The 2020 Vision of Information Risk Management

John Hermans, Alex van der Harst, Pieter de Meijer and Steven Verkaart

This article briefly surveys the history of business information risks, from early risks to business continuity to increasingly severe cyber attacks. Over the years, the Information Risk Management landscape has changed, and managing it has become more complex. Still, the Risk Management function hasn't changed that much. Looking ahead to 2020 we can imagine an ideal Information Risk Management process being in place, characterized by a number of key capabilities. Those capabilities would include real-time reporting and dynamic controls to monitor multiple factors, as well as flexible mechanisms to respond to higher or lower levels of risk. These features will need to be in place for businesses to perform effective Information Risk Management in the years ahead.

J.A.M. Hermans
is a partner at
KPMG Advisory N.V.
hermans.john@kpmg.nl

A.C. van der Harst
is a director at
KPMG Advisory N.V.
vanderharst.alex@kpmg.nl

P.R. de Meijer
is a manager at
KPMG Advisory N.V.
demeijer.pieter@kpmg.nl

S.R. Verkaart
is a manager at
KPMG Advisory N.V.
verkaart.steven@kpmg.nl

Introduction

Throughout the years, Information Risk Management has identified risks associated with the IT environment. Risks have evolved with changes to that IT environment. In the '70s and '80s, computers were entering the work space, and they were centralized and well managed. They were large mainframes, water cooled, taking up valuable space the size of a large office, but with less power than today's average calculator. Risk Management was focused on business continuity issues, which were mitigated by backup and recovery functions. In the beginning of the '80s new risks emerged as "high-powered" PC's were entering the market. Computing power moved out of the central computer room into the private working space of employees. Although the first network communications were slow, and were only enabled when needed, the current IT environment demands always-on, all-encompassing network connectivity. Businesses have been moving in parallel with these changes, becoming increasingly dependent upon the availability of PC's, servers, network connectivity, large storage capabilities, huge processing power, the internet and cloud computing. Data and information is the life blood of the business, and in some respects, is a company's most important asset. Imagine if all the information that is used to steer an organization were suddenly lost. In a manufacturing context, production lines would grind to a halt, distribution would lose all direction, and managing accounts would become a real challenge.

Although IT has changed dramatically, Risk Management in essence is still the same as always. The complexities in IT are much more difficult than they were in the '70s. IT has grown from specialty to commodity, and threats are changing by the minute.

This article showcases how Information Risk Management can work, and what Information Risk Management can bring to a company. It also describes the key capabilities that are needed to realize the benefits in common practice. The best Information Risk Management is not created overnight, certainly not in large and complex companies. Therefore we call this the 2020 Vision of Information Risk Management.

The Working Environment of an Information Risk Manager in 2020

Today most Information Risk Managers perform tedious risk processes, either on the input side or on the output side. On the input side, it is very difficult to definitively assess risk level. "Definitively" in this context means based on measureable risk factors instead of high-level assessments like: "The risk is about the same as last year, I think nothing has changed." On the output side, there are issues in reporting on risk, starting with collecting the requisite data to provide a clear overview to business management regarding the risks the organization is facing. Furthermore, it is very difficult to link the information risks to business risks. In most large organizations all the mentioned risk activities (input, processing, output) take up enormous amounts of energy, without producing a definitive risk overview.

In drawing this picture of today's Information Risk Management, we want to envision an ideal situation in the Information Risk Management of tomorrow. There certainly is a need to move toward better Information Risk Management, which today is insufficiently aligned with the current environment. Today's environment is a hyper-

In most large organizations risk activities (input, processing, output) take up enormous amounts of energy, without producing a definitive risk overview

connected world in which managing your own network is not enough. It is also an environment that is much more dynamic than it was twenty years ago: new threats might emerge tomorrow or next week, threats for which we have no planned response. Today, your risk process has to be agile.

If an Information Risk Manager in 2020 had "carte blanche" to design the organization's IRM-world, what would it look like? Let's select a couple of items for a "wish list," and have a look at how they could contribute to risk management in 2020.

Single view of risk

First of all, the 2020 risk manager would have a single view of risk. This means that there would only be one place to find all the necessary data for reporting on Information Risk. This single resource would include information about all assets: from infrastructure assets such as routers, to business software and the business processes. Also, this single resource would contain information on risk factors related to joint ventures or third-party service providers, since they all impact risk levels.

