, with the limited possibilities to run own assurance activities, the price for the new agility is often a reduced comfort level on assurance.

Within organisations, the cloud security discussion often seems to take place on the assumption that an on-premise cloud data centre is fully secure and compliant with legislation. This is an assumption only and cloud providers that are not able to provide assurance leave a control gap for the organisation, which should be considered before relevant business processes are outsourced. As a result, appropriate contractual wording and clauses become more important, especially those requiring compliance with international best practice frameworks and standards, and also timely notification in case of cyber incidents.

Despite the clear advantages, some other risks (many bridging multiple functions such as IT, compliance, legal and security) are explained below.

- Risks of data compromise — cloud makes use of virtualisation technologies which allows the flexibility to allocate resources on a shared environment as and when needed. The use of shared environments relies heavily on logical separation of client data to maintain confidentiality and integrity. Any failure of logical separation, due to a configuration error or unforeseen security vulnerability, (e.g. Spectre/ Meltdown) could lead to serious risks of data compromise;
- Secondary risks from other clients sharing the service also exist, if those other clients are themselves malicious or ignorant of security controls;
- Additionally, other clients may attract attacks due to their size and nature of business, and these could cause collateral damage to others, for example, poor performance due to a denial of service attack;
- The varying cloud models involve varying levels of responsibility on the part of provider and client. Failure to understand who is responsible for what could lead to critical activities (such as security patching or security monitoring) not being performed;
- Data centres are distributed around the globe in different legal and regulatory jurisdictions;
- With cloud provision dominated by a few key players, there may be risk accumulation as an increasing number of organisation's services are hosted on the same cloud;
- Interfacing hybrid clouds or integrating cloud with internal systems brings potential security, consistency and interoperability risks;
- Data ownership may be put at risk if stored in the cloud without due consideration of terms of conditions and legal contracts.

1.3.3. Cybercrime/ Cyberterrorism

Due to increased dependency on IT, we observe a strong trend whereby the IT capabilities of organisations are increasingly misused to conduct criminal activities. Cybercrime activities may affect, not only the organisation, but the whole financial industry or beyond. Cyberterrorism and cyberattacks are a moving target and could manifest in different ways (e.g., espionage, financial crime such as credit and debit card frauds, copyright infringements, hate crime, sextortion, intentional mental harm, performing attacks on other computers, and/or networks).

More instances of cybercrimes are observed crossing international borders and are committed by one or more nation states.

As an example, the Petya virus, affecting specific accounting software updates, had a significant impact on the availability of a large number of companies worldwide (including the Rotterdam Port) in 2017.

Other examples relate to the so-called 'phishing' activities, which entail a fraudster from outside the company persuading someone, often through the use of fake emails or online communications, from inside the company to give confidential data or personal data to someone outside the company. The emails and communications used often look and feel very similar to those sent from reliable sources, whereas in reality they are sent by fraudsters who hide their real identity.

Fraudulent emails and websites are also used to persuade a person to 'click' on a link or to 'click' on a link in the received email that triggers the installation of malware (e.g., spam providers, or 'botnets' that infect IT devices.) Some botnet families can hide for a long time in an organisation's processes or infrastructure, especially where companies have backlogs in patch management. Ransomware, whereby an organisation's IT is crippled unless an amount is paid to an anonymous third party, is another prevalent form of cybercrime.

The development of cybercrime triggered new activities from emerging IT security companies that offer SaaS solutions to financial and other industries. These solutions help in monitoring outbound and inbound internet traffic to detect and prevent cybercrime activities or to detect vulnerabilities in an entity's cybercrime protection measures.

The US government identified the risks of hardware related backdoors[8] in technology products purchased from, for example, China resulting in growing concerns over potential cyber-espionage, already in May 2012. This situation is still applicable, and the US government regulation explicitly requires a federal approval for their main departments before buying or selling advanced information technology abroad[9]. Issues first perceived as irrelevant (such as backdoors in hardware) may change in importance over time as circumstances change.

In general, increasing expertise of criminals and fraudsters is leading to an arms race in reacting effectively to continuously changing IT environments, developments and maintenance

[8] U.S. House of Representatives 112th Congress, October 8 2012, Investigative Report on the U.S. National Security Issues (Chairman Mike Rogers)

[9] https://www.forbes.com/sites/allbusiness/2018/08/13/mergers-acquisitions-and-investments-involving-u-s-companies-with-chinese-other-foreign-parties/#612e661b6c8e and https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

> Regulators are concerned about the use of (big) data and how to ensure that it is to consumers' and society's benefit. In some markets, regulators have begun to express concerns regarding the consumer impact of potential information asymmetries, for instance, if certain market participants develop a dominant position with regards to data.

Cyber security measures to consider within companies are as follows:

- A requirement to have an up-to-date and robust configuration management data base (CMDB) that contains information about the hardware and software components used in an organisation's IT services and the relationships between those components;[10]
- Require, based on a company's internal policy, complex passwords and the necessity of two factor authentication for all external connections and the critical part of internal network;
- Examine, at least once per annum, the level of preparedness against cyberattacks (this could be done as part of the regular business continuity testing);
- Ongoing monitoring of suspicious deviations/aberrancy in the firewall traffic from and to the internet connections of your company. Periodically, review the firewall rule settings for ongoing appropriateness, ensuring that firewall rules like 'any-to-any' are avoided;
- Identify vulnerabilities in the IT environment based on (red team, in other words independent and unannounced) penetration testing.

1.3.4. Regulatory

Regulators will continue to be concerned about consumer outcomes, and specific concerns regarding digitalisation have begun to materialise in regulatory supervision.

In addition, regulators continue to show a strong concern for cyber security risks. Regulatory actions have begun to reflect these concerns — several regulators have carried out reviews of insurers' use of data, though few new regulations have emerged recently, which may be due to regulators not wishing to hinder industry innovation efforts. Regulatory concerns in European markets include:

- **Use of big data:** How to ensure that it is to consumers' and society's benefit? Is GDPR the role model to regulate data usage worldwide? How clear is the interpretation of 'legitimate purpose' or 'high risk'?
- **Algorithms, artificial intelligence (AI), robotics, machine learning:** How to get comfortable with algorithms taking decisions? How to rule out potential discrimination? Who is liable?
- **Information security risks like cyber risk:** How to make society safe? How can insurance support cyber security? Are international standards needed or useful? How could they look like? For example, the Italian regulator IVASS in its last regulation's update requires risk management to include the strategies, processes, procedures, including reporting, necessary to identify, measure, evaluate, monitor, manage and present, on an ongoing basis, current and future risks to which the company is or could be exposed, with particular attention to related interdependencies and potential aggregations.[11]

> Furthermore, regulators have begun to scrutinise the effectiveness of IT systems supporting and monitoring compliance with specific laws and regulations such as those regarding customer due diligence, sanctions, anti-money laundering and terrorist financing.

[10] https://searchdatacenter.techtarget.com/definition/configuration-management-database

[11] https://cms.law/en/content/download/334109/8412381/version/1/file/Indagine%20cyber%20risk%20dell%E2%80%99Ivass.pdf

- **Effectiveness of IT-based systems to support compliance with laws and regulations:** These include customer due diligence, integrity screening identified staff, anti-terrorist financing (transaction monitoring), anti-money laundering, and sanctions and politically exposed person monitoring.
- **Sufficient control and monitoring over outsourced processes:** When outsourcing a process or activity, sufficient capabilities should remain to ensure adequate control, monitoring and overseeing of the outsourced process. Questions to consider include whether risk or audit are involved at the start of the outsourcing process and whether assurance and control statements cover the right scope. The concentration risk of many financial institutions using the same vendors and/or of a potential over-reliance on one vendor should also be considered.

Several regulatory initiatives have been targeted at enabling innovation as a means to increase insurance coverage options for consumers. Whether enabling or limiting, the regulatory response to insurance innovation remains fragmented. If a higher degree of collaboration across markets cannot be achieved, large, global incumbents will be less able to harness scale benefits. The International Association of Insurance Supervisors (IAIS) has recognised the need for stronger coordination of regulation of technology-based innovation, but no effective international standards have yet been developed.

As insurers collect increasing amounts of personal data, the use of such data will require an increasingly robust governance and risk management framework. Compliance with legal requirements alone may not be enough as customer demands for data protection and privacy may exceed regulatory requirements. It may become increasingly important for companies to be able to explain how they use any data they collect and store, and to help consumers understand the benefits of sharing their data with insurers.

The world is constantly changing. New technological developments can be a game changer. The continuity and profitability of a company may be jeopardised , if a company does not adapt quickly.

Advances in the technical environment (internal/external)

1.3.5. Legacy

Legacy systems tend to be defined as those that are using ‘old’ technology, whether infrastructure, software or both, that has since been superseded. The term is often used to denote a system that is out of date and requires replacement. However, often due to its effectiveness, complexity, interrelationship with other systems, prohibitive costs to replace, as well as a desire to see a return on investment, many organisations continue to use them.

Despite their relative longevity, **legacy systems do pose specific risks to the organisation** which include:

- High and increasing maintenance costs; over time, systems undergo considerable change and customisation from their original implementation. Any upgrades may require such changes and customisation to be redone leading to increased costs. There is also a likelihood that documentation to support these changes has not been kept current, or even still available, which will add to both the cost and the upgrade failing to meet expectations;
- Functionality may not adequately support new business requirements, or that business processes are unduly restricted by their dependency on the legacy system, leading to a suboptimal business process and hindering future innovation;
- Lost or reduced service availability due to lack of support or lack of replacement components;
- A lack of integration capability with newer technologies will leave significant intellectual capital isolated, reducing its value to the organisation;
- A dwindling resource pool as the number of experts with relevant experience reduces, and will impact the organisation’s ability to operate, support, maintain and develop the system;
- Older systems are more likely to be vulnerable to security attacks (malware). The problem is further compounded if the system is impossible to patch or no patches are further available;
- Increase of data integrity risk while transferring data to newer systems, due to different format or conversion functionalities.

Despite the risks, it has to be acknowledged that replacing legacy systems in itself can be both costly and risky, especially if the legacy system is also mission critical. It should also be acknowledged that the intellectual capital invested in legacy systems may indeed have created a solution that provides the business with a competitive advantage over others, that may be using more generic packaged solutions.

The reality is that the majority of legacy systems are mission critical and represent a risk to the organisation that owns and operates them.

> **In general, the platform hardening should be considered as a baseline of a broad range of controls which should be in place as a sanity. Without these controls, any instance of automation is expected to fail.**

1.3.6. Platform ‘hardening’

Platform ‘hardening’ is the process of securing and, at the same time, reducing its surface of vulnerability of operating system, databases and applications. As examples, this relates to changing default passwords, assuring the latest version of updates are implemented (patching) and the disabling or removal of unnecessary services.

A general information security threat relates to platform hardening. If the IT environment is not sufficiently hardened, organisations could be faced with a significant risk of financial or reputation loss due to misuse, abuse or theft of information caused by unauthorised access.

The main objective to consider for platform hardening is to ensure controlled and validated authorised access to customer data and company data. Additional objectives include preserving data integrity and information systems configuration, and to assure that the availability of key systems is guaranteed.

The main controls around platform hardening relate to:

- Guideline for configuration management incl. hardening guidance being available;
- (Automated) report about configuration changes
- Patching of infrastructure, middleware and at application level;
- Ongoing anti-virus scanning (main purpose is to protect against malware);
- Ongoing scanning of the configuration and security settings;
- Penetration testing done by an independent third party, sophisticated hacking techniques such as social engineering and advanced persisting threats;
- Two factor authentication controls (based on biometrics or SMS code on a second device) to the most critical external facing platforms;
- Encryption of data at rest (stored on a hard drive or disk) and data in transit (data communication);
- Restricted firewall rules.

We increasingly observe a shift from data centre computing to internet of things (IoT), mobile devices and bring your own device (BYOD). This should be considered ‘within scope’ of platform hardening activities as well.

1.3.7. Network architecture

Network architecture and network control implementation are key attention topics.

Often, the complexity of remote connections, to control the network access of remote entities and to make sure sufficient life cycle management is in place, are not easy to understand and cannot be easily explained to non-IT skilled employees, although the information risks will be critical if not managed properly. Topics like too much complexity in network architecture, incomplete overview of network components, ineffective lifecycle management (LCM) and capacity management, lack of effective sound practices in maintaining the network will have not only an impact on the availability, but also an effect on the overall information risks. Within the

> **To know what you have – especially in large and international operating companies- and to maintain and control the complex set up of different hardware / network components is a challenge in itself.**

IT organisation, the scope of network ownership can be a subset of the total network used within the organisation. One key question is to identify who has full responsibility for the complete infrastructure within your company.

1.3.8. Software/Product development

Software and product development frequently gives rise to information security threats, as well as improper delivery of IT (e.g., wrong implementation of the business requirements). IT is often a main component and success factor in the development. The emerging best practice is for applications to be 'secure by design', as incorrect or insufficiently mature usage of IT within the development process is likely to result in inefficiencies (e.g., future repair cost and the cost of correcting errors made earlier).

In addition, calculation errors can easily be amplified by automation. This needs to be considered explicitly when developing products for customers, as script or programme errors could adversely affect customer suitability when combined with automation algorithms and technology.

For both software development and product development, the emerging best practice is to ensure controlled and consistent lifecycle management in the development of products and self-developed software. A key control is to have all the stakeholders involved in development and to use a standard set of tests and approach to testing. When using incremental development methods such as 'scrum and agile', a small change can have a significant impact on the overall quality if testing is not properly executed and identified bugs not addressed. Also, maintaining adequate documentation of developments in a scrum or agile environment is a challenge.

To ensure consistent quality control over time, segregation of duties between the development environment, testing environment, acceptance environment and production environment (DTAP) is necessary. In addition, a solid software version control system should be implemented.

The general trend is to use generic building blocks in day-to-day processing, like Software as a Service (SaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS), or to use end-user computing for informal, easy-to-apply automation. In all these situations, effective testing and acceptance of the targeted functionality by all stakeholders should be implemented in all phases of the product lifecycle. Potential risk indicators around testing and acceptance include:

- Limited processes in place to identify, mitigate and coordinate interdependencies effectively;
- No consideration of the complexity and inflexible enterprise architecture when new software and new products are developed;
- The impact on IT infrastructure, IT operations and users is not always considered in the release of new or modified applications;
- IT services do not reflect the enterprise needs, or delivery of IT services is not in line with business requirements.