Real time

Taking the concept of an optimum resource for assessing risk a step further, there would not only be a single place to find data about risk, but also the ability to view it in real time. With one push of the button, the Information Risk Manager could obtain a current overview of risk levels. No more ad hoc questionnaires or workshop assessments; no more chasing non-responders for their assessment of the current status. Data is fed into the system, either by automated scanning or by specialized staff, and is evaluated in real time for increased levels of threat, impact or vulnerability.

Dynamic reporting

This real-time view would also provide more detailed information, on demand. Although high-level management would normally be interested in the company overview, there might be reasons for them to drill down. For example, if an alert were triggered, management might want a report on the situation: it might be the local IT infrastructure, or it might be the core-ERP system. This could be a very powerful tool for the Risk Manager, based on data analytics and well-designed dashboards.

Department-specific views

In developing a single view on risk, it should be easy to create custom views for Finance, Sales, IT, but also for functions like CEO, COO, etc. In these views, risks will be displayed that are very specific to the department at hand. For example, the Sales department would see risks of disclosing cost and markup prices (not the risk of hacking, which is not a direct risk the sales department typically faces). The IT department would see risks of hacking, and so on.

Evolution of risks

With all this data on risk, there is just one more element needed to see risks over time: a time stamp. The Information Risk Manager of 2020 has the ability to zoom in on specific risks, organizational entities, or threat categories, and would be able to see how the risk levels have changed over time. The risk of hacking or cybercrime would emerge somewhere in the 80's: popping up as a little dot, then growing to a serious threat over time. Another benefit of this is that it would be possible to extrapolate this view in order to predict the biggest threats. If linked