1.3.9. The internet of things

The internet of things (IoT) refers to the network of devices that include embedded computer systems connected to the internet (often through specially designed 'apps'), that are automatically collecting and sharing data. IoT, once the realm of science fiction, is now very much a reality. According to Gartner, there were approximately 3.9 billion connected devices in use in 2014 which had risen to 8.4 billion in 2017; that's more IoT devices than people.

Devices range from consumer-based wearable technology like health trackers (e.g. FitBits) that collect and transmit information about the wearer's activity or smart-home devices that learn our habits and adjust temperature and lighting automatically, to more complicated devices such as smart-sensors in cars, retail, agriculture and supply chain management.

The ability to connect devices to the internet and each other has already brought many benefits, but like the introduction of any new technology, it also has its issues, especially in relation to security and privacy. There have been many examples of IoT devices being compromised in recent years including taking control of webcams and baby monitors through researchers being able to remotely change a the in-car temperature of a vehicle by a prominent manufacturer and to influence the vehicle's steering and braking systems. IoT is also expected to have a significant impact within the insurance industry, for example, within health insurance, where some companies are already allowing customers to reduce their insurance premium by demonstrating through their activity tracker that they are attaining predetermined daily activity goals.

1.3.10. Big data

Big data is a term that is used to describe the large volume of data, both structured and unstructured, that inundates organisations on a day-to-day basis. Historically, organisations have collected this data over a number of years, often in discrete systems and multiple times with technology limitations on the ability to share and access the data between different parts of an organisation.

With the advent of technology such as IoT, the volume of data being collected during recent years has grown exponentially. In order to exploit such data better, businesses have been keen to establish big data solutions, to more effectively manage and complete meaningful analytics and insights to make better business decisions or, at the very least, derisk their decisions thus enabling cost reductions and increasing marketing and sales effectiveness. Therefore, it is necessary to have IT controls in place to mitigate the risk of loss of data integrity. Moreover, and depending on the kind of data (like personal data), it is also required to ensure confidentiality of the data.

1.3.11. Software robotics/Artificial intelligence

Software robotics or robotic process automation (RPA), is a software solution that automates manual business processes without the need to change existing IT systems. It works by monitoring, learning and replicating the activities that people undertake, using, for example existing business applications, manipulating documents and email systems to complete tasks. Not only can software robotics reduce operational costs, it can also improve service delivery and increase customer satisfaction.

Artificial intelligence (AI) takes software robotics to the next level making it possible for machines not just to mimic learnt behaviour but to actually learn from experience, apply reasoning, adjust to new inputs and to add value. It can also utilise data analytics algorithms to very quickly draw conclusions and insights from vast quantities of data which, for example, could be used by insurance companies to calculate risk premiums more accurately.

Besides the benefits mentioned above, there are risks to agility and IT delivery to be considered when designing this strategy.

- If deployment is not standardised, it could become another legacy;
- Interaction to other systems and applications will become a dependency for any change to those underlying systems (e.g., cross-functional and cross-application scripts);
- Artificial intelligence is programmed to do something beneficial, but the method it develops delivers unintended negative outcomes.

1.3.12. Agile development

Agile software development is an approach to software development under which requirements and solutions evolve through the collaborative efforts of self-organising and cross-functional teams. Other than in traditional software development, planning cycles are relatively short (usually two or three weeks) and adaptive, and teams are encouraged to respond rapidly and be flexible to changes and requirements of end users. The planning targets to quickly deliver a minimum viable product, which is then further improved through continuous development sprints.

From a risk management perspective, it is very important to consider how the second line of defence (LoD) functions such as information risk management, operational risk management and compliance should be involved in these agile developments. These functions need to be involved from an early stage and need to communicate requirements such as IT security standards or compliance standards at the start of the development. Traditional sign-off procedures for these functions, at the end of a product development cycle, are no longer an option.

The production and registration of sufficient fit-for-purpose documentation is an important attention point. The objective of software development is not the production of documentation. However, developing software without proper documentation is a recipe for disaster for later years. A reasonable balance should be found and maintained.

For further information, we refer to the ‘Agile Glossary 2016’, an open source compendium of the working definitions of agile practices enriched with experience guidelines of many agile practitioners around the global.

IoT will result in an increase in opportunities as well as complexity and risk.[12]

[12] The Internet of Things in insurance Shaping the right strategy, managing the biggest risks (EY, 2016)

2 The roles and responsibilities in operating and controlling IT environments

2.1. Introduction

In this chapter, we consider the different roles and responsibilities of staff working in the various areas of the organisation in managing and controlling information risks brought by modern complex and fast-evolving IT environments. Many different levels of a company's organisation interact to support effective IT risk management.

We will discuss in a practical way how the IT organisation, the supervisory board[13] and the management should manage and control the IT risk landscape, the supporting role of the CRO and risk function in assessing and measuring information risks, and the role of information system audit in providing independent assurance.

With increasing regulatory requirements, management boards, supervisory boards and CROs are increasingly being held to account for managing the risks within their organisation. Whilst in the past, the focus may have been more on financial and market risks, the fact remains that boards are also responsible and accountable for risk supervision of IT.

2.2. Three lines of defence model

Topics on the roles and responsibilities addressed are *'governance and oversight'*, *'policies and standards'*, *'risk culture'* and the *'Day-to-day control (management processes)'*. This document addresses the organisation of information risk management and the roles and responsibilities of each stakeholder group, against the backdrop of the well-known three lines of defence model:

- Board: sets tone at the top and establishes governance for information risk management;
- First line: business and IT management owning operational risks associated with the use of IT;
- Second line: information risk management which reports to the CRO;
- Third line: internal audit which reports independently to the management board and the supervisory board.

First line (business and IT) is responsible to assess risks to the business processes under their responsibility, determine risk response and if the risk response is decided to be mitigation by internal controls, implement these controls and test them for operational effectiveness.

Second line (CRO and information risk management) is responsible for monitoring and challenging the risk assessments, response, controls testing and risk reporting of first line management.

Within some organisations, the trend is to shift risk management responsibilities from the second to the first line, enabling faster detection and response/ recovery to incidents. The monitoring and challenging function within the IT organisation or within the chief information security officer (CISO) can be considered as a compromise model of sorts. In its purest form, the challenge function on information security is not part of CISO but is part of the information risk management function. If this was not the case, steps would need to be taken to ensure effective segregation of duties and to avoid delivery, execution, challenging and monitoring activities being done within one operational department.

Third line is responsible for providing independent assurance around the level of process controls (owned by first line) and on the effective functioning of governance and risk management. Most of the larger companies have their own independent internal audit function, centralised or decentralised or in matrix form. Also, examples exist where parts of the audit function are outsourced under management of the chief internal auditor.

In various jurisdictions, different forms of this model exist, and companies might have preferences for softer or stricter separations of tasks. The figure above shows two alternative structures, both

[13] The roles and responsibilities of supervisory board, executive board, management board and senior management can differentiate per country. In this paper, we choose supervisory board (for supervision of the management) and senior management (for day-to-day responsibilities).

1 LoD Business Unit	• Day to day risk management • Apply internal controls and risk responses • Follow a risk process
CISO	• Monitoring and challenging first line • Preparation of detailed IT security standards
2 LoD Risk and Compliance	• Oversee and challenge risk management • Provide guidance and direction • Develop risk management framework
3 LoD Internal Audit	• Review first and second lines • Provide an independent perspective and challenge the process • Objective and offer assurance

1 LoD Business Unit	• Accepts risks in business operations • Day to day risk management and control activities
2 LoD Risk	• Defines policies • Provides assurance • Control functions, like CISO • Independent risk management
3 LoD Internal Audit	• Performs tests of controls, like RCA's • Substantive procedures to detect material misstatements or test assertion levels • Provides independent challenge and assurance regarding the appropriateness and effectivenes of Internal Control Framework

of which are currently in use within large European insurers. Most national regulators appear to prefer the first (left hand side) model, but several variations exist in practice. The size, complexity, cost and other practical considerations in different companies may very well provide acceptable reasons to organise information risk management differently than the theoretical model would suggest.

No matter which model is selected, CROs should monitor that there is clarity about roles, responsibilities and accountability in both the first and second line, that this is documented well, and that clear communication exists between the different lines to prevent possible gaps and overlaps. During the implementation of the three lines of defence model, an organisation might face one or more of the following challenges:

- Has the first line truly taken IT risk ownership? Or is it the case in practice that the second line is still executing first line activities such as risk and control self-assessments and control testing;
- The allocation of sufficiently skilled resources, which are typically scarce, in every line of defence, especially related to complex cyber security related controls;
- Evidencing and documenting risk assessment, control testing and monitoring and audit activities to prove the effectiveness of three lines of defence model, for example, determining the required level of control assurance in conjunction with key stakeholders (external auditor, regulators), requires considerable resources and standard setting.

2.3. First line: the managing role of business and IT management

The operational management should emphasise the proper behaviour regarding information risk management. It should also implement information risk management processes and practices in line with the governance established by the board's senior management roles in first line.

The chief operations officer **(COO)** is responsible for the ongoing processing, including the management of IT environment, middleware and applications necessary to achieve this. Although the overall responsibility stays within the management board, the chief technology officer (CTO), chief information officer (CIO) and COO and management (business owners) can take accountability in managing the IT risks, implementing controls and in the ongoing IT hardening.

The **CTO/CIO** is, amongst others, the most senior official accountable for IT strategy, aligning IT and business strategies, planning and resourcing and managing delivery of IT services, information and the deployment of associated human resources. (definition ISACA). The CIO and CTO often reports to the COO.

The **CISO** is responsible for assessing the company information security maturity level, supporting definition and execution of action plans to reach and maintain this maturity level, setting-up and managing the local information security organisation, and defining and managing information security budgets and resources.

Examples of topics on which the management should focus are as follows:

- Employees should feel responsible for the protection, including confidentiality, availability and integrity of customer and company data;
- Take ownership of end-user computing (enriched data) within their scope;
- Feel responsible to report and investigate the vulnerabilities and incidents noted within the IT environment;
- Take ownership in ensuring proper risk governance in operations management (such as IT architecture, maintenance of IT systems, etc.) and project management of information

risk improvements (e.g., include IT and security review in all steps of project cycle, involve business management and other key relevant stakeholders in project governance, etc.), including technology disruptive projects;
- Take ownership in spreading and enforcing information risk culture across the organisation, implementation of information risk controls within the company, and ensuring it is applied by third parties.

2.4. First line: align business and IT strategy

In a world inclined towards digitalisation, an ineffective IT strategy is one of the most significant risks facing the board of any organisation. Failure to suitably align IT and business strategies, including financial control over IT business plans and investments, could lead to wasted investment and an inability to adequately support the business process raising costs and reducing responsiveness and the ability to innovate.

The IT strategy provides general direction for development and evolution of the IT landscape. The IT architecture operationalises the IT strategy in particular, regarding the IT systems that must, should or must not be used for a respective usage purpose, with minimum requirements including information security requirements and cyber resilience.

Given the prominence of cyber security, data leaks and system availability incidents during recent years, there have been growing expectations of the management boards to have greater insight in IT risks by their stakeholders including regulators, rating agencies and clients.

Responsibilities in the first line management differ between business management and IT management.

Business management
- Business management is responsible for operating business processes in line with company strategy and objectives.
- As such, it assigns business value to information assets, identifies risks to information and technology assets as they relate to achievement of business objectives (strategic and operational).
- It decides the risk response and identifies internal controls in its business processes or adopts IT controls as offered by IT management.

IT management
- IT management supports business management by establishing an organisation and technology landscape that enables business processes.
- IT risks are derived from business objectives as these are translated to IT objectives (operational and strategic).
- IT management identifies and implements internal controls based on input from the various business owners, and, in addition, identifies risks associated with the specific technologies adopted and IT organisation it has established.

Both business and IT management need to gain comfort that the controls selected and implemented operate effectively to bring risks down to within the risk appetite of the company. To this end, management will test effectiveness of key controls and report to the board when ineffective controls may cause a rise in risk profile up to or exceeding the risk appetite.

2.5. Second line: the role of risk management

The role of the CRO and the second line of defence, represented by the information risk management team within the risk management function reporting to the CRO, is crucial in assessing and measuring the information risks.

> Although the overall responsibility for risk culture lies with the senior management, the CRO is usually a major carrier and ambassador of this culture.

The CRO community is expected to provide risk culture trainings, to set clear guidelines around the risk culture and to measure and assess the quality of the risk culture. The CRO should oversee the different departments of quality and review the risk framework. Although overall accountability stays within the first line management, the CRO should feel the responsibility of reporting that risks are managed in a consistent and effective way. This requires a holistic approach and integral control of all the relevant information risks by high quality information risk management policies and processes.

Setting the risk appetite itself is not enough. Also, systems to measure or even timely forecast actual exposures and levels need to be put in place, allowing for timely actions to stay within approved risk appetite.

The CRO department is expected to develop an annual review of the IT-related policy, standards and guidelines to check that those documents adequately address the company risks.

The CRO should also provide an opinion to the management board and the supervisory board on the quality of reporting of the first line to (IT) risk committee on IT and cyber security posture, and more globally to report on risk exposure to the management and board to support decision-making processes. A key question addressed by one of the CIOs of an insurance company was, if with the increasing complex (use of) IT, we have sufficient skills within the risk function that can perform a critical advisory and monitoring role. In other words, is the risk department capable of performing risk processes diligently based on a credible understanding of the underlying IT risks.

The risk function's main tasks will typically be to monitor first line´s control activities and the effectiveness thereof, and to develop an escalation and waiver process. An internal control standard for identification, protection, detection, response and recovery should be designed and maintained, or at least supervised, by information risk management. The information risk function should evaluate if the appropriate level of a mix of preventive, detective and corrective controls are implemented and should escalate where it is not the case. Topics like the IT risk scenario analysis, collect loss and incident data and perform analysis, develop and implement system of key risk indicators, challenge and evaluate specific IT critical projects and functions should be taken into account.

The information risk management function should ideally report directly to the CRO in line with the risk strategy. A specific dashboard should ideally be defined[14] for the follow-up of information risks among the company, and define key risk indicators that should be provided by the first LoD, and to enable the CRO to have a global view of the evolution of information risks among the company. This dashboard and report should be presented to the risk committee or a similar body for information and decision purposes. Therefore, this dashboard and report could be presented to the management board and the supervisory board.

> The CRO is responsible for developing a specific risk appetite framework, including defined tolerances for information risks, and to make explicit to what extent the IT strategy sufficiently addresses IT risks and cyber risks in particular.

[14] Insurance companies have different implementations and setups in their three lines of defense. Examples with more responsibilities shifted to the first line on drafting the risk reporting with limited second line role on review and endorsement.

2.6. Third line: the role of audit

The internal audit department should provide knowledge and skills of the information systems auditing (IS-audit) to deliver an independent assessment of all information risk management related topics. Information system audit should provide assurance that, amongst other topics:

a) the long-term IT strategy is aligned with and supporting the business strategy. To this end, the IT strategy needs to be worked out in a clear vision or roadmap for the IT infrastructure developments in coming years;
b) the short-term IT implementation plans are feasible;
c) the IS security policy is appropriate and correctly implemented;
d) the outsourcing and insourcing of IT services is also a key topic to address in the independent assurance of the audit. Point of attention is to contractually arrange the right to audit. Often, vendors provide ISAE/SOC statements that do not cover the right scope of outsourced activities, or are conducted with insufficient quality of testing of controls.

An independent opinion can also be expected on the IT systems maintenance processes, IT infrastructure, IT lifecycle management and the users' access controls. Specific deep dives on the operating system controls, application systems controls, software development lifecycle management, change management, incident management, database controls, network management and cyber security measures could reasonably be expected as well.

Often, internal auditors work in close cooperation with the external auditors, for example, regarding testing design and effectiveness of IT general controls relevant for the financial reporting processes. Such close cooperation is necessary to prevent that external auditors have to reperform all the test work already performed by first and second lines.

"Condition for an effective function is that the IS-audit must work independently and in accordance with appropriate audit standards and professional practices (e.g., Institute of Internal Audit (IIA)[15] or Information Systems Audit and Control Association (ISACA)[16] ."

Having said this, it is equally important that information risk management and IS-audit align on the use of one common taxonomy, use of one company wide accepted system for allocation of materiality and risk rating, and that both focus on optimising the effectiveness of audit and risk recommendations by using one system for issue tracking and overdue reporting. Both functions work independently, but they act within the same company and ultimately with the same purpose.

The IT audit strategy is focused on assessing whether the entities' combination of internal controls, governance and risk management effectively safeguards the confidentiality, integrity, availability, authenticity of data and the agility/delivery of IT (CIA-AD), regardless of whether the process are performed internally or outsourced.

A well-planned, well-communicated, well-managed and properly structured IS audit program is essential to provide an independent, traceable and repeatable audit process that delivers high quality audit reports in a timely and controlled matter.

Specialisation within the information system audit will also be required, due to the wide range of knowledge needed to provide the relevant assurance.

2.7. The governing role of senior management

As for many other topics, the tone regarding information risk management and information risks, is at the top. It is therefore necessary that the supervisory board and senior management is considered accountable for the propagation of a proper and solid risk culture among the company. The governance establishing the foundations for a three-level defence model is established at board level. First and second line report to the senior management, while the third line reports to the supervisory board to maintain independence.

The IT governance is a cornerstone to build a sound, controlled but also ethical operational management. Good IT governance is required to protect stakeholders' interests and rights of shareholders, creditors, policyholders and other interested parties.

Senior management is accountable for establishing the IT governance. The IT governance encompasses organisational structure, determination of IT objectives, policies, standards and guidelines that provide direction, as well as the means to measure, monitor and manage risks on day-to-day basis.

[15] For more information, refer to https://na.theiia.org/.

[16] For more information, refer to https://www.isaca.org/.

Senior management should clearly communicate to the rest of the IT organisation how important information risk management is. They are expected to consult regularly with information risk management departments and show appreciation for the independent and critical attitude of the function. This tone at the top is extremely important, and if voiced well, it can strongly support the information risk management functions, but if not voiced at all or in the wrong way, it may undermine the effectiveness of the function.

Senior management sets the conditions by which the key players (usually the C-level officers) are bound and decides on the reporting lines. Furthermore, senior management approves risk appetite and tolerance for IT-related risks and is ultimately responsible for the implementation of an effective information risk framework. Also, senior management needs to consider how tasks and responsibilities around control monitoring, testing and reporting are divided within the applicable three lines of defence model. It might be helpful to have clear responsible, accountable, consulted and informed RACI tables or a control monitoring and testing standard in place to univocally clarify the governance on this topic.

Most organisations have a board-level risk committee involving senior executives normally chaired by the CRO and this may cover IT risk as a standing agenda item. Others may create a sub-committee just for IT and/or information security to facilitate greater oversight of IT and IT security risks due to their inherent complexity and the need for closer interaction with IT and security subject matter experts (SMEs).

Senior management may delegate the decisions to grant waivers of group policies to the CRO. For new policies, a 'grace period' of 'soft launch' is commonly used to allow the relevant organisation to implement the requirements, after that moment for deviations of the policies, a waiver is needed.

The waiver process should set limited timelines to become compliant with the group policies, should pay attention to temporary mitigating measures and should appoint persons to act (PTA). Overviews of all the granted and still valid waivers should be reported to the management periodically.

Senior management will often delegate preparation of details following from their accountability to a **non-financial risk committee** or a **more dedicated information risk committee**. The risk management function's responsibilities in this committee are as follows:

- Develop the IT risk framework;
- Prepare associated policies and standards;
- Prepare the risk appetite of the company;
- Define the tolerance level of the company regarding IT risks;
- Review the results of the company's information risk profile;
- Take decision on any major deviation with the risk appetite framework.

This committee should at least be composed of a combination of senior leadership functions spanning first and second line, which could include a COO, a CISO, a CTO, a CIO, a CRO and other relevant stakeholders such as chief compliance and data privacy officer, chief internal audit officer, etc. In addition to providing oversight, dedicated committees also send a strong and positive message to stakeholders that the organisation considers these subjects of high priority.

All of the activities described above should result in the management having a clear understanding of the information risks and how they are controlled in the organisation. CROs play a pivotal role in achieving this important objective.

Key considerations for the senior management on governance include:

- Consistency between corporate strategy and IT strategy that supports the requirements of the business;
- Overseeing of critical information risks, incl. cyber security risks and their positioning with respect to company risk appetite;
- Understanding of key trends and regulatory requirements for IT;
- Reviewing and approving adequate budgets for development and implementation of protection objectives and measures, including IT security;
- Defining appropriate quantitative or qualitative criteria (KPIs/KRIs) for managing the further development of IT systems;
- Monitoring and evaluation of all significant investments and expenditure in IT;
- Effectiveness of data governance activities — those activities that maintain availability, usability, integrity and confidentiality of data used in the organisation;
- Cyber incident response, and IT resilience and continuity planning;
- Major risks posed by external service providers (ESPs).

The risk committee(s) should form part of the overall governance framework that provides the senior management and the supervisory board with oversight and transparency of IT (and associated information/cyber security) risks.

In many organisations, another aspect of the governance framework is the internationally recognised three lines of defence (3-LoD) model which provides a structured approach to information risk management (see section 2.2).

Risk policies and standards, prepared by the risk committee and approved by the management board, provide the expectations towards information risk management processes to be executed by the company.

3 IT risk framework

3.1. Introduction

This chapter describes the importance of selecting the right ('fit for purpose') IT risk framework, based on the strategy and covering the complexity of the IT environment and the regulatory requirements. The chapter studies different frameworks commonly used in IT, describes the main purpose, focus, main advantages and disadvantages of each framework.

3.2. Information risk management processes, and techniques

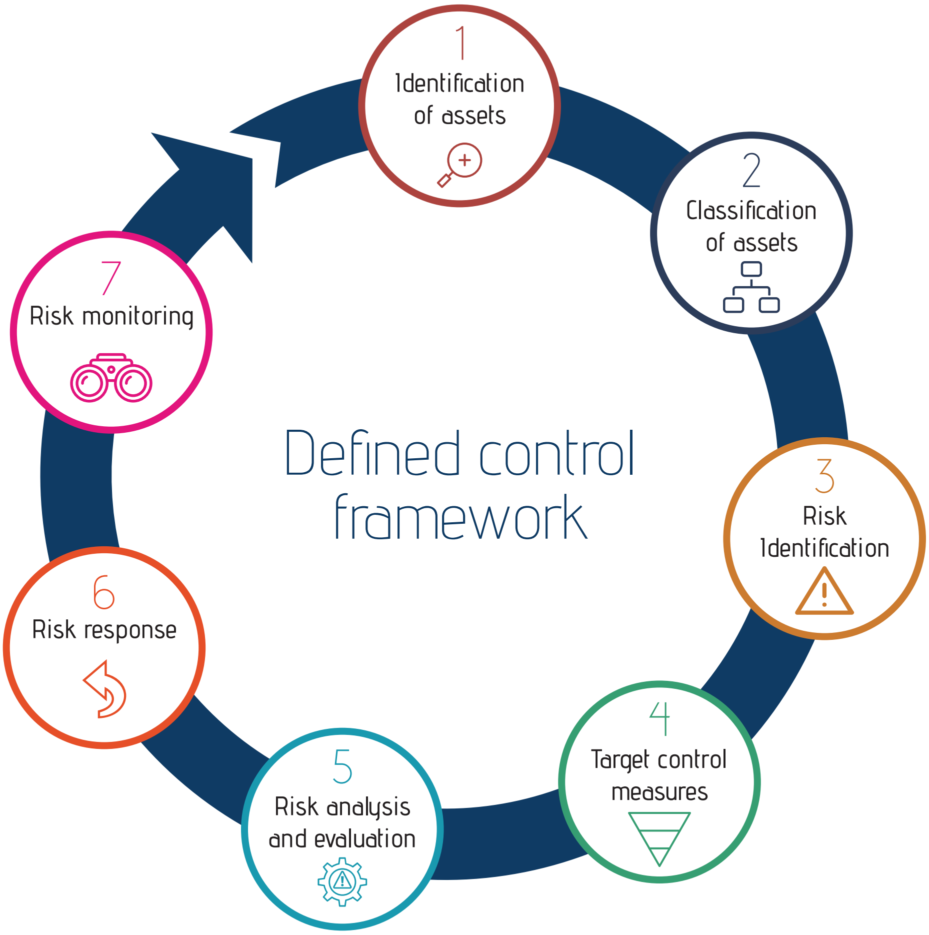
3.2.1. General principles of an information risk management system

Information risk management can have different approaches, based on controls, events, or assets. Since the digital landscape to be assessed is an interconnected system, the approach chosen to assess IT risks, is very important and will partly rely on a correct and complete asset inventory in order to develop an end-to-end analysis for the risks arising.

3.2.2. Information risk management process

Traditionally, the Information risk management process is composed of four relatively standard risk management components:

- Risk identification;
- Risk analysis and evaluation;
- Risk steering;
- Risk monitoring.



Increasingly, it is recognised, that in order to have an efficient and effective information risk management process, there need to be two additional steps:

- Identification of assets based on the abovementioned asset inventory;
- Classification of assets.

1 Identification of assets

The initial step is for organisations to identify relevant information assets. Once identified, appropriate details such as asset type, owner, location etc. should be entered into an appropriate asset register. In many legislations, such registers are a mandatory requirement of the regulators. Often, more specific registers are mandatory as well such as a cloud sourcing register, or an outsourcing register.

It is important to note that processes need to be established to maintain an up-to-date asset register and to make sure the regulators have access to these registers.
If possible, without the loss of any information, it may be more useful to focus on information asset categories (groups of assets) instead of single information assets. This approach seems to be adequate because protection demands and security measures often refer to information asset categories.

Typical information related assets	Result of this sub-step
• Information in all its forms • IT-relevant processes • Projects to implement IT systems and services • Software and application systems • IT hardware and equipment • Building and network infrastructure • IT services including services provided by suppliers such as outsourcing • IT organisational units including staff, and their qualifications, skills, and experience	All information-related assets have been identified on a sufficient level of details

2 Classification of assets

The second step is to classify the identified assets. This can be achieved by, for example, using a business impact assessment (BIA) process[17].

In this sub-step, the impact of a potential loss of **confidentiality**, **integrity**, **availability** and **delivery (CIA-AD)**, and in addition, **authenticity**[18] (CIA-AD)[19] explain difference CIAA with AGILITY is assessed and a **Criticality** Level is determined. This is typically done using an impact scale matrix (see example below) with, for example, the below mentioned predefined categories and three impact scales (low, medium, high).

Typical BIA process	Result of this sub-step
The typical BIA process consists of a number of questions that need to be answered. For example, how would a loss of CIA-AD impact the organisation's objectives with respect to predefined categories? Examples of predefined categories would be: • Competitive disadvantage; • Direct financial impact; • Loss of business; • Legal and regulatory liability • Staff morale; • Management decisions; • Business disruption; • Reputation.	Four impact scale matrices / impact level for CIA-D that determine the protection demand of each identified asset category; if one of the five perspectives (CIA-AD) is the primary business perspective, the remaining perspectives do not have to be considered if a low criticality is evident. Note: Within the BIA, only the gross impact of events is assessed, not the likelihood of occurrence. The likelihood is considered within the risk analysis and evaluation phase.

[17] BSI 100-4 Business Continutiy Management (2009): p.35 ff
[18] Authentication is newly required by VAIT (supervisory requirements in insurance undertakings, prepared by BaFIN, the German supervisory authority)
[19] See Appendix with Definitions

3
Risk identification

The objective of risk identification is to understand what is at risk within the context of the critical information assets and to generate a comprehensive register of risks based on the threats and vulnerabilities identified. A distinction can be made between inherent risk level (without any control) and residual risk level (taking the effect of controls in account).