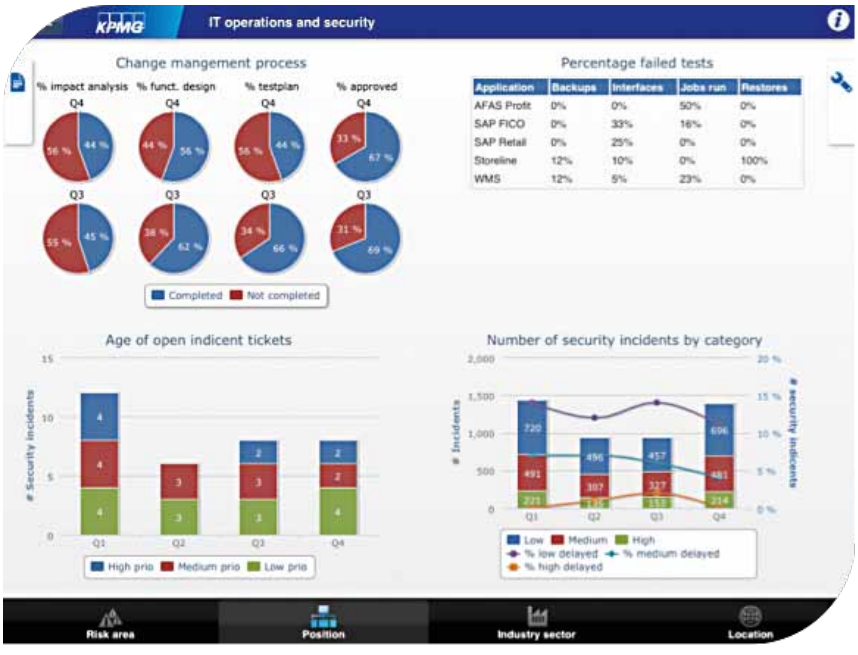

Figure 1. **A department-specific view.**

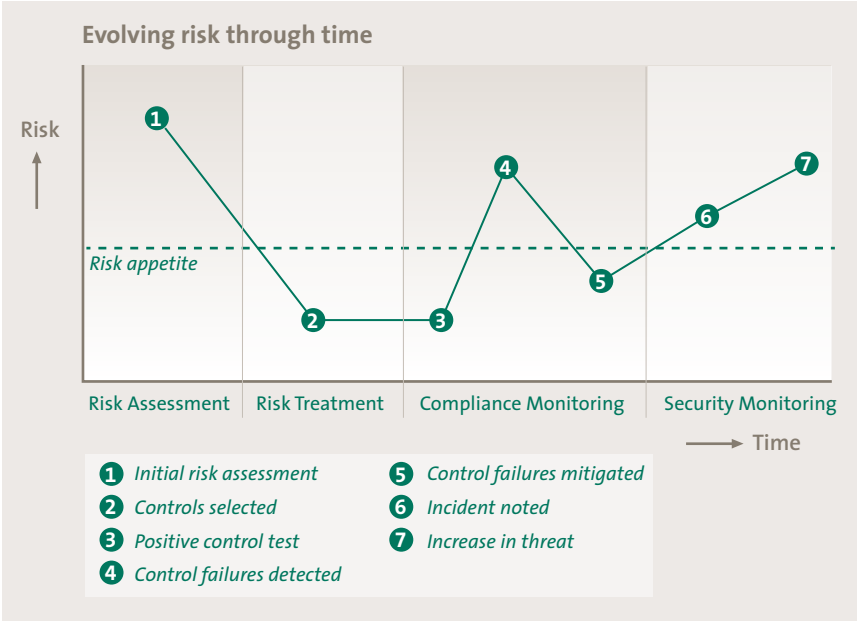

Figure 2. **Evolution of risks.**

to scenario modeling, it would be possible to identify the impact of possible future threats on the risks to IT and to the business.

Risk based, linked with the business

The main objective of the IRM function is to continuously manage information risk and link it to business risk, with the sole purpose of determining the impact on business risk in order to provide dynamic, risk-based protection. In many large organizations Risk Management is limited to Compliance Management, i.e. reporting on the percentage of controls that are effective. However, business is crying out for insight into Risk! If controls fail, what does it mean for my business? The level of compliance as a figure on its own is not informative. In the 2020 vision, the risk manager is able to report on risk instead of compliance. More importantly, the risk manager is able to report on business risks, because threat categories in the IT-domain are linked to business processes.

Risk appetite

The risk manager of 2020 has an updated overview of risk appetite. The risk appetite is set by the business, as a measure of the level of risk the business is willing to take. When risk levels rise above the threshold of tolerance, action is taken to reduce the level of risk, either by initiating controls or by implementing additional measures on the level of the IT-infrastructure. Risk appetite is determined by modeling worst-case scenarios, which help the business imagine possible impacts. Risk managers can select and present control measures to the business, immediately showing the business what the effect of implementing them would be on the risk level. Both the effect on the risk level and the cost of the control measures is set out. In this way it is possible to find the optimum balance between risk reduction and increased cost levels.

Rationalized remediation

Since the IRM manager can pinpoint risks, and what the sources of the risks are, it is possible to remediate only in the areas where risks rise above accepted levels. In essence, it is not necessary to remediate compliance failures by default, just because a control has failed. Also, it might not be necessary to act on increased threat levels, as long as the risk levels remain below what is acceptable to the organization. Of course, spending money to remediate is not just based on compliance failures. It is also based on projections, emerging threats and so on. By extrapolating current trends, it is possible to make well-balanced investment decisions.

Overlooking the risk chain

In the hyper-connected world we live in, there is a need for looking beyond our own familiar boundaries. Depending on the relationship, partners in joint ventures and third-party suppliers can have a huge impact on a company's data flows . A well-accepted risk level in our own organization might rise sky-high when security at a third-party data communications provider is found to be not up to specs. In the risk management processes of 2020, there should be a link with the risk management processes of our business partners. The same risk assessment processes would be used, making it easy to obtain risk levels from our vendors and link them to our risk levels. The drill-down capability mentioned earlier in "Dynamic reporting" could identify a specific vendor as the source of an increased risk.

Needed Structure and Key Capabilities for the IRM Function in 2020

In order to continuously manage and mitigate the information risks, the organization needs to be able to address these risks in a flexible and ongoing manner. This requires a central and overarching perspective on those risks that require management attention. An emerging threat landscape, a change in business activities, and a shift to using new technologies: these are all indicators that the risk landscape is changing. So far IRM methodologies and IRM models have not been able to capture this, in practice, in a dynamic way. For IRM practice to be able to provide a real-time and accurate view of the current risk environment would be the next step in the maturity of IRM.

The major elements in the 2020 vision are:
a real-time view of actual IRM risks that provides senior management with insight into the risks that exceed the organization's risk appetite and require attention. The risk view is an integral part of the business, and is aligned with enterprise risk management. IRM is able to assign resources to the risks that matter in an agile way, and is able to provide business opportunities.

Combining the earlier mentioned "wish list," the IRM function of 2020 would look like Figure 3, outlining the required key capabilities. These key capabilities will be explained further in this article.

Key Capability 1: Integrated, standardized IRM processes, linked together by the Risk Register

In the center, we see the *four core IRM risk processes*, in effect:

- Risk Assessment – the process of performing risk assessment;
- Risk Treatment – the process of controls selection and implementation, or determining other treatment options, including risk acceptance or avoidance;
- Compliance Monitoring – the process of control compliance monitoring;
- Security Monitoring – the process of incident response and surveillance, threat and vulnerability management.

The four core IRM processes must be fully standardized across the organization. They must also be integrated via a Risk Register and by using automated processes to perform IRM with extensive workflow mechanisms. Integration also means that newly identified threats will feed the risk assessment process, making the risk register a dynamic system.

The IRM function ensures all information risks are monitored, identified and handled as part of regular business processes. The concept of a Risk Register plays a crucial role in this model: it acts as the heart of information risk management, where all risks are listed as they are input

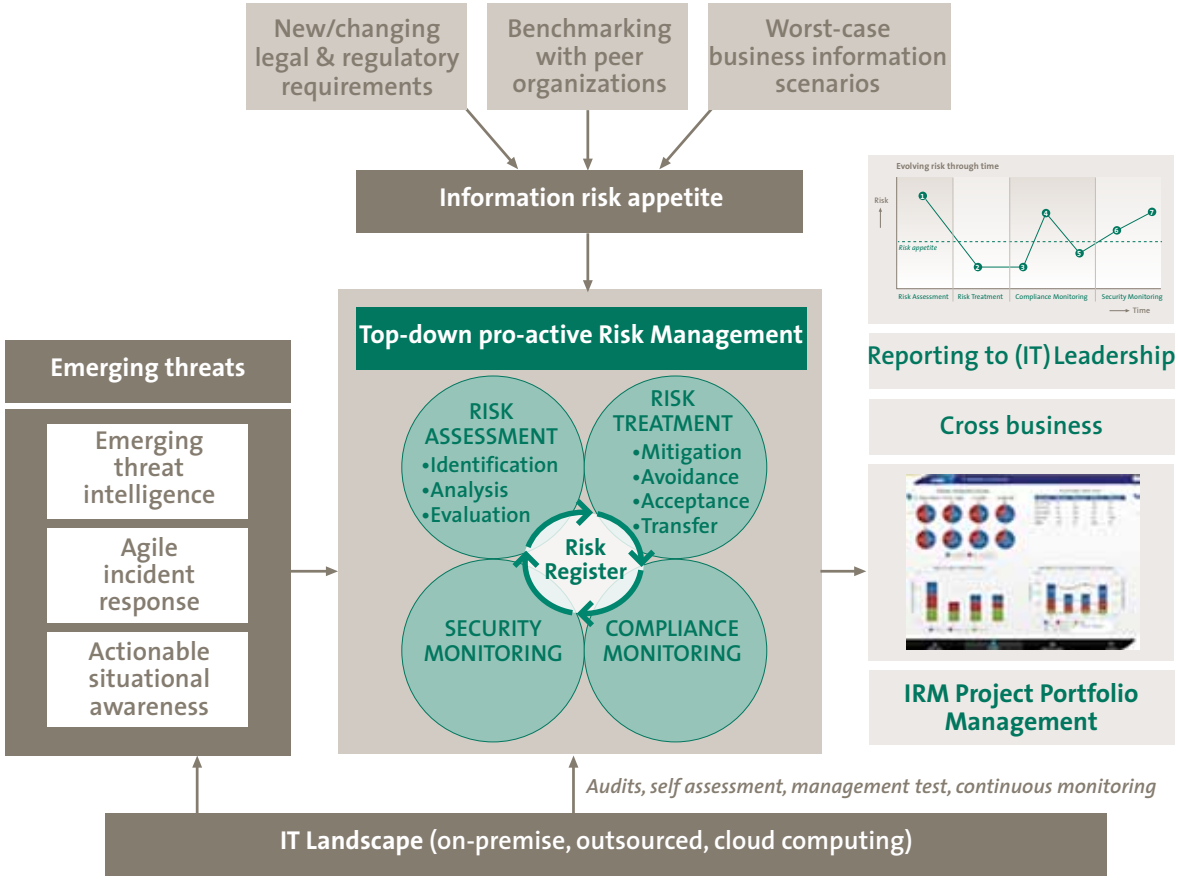

Figure 3. **Key capabilities of IRM.**

from the IRM processes, and where the strategy of managing relevant risks comes together. Based on the information in the Risk Register a real-time view of the risk status can be provided (both within the IRM function and also outside of the function) to stakeholders in the business and to IT management.