Risk identification process	Result of this sub-step
When an organisation seeks to identify risks, it needs to consider a number of key elements including, but not limited to,: • the types of threats it faces, for example, is the organisation a potential target for state sponsored attacks; • potential vulnerabilities based on threats and existing controls; • the robustness and maturity of its control environment if focussing on net risks; • its technology landscape. Changes in threat situation need to be monitored and factored in as required.	Following this step, there should be an updated risk register.

4
Target control measures

It may be helpful to develop a central information security standard (documentation of target measures/ minimum protection requirements) for predefined protection groups depending on the criticality (low, medium, high for any of the CIA-D protection goals) of the information asset categories. This information security standard ensures a standardised and consistent approach when implementing mitigation measures.

Types of control measures	Result of this sub-step
Control measures for IT can be either: • **Preventative** — are intended to prevent an incident from occurring; • **Detective** — are intended to identify and characterise an incident in progress; • **Responsive** — are intended to limit the extent of any damage caused by the incident. In an IT environment, these controls can cover: • Physical security; • Technical security; • Administration; • Procedures; • Process.	An organisation specifies a set of risk mitigation measures, controls, safeguards, procedures etc. to avoid, detect, counteract, or minimise IT risks to information, systems, applications and other related assets.

5 Risk analysis and evaluation

Risk analysis and evaluation is used to determine the likelihood (probability) of the given risk development and the severity (impact) on the organisation if it was to occur. The risk analysis and evaluation process focuses on the residual risk position, i.e. after consideration of the current control environment in place.

Depending on the present situation in a company as well as the status of information risk management, it has to be decided whether to consider the inherent risks at the first stage (risks without consideration of already implemented protection measures) or to consider the net risks directly.

Risk identification process	Result of this sub-step
The risk analysis process consists of a number of steps: i. Identify the likelihood of occurrence for all identified risks per asset category and determine the gross risk or, directly, the net risk (integration of step ii); ii. Analyse the existing protection measures and controls that are already in place for the considered asset categories and apply their status to the gross risk estimation (present net risk); iii. Compare these protection measures/present net risk with the applicable protection requirements and identify existing threats and vulnerabilities (gap analysis); iv. Estimate the remaining risks. These risks are the deviation of the present net risk to the targeted net risk (result of gap analysis); v. Approval and sign-off. The results have to be approved by the management; vi. Review of risks. On a regular basis, the results have to be reviewed and possibly updated.	A view of the present net risk as well as the deviation to the targeted net risk for all the asset categories.

6 Risk response

Risk response, also called risk steering or risk management, refers to the decisions about how the present net risk is to be managed to an acceptable level (targeted net risk). The main question will be to understand whether the risks are within or outside the agreed risk appetite.

Treatment options	Result of this sub-step
Typically, there are four potential responses to a risk: • **Treat** — implement mitigating actions based on the (adjustment of) abovementioned target requirements/ information security standard to reduce probability or occurrence and/or severity of the impact; • **Tolerate** — formally acknowledge and accept the risk (should only be done if the risk is within tolerance and the relevant risk appetite); • **Terminate** — stop the activity, process etc. that give rise to the risk; • **Transfer** — this can be done, for example, through corporate risk insurance (including self-insurance or specific cybercrime policies). When selecting the most appropriate response or a mixture of adequate responses for a given risk, the cost-benefit aspects need to be taken into consideration.	Approved and implemented risk mitigation/protection/formal acceptance.

7
Risk monitoring

Once a risk assessment has been undertaken, the risk monitoring phase is essential to track the risks over time.

Monitoring process	Result of this sub-step
The purpose of the risk monitoring process is to: • ensure that any identified mitigating actions are being implemented, as planned by adding control testing measures; • periodically reassess the risks to make the existing net risk transparent; • to escalate any issues or delays in mitigating the risks.	All risks and risk treatments are reviewed and updated, and where required, appropriate escalations are made.

Note: The following **risk approaches** and/or a mixed approach are possible to have an effect on the risk. While risk treatment/risk prevention is a proactive measure, contingency is a reactive activity to be prepared for a risk that occurred, in order to minimise the potential impact. The definition and set up of contingency measures should consider and be dependent on the potential impact, the range and the probability of occurrence of the risk. Reactive measures may be helpful if proactive measures are inefficient or there is a bad cost-benefit ratio. Contingency measures may include discovery, response and recovery sub-processes.

Contingency measures can be activities that are reactions to a risk that occurred in order to minimise and manage the impact, such as shorten the period of disruption and defined communication, or also activities to bring back the risk asset such as the organisation or a system back to regular operations. The definition of contingency measures in the context of information risk management just has a descriptive nature and has the function of an indicator whether there is a need for action to initiate such measure or not. The basic management and the operational execution is handled within the IT service continuity management.

The required steps for risk response are listed below.

1. Identify potential measures to close the gaps
2. Decide on the risk approach (treat; tolerate; terminate; transfer)
3. Based on the selected risk approach, develop detailed protection measures and estimate costs
4. Agree with all the relevant stakeholders
5. Estimate updated net residual risk
6. Document and approve
7. Implement the protection concept
8. Review

3.3. Risk appetite

The global financial crisis placed risk appetite and risk management in the spotlight as a developing concept for many insurance companies. In December 2013, the CRO Council and the CRO Forum published the paper ***'Establishing and Embedding Risk Appetite: Practitioners' View'***, to present a variety of sound practices that organisations use to establish and embed effective risk appetite frameworks. At the highest level, a strong risk appetite framework is a core tool for performance management that helps bring discipline to major strategy decisions; but when cascaded down through an organisation, it also encourages them to be more resilient and make better investment decisions by balancing potential returns with the associated risks. Regulators, particularly those across Europe, have also taken an interest in risk appetite because of the intrinsic link to good corporate governance, behaviour and risk culture, as well as setting expectations on organisations to define specific risk appetite statements for operational risk themes including IT. In addition, external stakeholders, including rating agencies and shareholders, are increasingly seeking clear risk appetite statements from the organisations that they assess or are invested in.

3.3.1. Definition

There is no universally accepted definition of risk appetite; listed below are a number of examples.

"A company's risk appetite establishes boundaries for the aggregate level or types of risk a company is willing to assume in order to achieve its business objectives."
[Source: CRO Forum: Establishing and Embedding Risk Appetite: Practitioners' View];

"The degree of risk, on a broad-based level, that a company or other entity is willing to accept in pursuit of its goals".
[Source: COSO Model for Enterprise Risk Management];

"Amount and type of risk an organisation is prepared to pursue or take"
[Source: British Standard 31100].

In principle, the purpose of risk appetite statements is to:

- define risk preferences, limits and appetite for the relevant risk types, and how they relate to the company's risk management requirements;
- articulate the amount of risk the organisation is willing to take to deliver its strategy.

3.3.2. Risk appetite in an IT risk context

Organisations are increasingly reliant on information technology (IT) requiring a robust, resilient and agile infrastructure that meets the needs and demands of its workforce and customers. To this end, there is increasing pressure and focus on IT organisations to ensure risks relating to their IT environment are appropriately identified and managed. It is also essential that CROs do not view IT risk in isolation. It needs to be compared with other risks so that investment in IT risk prevention and mitigation can be considered simultaneously with other enterprise risks.

Overall, it is the company board which is expected to oversee the enterprise-wide information risk management strategy, including an appropriately set appetite, and to define the risk the organisation is willing to assume within its risk capacity. It must also validate that information risk management strategies and IT risk appetites have been cascaded throughout the enterprise.

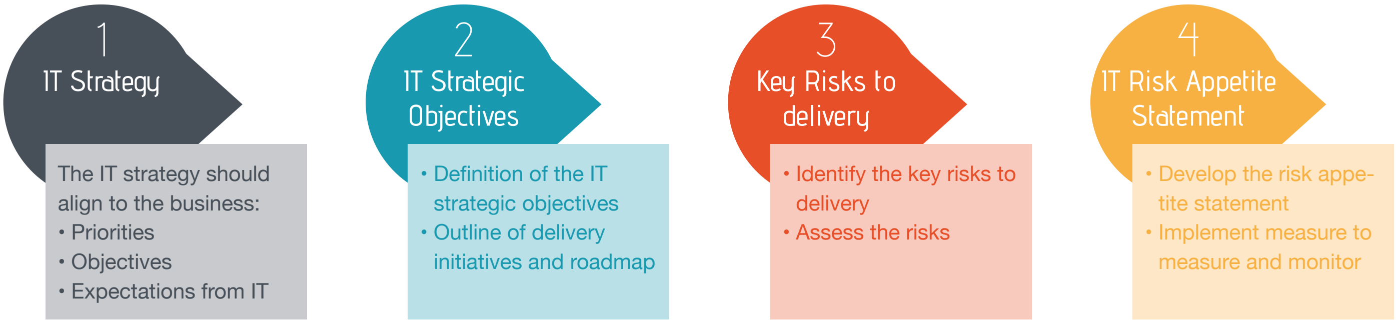
Generally speaking, an organisation's IT risk appetite is a subset of its operational risk appetite and its overall enterprise risk appetite, therefore it must not be developed in isolation. The IT organisation can define and document the relevant key IT risk themes, the associated risk appetite statements and risk tolerances and communicate these to the business leaders, but ultimately it is the responsibility of the board to define the overall risk appetite.

In reality, explicit quantified statements of IT risk appetite rarely exist, and what are generally in place are relatively high-level and qualitative in nature. IT-related-risk decisions on whether to accept or mitigate a risk are often based on judgment and on what resource and budget are available for a particular situation. Some examples of risk appetite statements are provided in the table below.

Risk type	Appetite	Tolerance
Security of data	The company will not accept a risk that potentially compromises the security of confidential data. All such risks must be managed.	Very low tolerance
Continuity of business	Risks that expose critical processes to downtimes and/or recovery times greater than those defined by the business are not acceptable. All such risks must be managed.	Moderate tolerance
Legal and regulatory	Material breach of laws/regulations relating to the protection of personal data is not acceptable.	No tolerance

3.3.3. Setting an IT risk appetite

The diagram below shows a simple four-step process to establish an IT risk appetite.



1
IT Strategy

The IT strategy should align to the business:
- Priorities
- Objectives
- Expectations from IT

2
IT Strategic Objectives

- Definition of the IT strategic objectives
- Outline of delivery initiatives and roadmap

3
Key Risks to delivery

- Identify the key risks to delivery
- Assess the risks

4
IT Risk Appetite Statement

- Develop the risk appetite statement
- Implement measure to measure and monitor

1. **IT strategy:** The starting point should be an understanding of the IT strategy of the organisation and the priorities and objectives that have been established, as well as the business expectations of IT beyond the strategy.
2. **IT strategic objectives:** Once the strategy is established, IT, like any other business function, will establish a set of delivery objectives and plans. Common objectives relate to level of automation, integration, stimulating mobility, reducing risks in business processes, timeliness and reliability of information, processing time for transactions, requirements for foundational infrastructure, prevention of unauthorised access, loss or change of information, service quality, business continuity or maximum downtimes, effectiveness of IT controls, and stimulation of IT innovation.
3. **Key risks to delivery:** The next step would be to complete a risk review to identify the key risks to delivery of the strategy, objectives, and how to assess them.
4. **IT risk appetite statement:** The risk appetite statement is then developed by reviewing the risk assessment and determining what level of risk can be accepted in pursuit of the objectives. Often target levels, thresholds and hard limits are set.

3.3.4. Benefits of an IT risk appetite statement

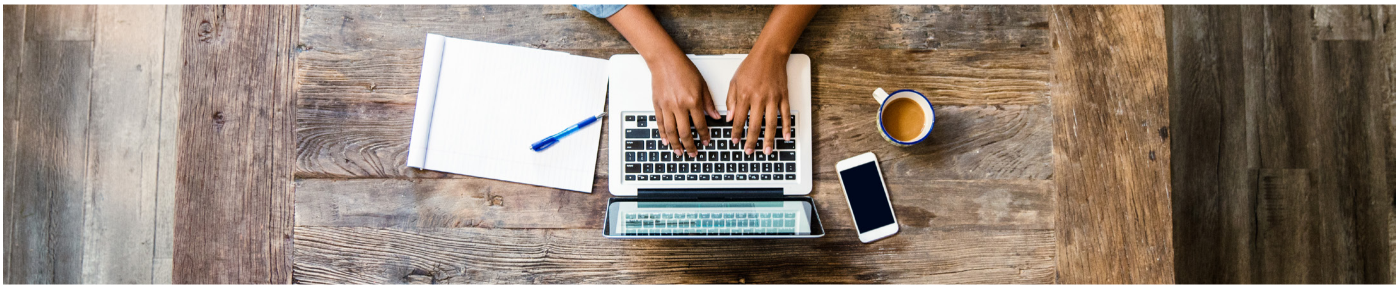
A well-defined and comprehensive IT risk appetite statement has a number of intrinsic benefits that include:

1. Support of conscious and informed risk taking by defining how much IT-related risk the organisation is willing to accept;
2. Provision of a decision-making framework that communicates explicitly what is acceptable so managers can take ownership and accountability for their choices without having to refer all the decisions to senior management for approval;
3. Increased transparency by enabling a better understanding of the organisation's position on IT risk;
4. Better identification of opportunities for further risk taking or identify areas where unacceptable risk taking is occurring;
5. Enable a more structured conversation on IT risk between IT managers, senior executives and the board.

3.3.5. Challenges in implementing IT risk appetite

There are a number of challenges faced during implementation of an appropriate risk appetite statement for IT. These include:

1. **Complexity:** IT environments, by nature, are complex, inter-linked environments. Any risk appetite framework for IT has to take account of these complexities. Creating a simple high-level risk appetite framework, whilst attractive at one level, will lead to an ineffective, superficial view of IT risks that adds little value.
2. **Language:** IT risk appetite statements must be written in a language that the business understands, filling them with technical jargons and three-letter acronyms will leave senior managers with little insight or value.
3. **Setting and monitoring limits:** Another challenge is in setting, measuring and enforcing risk appetite limits and reacting to breaches.



3.4. Key risk indicators

In order to be relevant and support an organisation's decision making processes, an IT risk appetite statement should ideally be measurable in order to understand how IT performance drivers are impacted by risk.

KRIs are metrics that provide insights and early-warning signals of increasing risk exposure on the identified risks. The design and rollout of KRIs should be an important element of any organisation's enterprise risk management (ERM) framework and should cover all risk types and themes across the organisation.

At the basic level, KRIs are just key ratios that senior management monitors as indicators of evolving issues with the achievement of objectives and are used to identify areas where mitigating actions need to be taken. Mature organisations may have a more complex KRI structure involving aggregation of a number of risk indicators into a compound risk score, relating to overall risk exposures for given risks.

3.4.1. Process for establishing KRIs

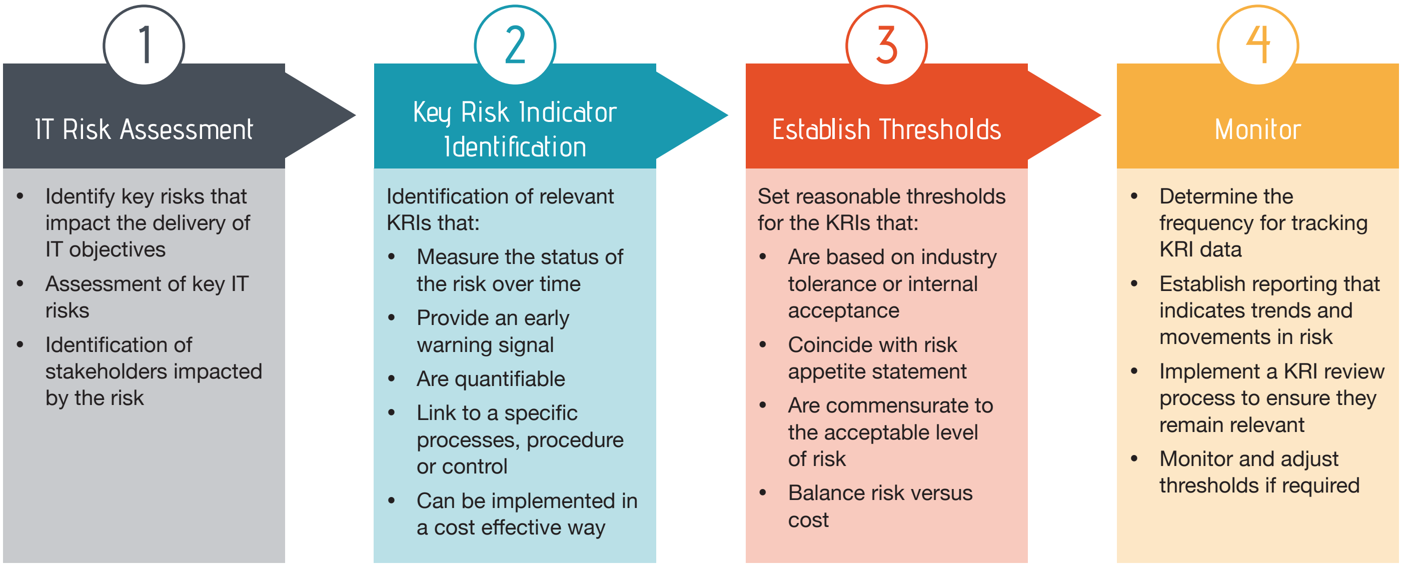
The diagram below shows a simple four-step process for establishing KRIs.

1. **IT risk assessment:** The first process is to identify the key risks relating to the implementation of the IT strategy and the related strategic objectives and roadmaps. The IT risk assessment should encompass the full gamut of IT-related risks including cyber security, IT resilience and continuity, technology vendor and third-party risk, data management, operational delivery change management and projects.
2. **Key risk indicators:** Once the risks have been identified, the next step is to identify an appropriate set of metrics. These need to be measurable, meaningful, a good mix of leading (predictive), and lagging (historical) indicators to support effective risk management. It is possible that a single KRI could be applicable for a number of different risk scenarios.
3. **Establish thresholds:** KRIs need to have appropriate threshold levels set, which, if not attained, can trigger the implementation of timely mitigating actions to prevent a given risk from breaching the defined appetite.
4. **Monitor:** The final step is to determine the frequency for tracking KRI data and establish simple reporting that indicates trends and movements in risk. There also needs to be a KRI review process and frequency established to ensure KRIs and their associated thresholds remain relevant.

3.4.2. Challenges in establishing appropriate KRIs

There are a number of challenges faced in designing a set of KRIs to support information risk management. These include:

1. **Defining KRIs:** One of the main issues is identifying KRIs that are appropriate to the risks and provide the right monitoring capability. Utilising IT SMEs to support and review KRI definition will support the successful selection and implementation. Such experts will understand some of the technical constraints that may be applicable in the environment and will have background knowledge on the root causes of past events or inherent weaknesses within the IT environment or the supporting processes.
2. **Selecting the right number of KRIs:** There is no best practice for the number of KRIs that need to be adopted for a given risk. However, in order to ensure a level of consistency and clarity around the status of a given risk, it is essential to keep the number of KRIs being monitored to a manageable number. Often, KRI dashboards are implemented. The key success factor for such dashboards is not to overengineer or overcomplicate them. For example, while driving a car, one does not need 20 metres on the dashboard, although the motor management system collects thousands of different data.



- Identify key risks that impact the delivery of IT objectives
- Assessment of key IT risks
- Identification of stakeholders impacted by the risk

Identification of relevant KRIs that:

- Measure the status of the risk over time
- Provide an early warning signal
- Are quantifiable
- Link to a specific processes, procedure or control
- Can be implemented in a cost effective way

Set reasonable thresholds for the KRIs that:

- Are based on industry tolerance or internal acceptance
- Coincide with risk appetite statement
- Are commensurate to the acceptable level of risk
- Balance risk versus cost

- Determine the frequency for tracking KRI data
- Establish reporting that indicates trends and movements in risk
- Implement a KRI review process to ensure they remain relevant
- Monitor and adjust thresholds if required

Fine-tuning the available dashboards to the information need is key. For example, a board member needs dashboards more than a person monitoring the enterprise websites.

3. To this end, it is necessary to select a few that best reflect IT management's collective understanding of the key causes of each potential risk. Given the potential, multiple sources of data points for IT KRIs, the objective should be to develop a high-quality set of KRIs, rather than focusing on quantity.
4. **KRI data:** The effectiveness of a given KRI at measuring changes in the risk profile will be highly dependent on the quality of the data used to track a specific risk and the ease at which this data can be obtained. The ability to automate the collection of KRI data will go a long way in ensuring KRIs are a value-adding process and not another compliance burden.

3.4.3. KRIs examples

A number of KRI examples from member organisations are shown in the table below (a wider set of example controls and KRIs are shown in Appendix 2).

3.5. IT risk reporting and monitoring

To ensure an effective and comprehensive monitoring on IT risks, CROs play a primary role in supporting an end-to-end approach from business to IT departments and internal and external providers involved, as normally the scattered IT landscape leads to fragmented approach to IT risks. A lot of different reporting on IT topics gets done, for example on IT losses, IT incidents, IT risk scenario analysis, control assessments, with the risk that all these different reports confuse executive management on the real IT risk exposure of the company. The opposite of information overload could be the risk that with all the scattered reporting, still important risk areas are not covered and fall between the cracks.

In its role of challenging the first line of defence, information risk management will be a facilitator to bring a coherent picture on digital risks to the stakeholders involved in IT strategy design, considering all the different views that are normally available.

3.5.1. IT risk monitoring

Risk monitoring is an ongoing activity in charge of all the lines of defence and includes the control of IT projects and initiatives, monitoring of risk level through specific risk indicators (KRIs), internal control systems and progress of risk mitigations.

1. **Monitoring should start from the beginning,** in the design phase of major IT projects and initiatives, in order to avoid that projects can start without digital risks formally evaluated, accepted or managed. So for new projects, business and IT department or IT provider should work together in order to jointly perform a risk assessment on data impacted, integrated by technical and security risk assessment. Information risk management function should be continuously involved to ensure the methodology applied is coherent with IT risk framework chosen and to give an independent view on the assessment.
2. **Information risk management performs a second line of defence monitoring activity,** defining KRIs

Key Name	Key Risk Indicator
Endpoint protection	% of endpoints without hard drives encrypted
Access Management	% of leavers without corresponding disabled accounts
Unsupported systems	% Systems not upgraded to a supported software version
Risk management	% Risk with overdue mitigating actions
Third-party contracts	% of contracts without appropriate security clauses

for any major risk identified. To keep it simple, KRIs can use indicators already collected by IT department, setting specific thresholds of alert to identify new risks or risk severity changes (e.g., IT incidents, number of applications not governed by IAM solutions). Associating KRIs to the risk events identified allow information risk management to monitor how the risk severity level is changing the risk profile of the company, including the residual risk once the risk response actions are applied. Alerts on IT KRIs should also lead to escalation process to relevant committees.

3. Monitoring IT risk should leverage on internal control activities, in order to assess the risk level because of a combination between the risk exposure and the control adequacy assessment. Different approaches can be used when considering the control evaluation, to assess the residual risks after controls, or directly the real, and not theoretical, risk exposure.
4. **Another tool for information risk management is the monitoring of risk mitigation actions:** Information risk management should promptly intervene in case of significant changes or delays in mitigation action implementation. In particular, it should be considered during any delay causes that implies an arising/increasing severity of risk, consequently determining the need of escalation or corrections of mitigation actions.
5. **The information risk management department has some kind of issue overdue reporting to the Boards,** indicating relevant IT risk, where mitigating actions take longer than foreseen. It is common to have some kind of risk reporting system, capturing processes, risks, controls, issues, incidents, mitigating actions, persons-to-act and deadlines for mitigation.
6. Better practice is that **these risk reporting systems cover issues indicated by the business units and corporate staff departments** such as corporate audit, compliance, legal and risk, **but also issues from external sources** such as the management letter of the external auditor and reports from the regulators.

In this context, information risk management periodically aligns with IT, information security functions and control functions to ensure all are appropriately informed in the event of relevant IT incidents, audit findings or compliance issues.

3.5.2. IT risk reporting

Sharing of information on information risk management activities enables stakeholders to take the appropriate business decisions according to IT risks that could affect the company. In addition, good standards of information risk management reporting help to give confidence that the company is resilient and is more likely to be successful in the short and long term.

Risk reporting should be an activity completely in charge of risk management, and even if some activities are partially performed by the first line, the related deliverables shall be understood, challenged and presented to all applicable risk committees by risk management.

Familiarising executive management and Board of Directors (BoD) members to have a risk-based view, - as-well for IT, will help the first line when presenting a new initiative that requires budget and investment. Associating a risk level to the planned IT strategy can clearly show how the residual risk is changing in time or will change after the new initiatives are carried out. For BoD members and executive committees, investing in higher quality of reporting means avoiding bureaucracy in risk management and improving the decision-making process in a consistent way with risk profile and appetite.

Reporting can be performed at different levels to meet the awareness and requirements of the stakeholders and ensure a correct risk management.
IT risk can be shared at the following levels:

1. **IT risk responsibilities are often split among several actors and legal entities (LEs), including internal and external providers:** In this complex situation, sharing risk information ensures the overall end-to-end awareness of the linked risk impacts, so the involved LEs can speed up the identification of the risk response increasing the awareness at all levels and facilitating decision making. Sharing information between business, application and infrastructure providers can be done by exchanging specific risk reports, or continuous and regular alignment meetings. Internal providers often use in-control statements informing the users of levels of controls and deficiencies, while for external providers, often an ISO 27001 or an ISAE 3402 statement of an external auditor is used.
   For this reason, it is necessary to have a common and aligned approach to IT risk within the group, with aligned methodologies, scales and thresholds. In this way, business legal entities or business units get awareness on the problem and can allocate budget to solve it, by also authorising the needed downtime to complete IT activities.

2. **IT risks should be regularly shared with control functions** and security functions that have a privileged view on IT topics and can integrate the risk analysis.

3.5.3. Risk report

Despite the number of different sources available, reporting on IT risks should be done considering all current available information in order to provide a complete, consistent and integrated view on the risk profile of the company, and to let the senior management or BoD rely on unambiguous information.
For this reason, reporting should consider, at least:

- Collected losses deriving from IT events, for example, costs deriving from a security incident;
- Specific IT risk events collected and mapped on IT assets or IT processes, for example, risk of sanctions for under-licensed products, risks related to a planned hardware/software migration;
- Actual status of risk response, for example, implementation status of a specific IT solution;
- Scenario analysis on IT risk events, for example, detailed risk analysis;
- IT control assessments and any other assessment activity on the internal control system like external certifications, for example, ISO 27001[20] or ISAE 3402[21] statement;
- Any IT initiatives that can potentially move the risk profile of the company, for example, an IT project that adds additional processes and controls on cyber.

According to COBIT 5 for risks, the main goals of the risk report are:

- **Accuracy:** the report should accurately define the information risk management capabilities and actual status and trends with regard to risk, in such a way that it does not arouse confusion.
- **Objectivity:** the report information is based on the enterprise's risk culture and confirmed by observation.
- **Reputation:** the report source information is collected from competent and recognised sources.
- **Relevancy:** the report is tailored according to the requirements of the target audience.
- **Completeness:** the report covers the end-to-end enterprise structure as well as external stakeholders.
- **Currency:** the report is typically not older than one year because it should be kept up to date.
- **Amount of information:** the report should contain an appropriate amount of information, based on the requirements of the recipients.
- **Consistent representation:** the report shall always be presented according to the predefined format.
- **Interpretability:** the report should be understandable for target audience.
- **Availability:** the report should be available at required frequency to the stakeholders.
- Restricted access: **the report access** is determined by risk management function.

3.6. Requirements for monitoring and testing

In order to ensure that the IT risk profile is in line with risk appetite over time, appropriate monitoring and testing processes should be in place. This would allow finding out if the implemented controls were adequate and effective in addressing risks.

A monitoring process must be capable of addressing the need for revisions in the design of controls based on changing risk and considering the evolution of threats as well as the state of the technology. Regular controls adequacy evaluations must also consider any new technological solutions available to cope with the threats, or controls not implemented in the past because they were considered too expensive, but where cost has dropped and is currently justifiable.