One important prerequisite is having a uniform approach to Risk Management throughout the entire organization. In large organizations there might be multiple IRM staff who all need to adopt the same methodology to achieve comparable risk results. Clear governance needs to be in place to enforce this.

Key Capability 2: Top-down, proactive Risk Management – determining the risk appetite

Linking to enterprise risk management

IRM must be part of the business context and must be fully aligned with business goals and needs. Only then will IRM be able to show its added value by providing insight into business opportunities and risks that should be avoided. To be able to show the added value of the IRM function, the IRM risks need to be mapped or linked to business risks (or "enterprise risk management"). This enables a top-down approach where IRM and ERM are aligned instead of existing in two separate worlds.

This brings us to another important prerequisite: asset management. Since there is an undeniable relationship between business processes, applications and infrastructure, it is necessary to define these relationships, so that risks on the infrastructure level can be linked to specific business processes. This is not going to be easy to accomplish.

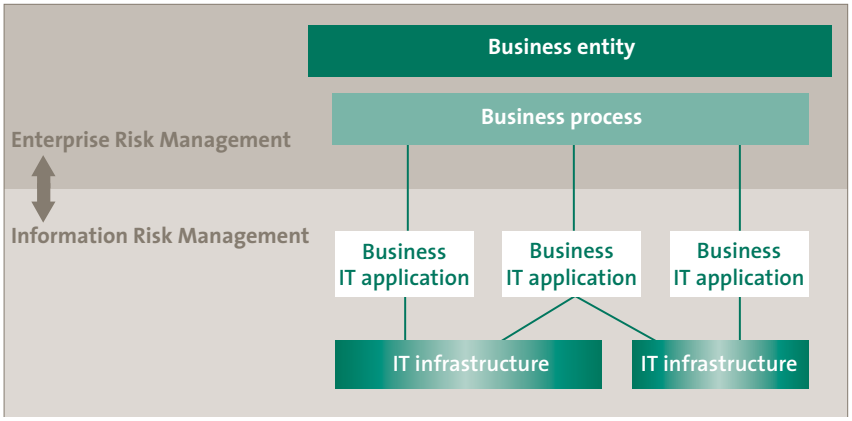

Figure 4. **Alignment of IRM and ERM.**

Using worst-case business information scenario planning to determine the information risk appetite

In many organizations it is a common "Pavlovian response" to immediately start drafting and implementing controls when a risk is identified, without asking what level of risk is acceptable. These decisions are often made, although with all good intentions, by IRM professionals without consultation with the appropriate business representatives.

In the IRM 2020 world, business representatives will identify the level of risk they are willing to take (risk appetite), which allows for risk management in the most efficient and economical way possible.

This requires a sound and structured process to define the risk appetite of the business, by using the technique of worst-case business information scenario planning. This process must translate the risk appetite into discrete levels of acceptable risk, taking into account factors like changing business models, new and/or changing legal and regulatory requirements, as well as emerging IRM industry standards.

Key Capability 3: Bottom-up continuous compliance testing / monitoring

Compliance testing / monitoring is also an essential function of IRM 2020. Whether it is monitoring for specific regulatory requirements, for internal control, or for certification reasons, organizations are used to testing typical controls. In the world of IT auditing, the results of controls monitoring are binary: either the control is operating effectively or it is not. Knowing the results from controls monitoring helps managers verify and approve current protocols, and it also provides valuable insight into whether, in practice, risks are being effectively mitigated or not. Where control failures are identified, the risk is apparently not being effectively mitigated.

In the IRM 2020 world, we will have extensive and continuous compliance monitoring, using sophisticated tools. This continuous compliance monitoring will enable an organization to have nearly real-time view on the compliance level of IT assets. Of course, IT assets that require continuous monitoring will not be limited to those within the boundaries of the organization. Some IT assets will be outsourced to managed services providers or cloud providers, and some will be managed by the organization's business partners.

Bottom-up real-time insight into risk shows the heartbeat of Risk Management

Key Capability 4: Anticipating emerging threats

Threats – changes in the threat landscape affect risk levels

A hot topic in the media these days is cyber attacks. It is almost impossible not to have noticed the increase in external threats sometimes called cyber crime or even cyber warfare. Organizations should be careful of believing too readily in media hype, on the one hand; but on the other hand, they should not be blind to the fact that cyber-related threats are emerging.