In case of controls based on outdated technology, it should be evaluated if they are still adequate to contain the threats, or result in an increase of the threats frequency and of the risk profile.

Therefore, corrective action plans may be required to bring back the risk exposure below risk appetite.

Testing and monitoring processes must be capable of containing risks at an acceptable level to ensure control effectiveness on an ongoing basis and that weaknesses in controls are identified in a timely manner. Any control gaps need more specific risk analyses in order to assess possible impacts on the evaluation of risk frequencies or magnitudes, as well as to address appropriate remedial plans. For example, the review of a disaster recovery testing that has failed will have consequences on the assessment of the magnitude of system unavailability scenarios due to longer recovery times. Furthermore, most organisations are subject to regulations that require a functioning and monitored framework to manage internal controls over financial reporting, e.g., Sarbanes-Oxley Act or national SOx-like regulations. These rules already require an assessment of the design and effectiveness of IT controls on a periodic basis. It should be considered whether it is necessary to extend approach to what is not in the ICFS domain in order to cover the full IT risk scope.

Organisations use a wide variety of monitoring procedures[22] on internal processes and outsourcing processes, including, but not limited to:

- self-assessments by first line (BU management or IT management) of controls' effectiveness;
- periodic controls evaluation and independent testing by corporate internal audit;
- combination of first line tracking of controls and independent second line of defence testing
- analysis of operational indicators or metrics, embedded in existing processes, that might identify anomalies indicative of a potential risk or control failure;
- continuous monitoring programs built into information systems;
- supervisory reviews of controls, such

[20] ISO/IEC 27000 Information Security Management Systems

[21] International Standards for Assurance Engagements No.3402

[22] Based on COSO - Guidance on Monitoring Internal Control Systems: "Organisations may select from a wide variety of monitoring procedures, including but not limited to: • Periodic evaluation and testing of controls by internal audit, • Continuous monitoring programs built into information systems, • Analysis of, and appropriate follow-up on, operating reports or metrics that might identify anomalies indicative of a control failure, • Supervisory reviews of controls, such as reconciliation reviews as a normal part of processing, • Self-assessments by boards and management regarding the tone they set in the organisation and the effectiveness of their oversight functions, • Audit committee inquiries of internal and external auditors, and • Quality assurance reviews of the internal audit department.

as reconciliations as a normal part of processing;
- analysis performed by IT experts on specific IT areas upon request of information risk management;
- service organisation control reports (e.g., ISAE 3402 on the reliability of third-party internal control frameworks) carried out by an external service auditor.

Appropriate monitoring and independent second line testing procedures should be implemented or extended to IT risk processes. Information flows should be activated from first line, compliance and internal audit to the information risk management function for the review of internal control effectiveness.

The review of any results of monitoring procedures should have a frequency that allows the timely updating of IT risk assessments, the management of any risk exposures and the adoption of appropriate mitigation actions.

Breadth, depth and independence of control testing are especially relevant for external audit purposes. Often, there is a multiplier effect between controls and technology elements with regard to risk and efforts to deliver assurance. It should be noted that external auditors are not much inclined to rely on internal IT control testing, which might lead to substantial parts of the test work being reperformed.

It is recommended to make clear agreements on controls to be tested, and how the test work needs to be performed and documented. For CROs, a point of attention is to follow up closely on deficiencies deriving from test work performed during the year to prevent that such deficiencies remain important audit issues during year-end closing processes.

3.7. IT risk frameworks overview

Selecting the appropriate IT risk framework from a multitude of approaches available is a challenge for CROs and CISOs because any such framework must be compatible with the overall ERM strategy. It can also have an impact on other critical programmes such as business continuity, crisis management, regulatory compliance, third-party management, and intra-group outsourcing obligations, among others.

Organisations should first go through a comprehensive review of their risk and security standards, processes and practices to gain a holistic understanding of their current approach to IT risk and then derive the entire IT security strategy accordingly, taking into account the business objectives and the defined and approved risk appetite of the company.

Next, they should complete a review of the current IT risk methodologies, frameworks and industry best practices, and then choose the one that better fits their own requirements and often also fits the mandatory regulatory requirement. Since multiple options exist, it is in the interest of the CRO Forum to get a comprehensive overview of all the main existing IT security risk methodologies.

The following section provides a summary of a number of existing frameworks with further details of the results of the research examining the applicability of main methodologies. This is carried out through inter-comparison of a range of industry recognised frameworks and techniques in the Appendix.

Several models have been developed to compare the main information risk management methods in recent years, for example, the *European Union Agency for Network and Information Security* (ENISA) and *US National Institute of Standards and Technology* (NIST), have developed their own comparison methods. Whilst these comparison methods offer similar approaches, the *Core Unified Risk Framework* (CURF) model, proposed by the Norwegian University of Science and Technology, addresses the issue from a different perspective.

In this method, originally published by the Department of Information Security and Communication Technology provides an all-inclusive, bottom-up approach to compare frameworks. Moreover, CURF takes into account *a privacy risk assessment framework* and *a cloud risk assessment* to obtain a more consistent, complete and updated model. Given the recent introduction of EU GDPR and the rising privacy-related concerns, as well as the transition to cloud-based services that many organisations have been facing in recent years, privacy risk assessments and cloud assessments have gained weight and thus it is a critical requirement that any assessment of IT risk frameworks should encompass requirements relating to privacy and cloud.

It should be noted that the frameworks covered here are under a finite list and other methodologies exist that are not presented or are any hybrid or amalgamated approaches.

As a CRO, the main objective is to assure a consistent framework is chosen and that this framework is used throughout the organisation by all lines of defence (one risk language). The following section provides a high-level overview of a number of methodologies, in no particular order of preference; more details can be found in Appendix 1. Some general frameworks are:

COBIT 5 for Risk & Risk Scenarios Using COBIT 5 for Risk (ISACA)

The *"COBIT 5 for Risk"* is part of the COBIT® 5 framework, released in 2013 and developed by the Information Systems and Control Association (ISACA).

It was designed mainly for CIOs and CROs in addition to the COBIT 5, in order to establish the risk governance and management function(s) for the enterprise providing them guidance on the overall governance of enterprise IT risk. This publication includes and replaces the *"Risk IT Framework"* (2009). COBIT 5 for Risk defines IT risk a business risk, specifically, the business risks associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise.

ISACA's *"Risk Scenarios Using COBIT 5 for Risk"* (2014) gives additional guidance on the development of IT-related risk scenarios, integrated with COBIT 5 for Risk, to solve for current business issues. It provides a high level overview of risk concepts, along with over 50 complete risk scenarios covering all 20 categories described in COBIT 5 for Risk.

Using both the publications in synergy, enables a company to cover the full life cycle for risk governance and risk management including especially IT-related risks. It is aimed to guide organisations in making appropriate risk-aware decisions, by providing end-to-end view of main IT-related risks and treatments and providing support to respond to risk that exceeds the enterprise's risk appetite and tolerance level. This methodology interprets risk as product of *frequency* and *magnitude*.

Advantages	Disadvantages
• The entire lifecycle management of IT risk is covered – mainly focused on providing the business perspective of the risks • Integrated with COBIT 5 and consistent with main techniques such as ISO 27005, 27001 and 31000, COSO ERM, NIST • Provide support and examples to respond to risk that exceeds the enterprise's tolerance level through the risk scenarios (111 risk scenario examples)	• Specialist resources required for the implementation • Strongly suggested the adoption of COBIT 5 within the organisation • Not designed to managed standalone in-depth Information Security method and therefore it should be integrated with specific security standard

Factor Analysis of Information Risks

The Factor Analysis of Information Risks (FAIR) methodology is part of the FAIR framework developed by Risk Management Insight LLC and published in 2005 under an Attribution-Non-Commercial-Share licence. The goal of the framework is to provide an effective alternative that doesn't rely on the practitioner's experience to be implemented. On the contrary, it is intended to provide a comprehensive risk quantification approach, deriving output from consistent computations easy to repeat. It is a sequential method, based on the classic risk = likelihood * magnitude definition, and it makes use of several types of matrices to articulate risk. It is also supported by a dedicated tool, called FAIRLite.

After step by step estimations and computations, an evaluation of total risk is obtained on ordinal scale. The risk assessment described is intended to use in simple, single level risk analysis, but a slightly more complex analysis can be achieved by simply running the basic assessment multiple times, once for each asset/threat community pair.

Advantages	Disadvantages
• Independent from the practitioner's experience to be implemented effectively • Detailed approaches and tools supporting the quantification of frequency • Threat agent / attacker's perspective taken into account in the estimation process	• Training courses needed to obtain the minimum level knowledge required – not very easy-to-use • Not thoroughly documented as other methods – documentation to perform more complex assessment not publicly available • Lack of completeness in risk identification process

ISF - Standard of Good Practice for Information Security

The Standard of Good Practice for Information Security (ISF Standard) has been developed by the Information Security Forum (ISF), an independent not-for-profit association of organisations, since 2011. The last updated was in 2016. It provides a set of high-level principles and objectives for information security together with associated statements of good practices. It comes with an extensive and comprehensive list of controls and guidance on emerging IT security topics.

The standard covers the controls areas of several methods such as COBIT 5, ISO/IEC 2700x series, NIST Cybersecurity Framework; as well as legislations such as PCI DSS 3.1 and SOX. It bases its risk definition on threat – in terms of confidentiality, integrity and availability related compromises, and vulnerability.

It is provided with several materials for the implementation and it comes with the ISF Benchmark, a tool specifically addressed to compare the ISF Standard with others security methodologies and regulatory requirements to achieve better implementation of security controls.

Supporting this standard, the ISF also conducts the ISF Benchmark survey every two years which provides objective analysis of member organisations allowing them to measure and benchmark against their peers both the effectiveness and value of security investments. The ISF also produces a Threat Horizon report that is intended for business leaders who want to understand cyber risks and their impacts to the future of their businesses.

Advantages	Disadvantages
• Complete and effective control set covering several topics of information security • Scope extended to the legislation perspective – PCI DSS and SOX • Updated every 2 years to keep up with last technology evolutions and regulatory changes	• Heavily focused on controls, risk treatment and recommendations – it doesn’t provide guidance for risk identification and evaluations • The entire lifecycle of information risk management is not covered • Rarely used as a standalone framework – it relies on the implementation of other methods

ISO/IEC 27005:2011 - Information Security Risk Management

There are many ISO/IEC standards related to security and several dependencies between these documents exist, with concepts from one standard being relevant for understanding those in another. ISO/IEC 27005 was published by the International Organisation for Standardization (ISO) and the International Electrotechnical Commission (IEC). The first version was launched in 2008 as a replacement of previous standards ISO/IEC TR 13335-3:1998 and ISO/IEC TR 13335-4:2000.

The standard is intended to provide guidelines for information risk management and it outlines a generic risk assessment process methodology, describing risk as result of threats, vulnerabilities, and impacts. The annexes contain examples for information security risk assessment approaches along with list of applicable threats, vulnerabilities and security controls.

Advantages	Disadvantages
• Complete and comprehensive framework as it covers the entire IT risk lifecycle • Not overly prescriptive – its principles can be applied to various organisations • Comprehensive tasks and processes descriptions – examples of applications and checklist templates provided	• Specialist skills may be required to support the implementation • It does not recommend a specific methodology with enough technical details for performing the risk assessment • Not easy to consult for novices – extensive use of technical terminology and interpretations

NIST SP 800-30

The Risk Management Guide for Information Technology systems by the National Institute for Standards and Technology (NIST) was firstly released in 2002, but it is still US government's preferred risk assessment methodology and it is mandated for US government agencies.

It is developed to give a practical approach based on the classic risk = likelihood * magnitude definition. It comprises a detailed process from the initial phases of preparing for the assessment and identifying context and assumptions, through determining probabilities and impacts, presenting resulting risks, and finally monitoring effectiveness of controls and verifying compliance. NIST SP 800-30 is addressed to organisations of all sizes in both private and public environments.

Advantages	Disadvantages
• Available for free from the NIST website with detailed checklists, mathematical formulas and other materials • Frequently assessed and restructured as new technologies/ regulations arisen • May be used in conjunction with other frameworks from NIST (such as NIST Cyber Security Framework) and/or other parties	• Heavily US-focused supporting documentation • Prescriptive and not easy to adopt • Finding appropriate support to effectively implement the methodology may be difficult outside the US

Some more specific frameworks:

CCTA Risk Analysis and Management Method

The CCTA Risk Analysis and Management Method (CRAMM) is based on the best practices of British government organisations. It was developed in 1985 by the British government organisation CCTA (Central Communication and Telecommunication Agency), now renamed into Office of Government Commerce (OGC). At present, the methodology is owned by Insight Consulting.

CRAMM is a qualitative method that bases the risk definition on a computation between threats, vulnerability and assets characteristics. Specific tools are required to provide full support to the methodology and this makes CRAMM rather complex to use without the dedicated software.

Advantages	Disadvantages
• UK government's preferred methodology and regularly updated • Historical data taken into account for quantification of losses • Provided with a complete and detailed database of countermeasures and controls	• Time-consuming and complex to use without the dedicated software tool • Expert knowledge and skills required to obtain sensible results – appropriate for large organisations and Public Bodies • Risk estimation process based on subjective estimations from practitioners

CORAS

CORAS – “A platform for risk analysis of security-critical systems” is the method and tool resulting of an EU-funded project called IST-2000-25031, in 2003. The method was created as a result of a project aimed primarily at the analysis of risks impacting critical systems of an organisation. Since its first edition, the method itself has not undergone any substantial updates. The ultimate goal was to develop a practical model-based framework and computerized support. CORAS estimates risk as chance of occurrence of an unwanted incident and relies on a modelling language which is an extension of the Unified Modelling Language (UML). It is based on a pre-defined set of symbols and it comes with a dedicated tool that supports the reporting through risk modelling.

Advantages	Disadvantages
• Compatible with most of risk assessment methodologies • Complete and effective description of risk identification process provided • Updated by the Open Source community	• Specific tool required to implement the method • Time consuming – participants need experience in the various techniques to be able to select and apply them efficiently • Knowledge of UML language required

Conflicting Incentives Risk Analysis

Conflicting Incentives Risk Analysis (CIRA) is a risk assessment approach initially developed thank to the contribution of the researchers Rajbhandari and Snekkenes in 2013. CIRA is based on the game-theory, decision-making theory and economics, and it approaches risk taking into account the existing incentives between the stakeholders, such as information asymmetries, moral hazard situations and opportunity risks. It is a sequential method specifically addressed to stakeholders, their actions, and perceived outcomes.

CIRA doesn’t rely on classic risk expression and it uses an alternative notion for risk. In this method, risk is framed in terms of conflicting incentives between risks owner and the other stakeholders while any probability or frequency calculations are neglected.

Advantages	Disadvantages
• Scope broaden to human-based factors impacting the evaluation of information security risk • Existing incentives and relationships between the various stakeholders considered • Opportunity risks taken into account during the risk estimation	• Probability and frequency based calculations are entirely neglected • Incompatible with most of IT risk frameworks • Expert knowledge required – a complete assessment may be time-consuming and overly-complex

Microsoft Cloud Risk Decision Framework

Microsoft Cloud Risk Decision Framework (MCRDF) is a sequential method realized by Microsoft to provide an overarching risk-management framework to allow organisations to conduct a risk-based assessment of a transition to the cloud. It was published in 2006.

The framework is aimed to assist IT and non-IT individuals to evaluate potential cloud-based IT capability providing a well-structured process, based on the ISO 31000 general risk management framework. MCRDF describes risk as the effect of uncertainty on objectives and quantifies it with likelihood and impact.

Advantages	Disadvantages
• Scope extended to cloud-based risks and controls • Provided with easy-to-apply examples of semi-qualitative calculations, practical tools and checklists • Consistent with ISO frameworks	• Specifically designed to provide a cloud vendor assessment or an assessment of the transition to the cloud • Approaches for identifying and managing risks that are out of cloud-scope are neglected • Inappropriate as standalone information security framework

NSMROS

The Norwegian Data Protection Authority’s (Datatilsynet) Risk Assessment of Information Systems (NSMROS) was derived from the Norwegian Security Act for compliance purposes and published in the 2006. In origin, the methodology was specifically designed to support organisations to become compliant with the Norwegian Security Act. NSMROS is based on a sequential, probabilistic approach which is focused on the protection of assets, threats, and vulnerability.

It is based on the classic risk = likelihood * impact definition and it makes use of several kind risk matrices to support the risk evaluation process.

Advantages	Disadvantages
• Compatible with most of risk assessment methodologies • Data losses taken into account for impacts quantification • Easy to use and to implement – well suited for beginners and small organisations	• Specifically designed to support organisations to comply with the Norwegian Security Act • Based on subjective probabilities estimations • Scarce explanations to perform key tasks and lack of supporting examples – business processes and stakeholder neglected

OCTAVE Allegro

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) methodology was developed within the Software Engineering Institute, part of Carnegie Mellon University, by the Computer Emergency Response Team (CERT) in 2007. It was initially funded by the US Department of Defence.

The goal of the OCTAVE suite of tools, techniques and methods is to allow risk-based information security strategic assessment and planning.

The framework consists of three OCTAVE methods and OCTAVE-Allegro is the one providing a faster, streamlined approach, addressing risk as the consequence of the event and related uncertainty. It is an asset-centric approach, which only considers information as an asset.

Advantages	Disadvantages
• Fast and easy to understand and to implement • Managed in a workshop-style – not requiring extensive expertise or investments in training or consultants’ fees • Extensive supporting materials available for free in a worksheet format	• Risk estimation process needed to be carried out by a skilled analysis team • Incompatible with frameworks based on the probability*magnitude risk approach • Subjective-driven analysis of probability

Privacy Risk Assessment of Information Systems (RAIS)

Privacy Risk Assessment of Information System (RAIS) is a sequential method scoped primarily for assessing privacy-related risks, developed by the University of Tennessee in 2006 and available at the US Environmental Protection Agency. RAIS comes with a domain-specific support tool for mapping and evaluating personal information, critical data and related impacts in terms of privacy. It is an asset-centric approach and it follows the classic likelihood * impact definition of risk.

Advantages	Disadvantages
• Scope broaden to personal information, critical data and related impacts in terms of privacy • Well described likelihood and impacts estimation process • Personal data mapping and PI identification taken into account	• Lack of focus on vulnerability, threat, and controls management • Exclusively designed to cover privacy risk • Not designed to cover the full spectrum of information and technology risk

Appendix 1
Framework assessments

By progressively taking into account most of the frameworks summarised in chapter 5, the core unified risk framework (CURF) model structure is framed. It is obtained by comparing and matching the majorly used information security risk assessment (ISRA) methods and is based on a recurrent structure of three core phases: risk identification, risk estimation and risk evaluation.
For each of these phases, the CURF model is articulated in a super set of attributes collected according to the following methodology: if an attribute is addressed in one of the ISRA methods in scope, but not in the model, it is added to the new super set.

In this respect, each of the ISRA methods have been surveyed and compared to the obtained model, taking into account the three core phases separately. The degree to which a single method covers all the attributes added to the superset is considered as a measure of completeness of the method itself.
As result, it is possible to derive the level of compatibility of a framework with each phase and to point out areas that are well overseen and those showing major gaps in management and controls.

With this in mind, ISO/IEC 27005 information security risk management resulted as the most complete approach considering the overall scoring. In particular, this ISRA method obtained the highest compatibility in the risk identification phase, while the factor analysis of information risk (FAIR) appeared to be the most compatible method for the risk estimation process. Finally, conflicting incentives risk analysis (CIRA) and OCTAVE Allegro resulted as the most compatible approaches for risk evaluation.

Details about the results of the research are reported below, along with the description of each attribute that constitutes the CURF model, articulated in domains, subdomains and outcomes.

Overall results					
Risk identification		**Risk estimation**		**Risk evaluation**	
ISRA	**Compatibility (*)**	**ISRA**	**Compatibility (*)**	**ISRA**	**Compatibility (*)**
ISO/IEC 27005	HC	FAIR	HC	CIRA	HC
CORAS	C	NIST SP 800-30	C	OCTAVE Allegro	HC
COBIT 5 for Risk	C	ISO/IEC 27005	C	ISF Standard	C
OCTAVE Allegro	C	COBIT 5 for Risk	C	COBIT 5 for Risk	C
CRAMM	C	ISF Standard	C	RAIS	C
FAIR	C	MCRDF	C	CRAMM	C
NIST SP 800-30	C	RAIS	C	ISO/IEC 27005	C
ISF Standard	C	CIRA	C	CORAS	C
CIRA	C	OCTAVE Allegro	LC	NSMROS	C
NSMROS	C	NSMROS	LC	NIST SP 800-30	LC
RAIS	LC	CORAS	LC	FAIR	LC
MCRDF	LC	CRAMM	LC	MCRDF	LC

(*) HC: Highly compatible, C: Compatible, LC: Less compatible

CURF attributes	
1. Risk identification	
Domain	**Subdomain**
Preliminary Assessment	• *Preliminary assessment* is the high-level or initial assessment of the ISRA, targeted to obtain an insight into the problems and scope (assets, vulnerabilities, threat agents).
Risk Criteria Determination	• *Risk criteria determination* is the process when the ISRA team and/or the decision-makers decide on risk criteria for the risk evaluation process used to assess the significance of the risk. This includes measurements of risk tolerance and appetite. • Several ISRA approaches suggest *identifying business objectives* to aid in scoping the risk assessment and increasing relevance. • *Key risk indicators* built according to the predefined appetite are metrics showing if the organisation is subjected to risks that exceed the appetite. • *Cloud-related risk considerations* are made specifically for cloud migrations and operations, (including infrastructure, platform, and application as a service risks).
Stakeholder Identification	• *Stakeholder identification* is the process of identifying and prioritising the main stakeholders involved in the risk assessment. • *Stakeholder analysis* is the process of analysing the stakeholders according to some relevant criteria, e.g. their influence and interest in the project.
Asset Identification	• *Asset identification* is the process of identifying assets. • *Asset evaluation* determines asset value and/or criticality. • *Business process identification* is the process of identifying business process. • *Identifying the asset owner* helps shape the scope and target of the risk assessment. • *Asset container* identifies where assets are stored, transported, and processed. • *Mapping of personal data* is a part of the privacy risk assessment process, where the system's handling of information assets containing personal data is mapped and assessed.
Vulnerability Identification	• *Vulnerability identification* is the identification of the vulnerabilities of an asset and/or control that can be exploited by one or more threats. • *Vulnerability assessment* is the process of identifying, quantifying, and prioritising (or ranking) the vulnerabilities in a system.
Threat Identification	• *Threat identification* is the process of identifying relevant threats for the organisation. • *Threat assessment* comprises methods and approaches to determine the credibility and seriousness of a potential threat.
Control Identification	• *Control identification* is the activity of identifying existing controls and mitigation measures. • *Control (efficiency) assessment* is the method to determine effectiveness of the existing controls in terms of risk mitigation.
Outcome Identification	• *Outcome identification* is the process of identifying the likely outcome of a risk (impacted asset, vulnerability, threat) regarding breaches of confidentiality, integrity, and availability. • *Outcome assessment* incorporates methods and approaches to estimate the potential outcomes of an event.
Outcome	
Risk Scenario	• Asset (including business processes) • Vulnerability • Threat • Outcome

CURF attributes	
2. Risk estimation	
Domain	**Subdomain**
Threat Assessment	• *Threat assessment* expands the definition of risk identification providing tools to estimate the particular threat agents. • *Willingness/motivation* to attack, *capability* in terms of know-how, *capacity* in terms of resources available to conduct the attack, and the potential *attack duration* can be provided by the ISRA method.
Probability and Impact Estimation	• *Frequentist (quantitative)* or subjective knowledge-based assessments *(qualitative)* are the available approaches for probability estimation. • Similarly, impact estimation can be based on relevant historical data *(quantitative)*, or be relied on knowledge-based assessments of impacts/outcomes *(qualitative)*.
Risk Specific Estimations	• *Privacy risk estimation* are specific methods to estimate privacy-related risks. • *Utility and incentive calculation* addresses the risk for each involved stakeholder and the related existing incentives. • *Cloud vendor assessment* includes methods for assessing the cloud vendor's existing security controls and compliance. • *Opportunity cost estimation* assess how much it will cost not to act against the risk.
Risk Aggregation	• The *risk aggregation* activity is conducted through rolling up several linked, often low-level risks into a more general or higher-level risk. Interconnected individual risks can also aggregate into a worst-case scenario.
Level of Risk Determination	• *Level of risk determination* consists of the assignment of likelihood and consequence to the estimated risk (or incident), compiling a list of risks with assigned value levels.
Outcome	
Risk	• Events • Consequences • Uncertainties • Probability • Model sensitives • Knowledge about risk

CURF attributes	
3. Risk evaluation	
Domain	**Subdomain**
Risk Criteria Assessment	• *Risk criteria assessment* is the process of either creating or revising risk criteria to evaluate risk levels.
Risk Prioritisation/ evaluation	• *Risk prioritisation/evaluation* is the process of evaluating risk significance and prioritising in view of further risk treatments and investments.
Risk treatment recommendation	• *Risk treatment recommendation* is the process of suggesting treatments to assessed risk.

Detailed results

ISO/IEC 27005

- The ISO/IEC 27005:2011 scored the highest on the ISRA completeness measurement. The only attributes that are not specifically addressed in the risk identification process are *key risk indicators, asset containers, preliminary assessment,* and *stakeholder analysis*.
- In the risk estimation process, the standard supports the execution of both *subjective knowledge-based* and *frequentist-based* estimations (for the latter, prior knowledge of statistics is required). Regarding risk calculation, *uncertainty, model sensitivity, and knowledge aspects* are mentioned. On the other hand, it does not address the *specific threat assessment* activities as a part of the process.
- In the risk evaluation process, the predefined risk criteria are applied while several types of *matrices* for risk evaluation and prioritisation are provided.

FAIR

- Out of the surveyed ISRA methods, FAIR stands out as the most focused on risk estimation and risk quantification. However, it shows lack of completeness in the risk identification process. FAIR only proposes a *preliminary assessment* of assets and threats to identify risk and obtain a scenario.
- The strength is in risk estimation, in *frequency quantification* specifically, where it appears as the most mature of the methods. In addition, it provides tools for *risk measurement* and *quantification*. Threat agent's capability is evaluated through *knowledge and experience requirements*, and *capacity resources* available to the attacker.
- For risk evaluation, FAIR approach makes use of several types of *matrices* to frame risk.

COBIT 5 for Risk

- ISACA's COBIT 5 for Risk can be seen as an assistant method due to the extensive support documentation it provides. Risk IT scores the second highest in overall completeness. For risk identification, it should be used in conjunction with the 'Risk Scenarios Using COBIT 5 for Risk' publication as this is focused on *risk scenarios*, covering *vulnerabilities* and *controls identification*.
- In risk estimation, the identified risk scenarios take into account *losses and consequences*, based on several factors such threat *type, actor, event and attack duration*.
- Regarding risk evaluation, it proposes a risk ranking based on company's risk appetite and tolerance levels with four possible *treatments*: avoidance, mitigation, transfer and acceptance.

NIST SP 800-30

- NIST SP 800-30 scored in the bottom range of the risk identification compatibility. It is a threat-centric method, and this creates a gap in asset identification and evaluation processes. NIST's methodology proposes a *threat-based* approach to risk, instead of an *asset-based* one. Finally, it neglects attributes such as outcome and *stakeholder assessments*.
- In the risk estimation, it provides a comprehensive *threat assessment* process. It supports both *subjective knowledge-based* and *frequentist probability estimations*. Anyway, it only supports *subjective impact estimations*. However, it proposes different risk models and scores the second highest in compatibility in this stage.
- In risk evaluation, the method suggests to evaluate and prioritise risks in tables consisting of *descriptive categories*.

ISF Standard

- ISF Standard can be used individually or together with the other tools provided as a suite. It scores as medium in compatibility for risk identification, as it neglects attributes such as *asset and business process identification* as well as *risk criteria* determination. On the other hand, it offers an extensive coverage of *vulnerabilities* and *controls* up to date.
- The standard is less compatible for the risk estimation process as it does not provide sufficient guidance to estimate *likelihood* and *impact* and to finally derive risk levels. As a result, ISF is scarcely applicable as a standalone method for the risk estimation process.
- For risk evaluation, the method scores among top performers in *risk treatment recommendation* as it provides the most comprehensive list of controls and mitigation measures, collected from other globally accepted information security approaches and related international regulations.

Detailed results

OCTAVE Allegro

- OCTAVE Allegro can be defined as an assistant method as it offers to the practitioner an extensive amount of worksheets. The risk identification process scores well in compatibility, while *vulnerability, control,* and *stakeholder assessments* are the main gap-areas.
- The method scores low in compatibility in the risk estimation due to the fact that it does not provide activities to address probability besides a *subjective-driven analysis* in a worksheet. Moreover, it does not address *vulnerability* and *threat assessments* in any part of the process.
- For risk evaluation, *risk matrices* are provided by the method, as well as *risk treatments* techniques.

CORAS

- CORAS method resulted as one of the most complete ISRA regarding the risk identification processes. Although it does not directly address *business processes*, it proposes to map various assets into processes and mentions business process identification as a part of the *structured brainstorming* stage. It does not provide any steps for identifying and *assessing* existing *controls*, although identifying insufficient controls is part of the *vulnerability identification* activities described. Finally, *stakeholder communication* is well emphasised.
- CORAS lacks more advanced threat intelligence activities for risk estimation. CORAS proposes *frequentist estimations*, but primarily following a *qualitative approach* using workshop forms.
- Concerning risk evaluation, CORAS makes use of various *risk matrices*.

CIRA

- CIRA method relies on game theory and decision-making techniques; therefore its view is very different from the other ISRAs taken into account. According to the risk identification comparability results, CIRA performs well in *threat actor* and *stakeholder assessments*.
  However, it does not include *business activities* nor does it directly provide *vulnerability* and *controls identification* techniques.
- On risk estimation, CIRA is primarily concerned with the threat-side of the estimation but avoids probability calculations. However, CIRA also takes into account *opportunity risks*.
- Regarding risk evaluation, the method addresses risk criteria as defined by *risk owner's tolerance*. Finally, the method applies an *incentive graph* for visualising risks and opportunities.

CRAMM

- Regarding risk identification process, CRAMM can be defined as an asset-based method as it considers specific threats and vulnerabilities associated to each asset. The *business*- and *stakeholder*-related attributes are neglected.
- The risk estimation process is based on *subjective estimates* from experts. However, the method also proposes for quantifying losses with *historical data*. CRAMM lacks all advanced threat intelligence attributes for risk estimation.
- For the risk evaluation process, CRAMM relies on several kinds of *risk matrices*.

RAIS

- RAIS is a sequential method scoped for assessing privacy risks so the emphasis is on the identification of personal information. The method comes with domain-specific tools for mapping and evaluating personal data and adds two additional categories to CURF: *mapping of personal data* and *privacy risk estimation*.
  On the other hand, risk identification process compatibility scores the lowest of all ISRAs, primarily due to the lack of focus on *vulnerability, threat,* and *controls*.
- The *threat assessment* tools provided for the risk estimation are comprehensive, while the process to estimate likelihoods and impacts is well described, making the method score high in compatibility for risk estimation.
  The main drawback of the method is that it overall lacks tools in control and vulnerability analysis.
- RAIS emphasises *risk criteria* and *acceptable risk* but does not suggest revising them in the risk evaluation phase.
  Anyway, its compatibility grade is above average in this last phase.

Detailed results

MCRDF

- Microsoft's CRDF is an ISRA scoped to provide support in the decision about cloud-based risks. Although the method results as less compatible with the risk identification process, it adds *cloud-specific risk domains*.
- In the risk estimation phase, a *cloud vendor assessment* is provided. Anyway, the method scores low in compatibility regarding common ISRA-related tasks, such as asset evaluations and threat assessment. The main strength of the method is the overview of *cloud risks control areas*. Finally, MCRDF provides easy-to-apply examples of *qualitative calculation*.
- For the risk evaluation process, MCRDF scores low in compatibility as it does not provide additional approaches for identifying and managing risks that are outside of the risk control areas.

NSMROS

- The NSMROS ranks the lowest in overall completeness measurement. In particular, its risk identification process is mainly focused on *assets, threat, vulnerability*, and *outcomes*, and it covers very few additional attributes. In addition, main business-related attributes, such as *business processes* and *stakeholder assessments* are not present in the method.
- The more advanced threat assessment aspects are missing from the risk estimation process. The method provides *subjective probabilities* estimations, but does not exclude *frequentist-based* approaches. In addition, it suggests gathering *data losses* as a way to quantify impacts.
  In risk evaluation, the method is supported by *risk matrices*.

Appendix 2
Example controls and KRIs

Example controls
Ensure that information assets (systems and data/information) ownership and classification are performed.
Ensure that any incidents are properly responded to, recorded, resolved or investigated for proper resolution.
Ensure implementation and maintenance of preventive, detective and corrective measures in place (especially up-to-date security patches and malware control) across the enterprise to protect information systems and technology from malware.
Ensure that user access rights, including roles and segregation of duties are appropriately managed to prevent unauthorised use, disclosure, modification, damage or loss of data.
Ensure that IT assets are monitored on a regular basis by an appropriate governance committee, including legacy and IT refresh aspects.
Ensure a process is defined, documented and implemented to monitor software licenses and contracts on an annual basis.
Ensure that service levels with respect to the quality and the availability of the information system are defined annually with the business, documented in SLAs and monitored regularly.
Ensure that an incident management (from detection to resolution) and problem management processes are defined, documented and implemented, in line with business requirements.
Ensure that an information security governance is defined, documented and implemented.
Ensure that appropriate network security controls are defined, documented and reviewed on a regular basis by the local defined governance.
Ensure that appropriate patch and vulnerability management process is defined, documented and implemented.
Ensure that all facilities hosting IT equipment are physically secured.

KRI family	KRIs
Endpoint protection	% of endpoints without hard drives encrypted
Endpoint protection	% of laptops with encryption solutions
Endpoint protection	% of systems without up-to-date malware protection signatures
Endpoint protection	% of vulnerabilities not addressed within SLA for end-user devices
Endpoint protection	% of local administrator (open client/close client) access without appropriate justification
Endpoint protection	% of deployments on end-user devices which have not been tested prior to deployment
Endpoint protection	% of endpoints not protected by active data loss prevention (DLP)
Endpoint protection	% of classified data related to the IT applications to the total amount of IT applications in the entity
Access management	% of servers not enforcing password requirements
Access management	% of systems considered critical without periodic access recertification
Access management	% of leavers without corresponding disabled accounts
Access management	% of applications containing confidential data without least privilege and segregation of duties
Access management	% of internet-facing applications not controlled by authoritative identify management systems of record
Access management	% of web applications' penetration tested
Access management	% of privileged accounts (different levels, e.g. domain admin, local admin, etc.)
Access management	% of sleeping accounts (accounts not in use)
Resilience	% of critical applications without full operationalised disaster recovery capability
Resilience	% of critical applications hosted by third parties not meeting disaster recovery obligations
Vulnerability management	% of identified (high) critical vulnerabilities per device to the total amount of devices (older than one patch circle)
Vulnerability management	% of servers hosting critical applications without vulnerability scanning
Vulnerability management	% of servers that have patches not applied within the set time frame
Vulnerability management	% of critical vulnerabilities over 60 days old
Vulnerability management	% of active and monitored servers with antivirus signatures over 24 hours
Vulnerability management	% of spam/malware emails not filtered
Incident response	% of security incidents that are not responded to within defined response time
Incident response	% of accurate classification of incidents to the total amount of incidents
Incident response	% of lured people during a phishing simulation targeting all employees

Appendix 3
Definitions

Term used	Definition
Artificial intelligence (AI)	The ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings. Intelligent beings are those that can adapt to changing circumstances (source: Encyclopedia Britannica).
Big data	Datasets whose size (structured or unstructured) is beyond the typical database software tools' abilities to capture, store, manage, and analyse (source: 2011 big data study McKinsey). Often organisations have collected this data over a number of years on a day-to-day basis.
Business impact assessment (BIA)	A process that identifies and evaluates the potential effects (financial, life/safety, regulatory, legal/contractual, reputation and so forth) of natural and man-made events on business operations (source: Gartner IT-glossary).
CIA-AD criteria	Aspects to materialising risks with a devastating (potential) effect on confidentiality, integrity, availability, authenticity of data and the agility/delivery of IT. These criteria are used within this paper for the business impact assessment (BIA).
Cloud computing	Style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service using internet technologies (source: Gartner IT-glossary). This can occur as Infrastructure as a Service (IaaS) or Platform as a Service (PaaS) or Software as a Service (SaaS), deployed in a public, private or hybrid model.
Cyber-security	Cybersecurity is the domain providing trust, protection and safety to all cyber assets (i.e., software and information) of an organisation (source: Gartner).
Data classification of assets	Identify critical information assets based on their value to the business (source: ISF security forum).
Data ownership	As CIOs mature their group to a service-optimised IT organisation, they need to separate responsibilities for service outcomes from process outputs. Each of these requires a distinct 'owner' role to ensure processes and services are defined, coordinated and executed consistently and reliably (source: Gartner).
External services provider (ESP)	An external services provider (ESP) is an enterprise that is a separate legal entity from the contracting company that provides services such as consulting, software development — including system integration and application service providers (ASPs) — and outsourcing. ESPs supplement the skills and resources of an in-house IS department (source: Gartner IT-glossary). A financial institution must stay in control over outsourced activities and identify and manage the risks associated with its use of ESPs.
Event logs	A file that records either events that occur in an operating system or other software runs, or messages between different users of a communication software. Logging is the act of keeping a log. In the simplest case, messages are written to a single log file (source: Wikipedia).
EU-GDPR	General Data Protection Regulation (GDPR) standardises data protection law across all 28 EU countries and imposes strict new rules on controlling and processing personally identifiable information (PII). It also extends the protection of personal data and data protection rights by giving control back to EU residents. GDPR replaces the 1995 EU Data Protection Directive (source: Forbes).
Information risks	Includes risks involving IT, information security, project and programme management, business continuity, data governance including data privacy, digital, and related innovation/emerging technologies (source: ISO 27001:2013).
Inherent risk	Risks without consideration of already implemented protection measures.

Term used	Definition
Internet of Things (IoT)	Internet of Things (IoT) refers to the network of physical objects that contain embedded technologies to communicate and sense or interact with their internal states or the external environment (source: Gartner IT-glossary).
IT infrastructure	A combined set of hardware, software, networks, facilities, etc. (including all information technology-related equipment), used to develop, test, deliver, monitor, control or support IT services (source: ITIL).
Legacy systems	Systems is based on outdated technologies, but is critical to day-to-day operations. Replacing legacy applications and systems with systems based on new and different technologies is one of the information systems (IS) professionals' most significant challenges. As enterprises upgrade or change their technologies, they must ensure compatibility with old systems and data formats that are still in use (source: Gartner IT-glossary).
Machine learning	Artificial intelligence that uses statistical techniques to give computer systems the ability to 'learn' (e.g., progressively improve performance on a specific task) from data, without being explicitly programmed (source: Wikipedia).
Net present risk	A method to value risky future cash flows (source: Wikipedia).
Patching	Patching of infrastructure, middleware and at application level a set of changes to a computer programme or its supporting data (middleware, infrastructure) designed to update, fix, or improve it. This includes fixing security vulnerabilities and improving the usability or performance (source: Wikipedia).
Platform as a Service (PaaS)	The process of securing and at the same time reducing its surface of vulnerability of operating system, databases and applications. The main objective is to ensure a controlled and validated authorised access to customer and company data (source: ISACA).
Personal data	Any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data (source: ec.europa.eu).
Recovery point objective (RPO)	The maximum time difference between last backup and breakdown of a system including loss of all recently entered data.
Recovery time objective (RTO)	Is the acceptable amount of time to restore the service as well as Recovery point objective (RPO) is the maximum time difference between last backup and breakdown of a system including loss of all recently entered data) are defined.
Risk appetite	Explicit understanding within the organisation of the relevant key IT risk themes and the associated risk tolerances. Ultimate responsibility is with the management board to define the overall risk appetite (source: theirm.org).
Risk culture	A term describing the attitude, knowledge and understanding of employees to be aware and see the urgency of IT as a main enabler in the day-to-day processes. An ongoing training is needed as IT technology is developing fast, requiring changing skills to keep IT knowledge and experience up to date (source: theirm.org).
Robotics	Robotics deals with the design, construction, operation, and use of robots, as well as computer systems for their control, sensory feedback, and information processing (source: Wikipedia).
RTO/RPO	RTO is the amount of time allowed for the recovery of a business function or resource after a disaster occurs (source: ISACA).
Security by design	An approach to software and hardware development that seeks to make systems free of vulnerabilities and impervious to attacks as much as possible through measures such as continuous testing, authentication safeguards and adherence to best programming practices (source: techtarget.com).
SOC report	System and organisation controls (SOC) report, based on an auditing standard for service organisations (source: Wikipedia).
Virtualisation	The process of adding a 'guest application' and data onto a 'virtual server', recognising that the guest application will ultimately part company from this physical server (source: ISACA).

Disclaimer

Dutch law is applicable to the use of this publication. Any dispute arising out of such use will be brought before the court of Amsterdam, the Netherlands. The material and conclusions contained in this publication are for information purposes only and the editor and author(s) offer(s) no guarantee for the accuracy and completeness of its contents. All liability for the accuracy and completeness or for any damages resulting from the use of the information herein is expressly excluded. Under no circumstances shall the CRO Forum or any of its member organisations be liable for any financial or consequential loss relating to this publication. The contents of this publication are protected by copyright law. The further publication of such contents is only allowed after prior written approval of CRO Forum.

The CRO Forum is supported by a Secretariat that is run by KPMG Advisory N.V.

Laan van Langerhuize 1, 1186 DS Amstelveen, or
PO Box 74500, 1070 DB Amsterdam
The Netherlands
www.thecroforum.org