These threats are a factor in determining risk levels, but the actual threat is difficult to assess with a mathematical accuracy. These threats are external, and it is difficult to estimate the threat level. There are, however, several sources that can determine changes in threat levels. Scientific reports on natural disasters, internal data on IT equipment theft, and cyber intelligence reports from governmental institutes are just a few examples of sources that can provide insight into the decrease or increase of a threat level. It is important to include a threat-management process in the IRM function, as an increase or decrease in the threat level might mean that an organization's response is no longer appropriate (either too much or too little is being done to mitigate the threat).

Changes in threat levels often focus on cyber-related areas, such as hacking and espionage. Although this area is seeing the highest degree of change, it should not be forgotten that other threats are also subject to change. In the IRM 2020 model, threat intelligence is considered to include all areas of threat management.

Vulnerabilities – findings have impact on risk levels

In recent years the focus has been on identifying vulnerabilities in the IT environment, especially within the IT infrastructure. Ethical hackers identify numerous technical vulnerabilities in IT systems through performing penetration tests. In addition, automated tooling performs scanning activities with even more (negative) results. Apart from the obvious response (fix the vulnerabilities), these results should be assessed to determine whether these vulnerabilities affect the risks documented in the Risk Register.

This poses a challenge for the security professionals, as the identified vulnerabilities cannot be related one by one to specific risks. It is not uncommon that an ethical hacker or penetration test discovers several hundred vulnerabilities. Therefore it's necessary to translate from individual vulnerabilities to categories of vulnerabilities on the level of risks. In this way discovering vulnerabilities leads to an increase in the risk level. As long as the adjusted risk level does not exceed the risk appetite level, no direct action is required.

There is a critical consideration that is easy to forget here. Performing penetration tests or other scanning activities results in discovering vulnerabilities in the selected areas, while other areas not subject to the test might appear to be safe. It is therefore important to be able to extrapolate the results of testing in one area to other areas, when there is sufficient similarity to support comparison. This might mean that a vulnerability category is adjusted over a range of assets, although not all these assets have been tested.

Incidents – analysis leads to understanding threats and vulnerabilities

As indicated by an ISF report in September 2012 ("You Could Be Next: Learning from incidents to improve resilience, ISF 2012"), incident response is an often overlooked area. The ISF report even states that Risk Management is incomplete without post-incident review. An information risk management incident is the exploitation of an existing vulnerability by a threat. Vague definitions, such as provided by ITIL ("Information security incidents are those events that can cause damage to confidentiality, integrity or availability of information or information processing") do not help much. In practice a distinction is often made between an event of interest (EoI) and a security incident, where the EoI can, but not necessarily will, lead to an incident. Organizations are inclined to solve incidents as quickly as possible to be able to get back to normal operation. This is not surprising: the controls that have been implemented to mitigate the risk have failed, and the risk of an incident occurring has become reality. However, security incidents should be carefully analyzed for the underlying problem (also known as the root cause), as this might indicate a structural failure among controls, a general increase in vulnerabilities, or an increase in a threat. This information must be captured and incorporated into the central Risk Register to be able to determine changes in the risk posture.

Key Capability 5: Risk quantification to compile extensive risk dashboarding and steer to sustainable IRM investments

Small business environments might benefit from a qualitative approach where risks are categorized and described in a few paragraphs. Providing senior management with insight into the risk posture requires a risk manager to analyze the risks and aggregate them into a high-level report.

However, in large-scale IT environments with hundreds of applications, multiple networks and various sites, this approach would take months, and the aggregated report would consist of hundreds of pages.

To solve this, large organizations move from a purely qualitative risk management approach to a more quantified approach. This requires some more explanation. Risk Quantification as a financial instrument that provides exact, numerical values on impact and likelihood is a common method in the financial services industry. Insurance companies have a huge amount of historical data on the chance that an event will occur and the average cost of this occurrence. Depending on how much risk the company is willing to take, it can calculate the insurance fee that it will charge for its product. Due to the large volumes of data, these calculations have a relatively high degree of accuracy. Individual deviations will be relatively few and will be compensated for within the largely predictable insured population.

Risk Management Fundamentals

- Risk Management should, ideally, take inventory of threats and probabilities, producing an overview of the risks sorted from highest to lowest, so that the most invasive risks are handled first. It should monitor the mitigating controls and/or actions, in order to ensure that identified risks are correctly handled by the organization.
- Risk = Threat × Vulnerability × Impact. There is no one single risk. Risk is always related to a threat. If there are 50 relevant threats (or threat categories) identified, this would result in 50 risks (the ISF standard of good practice (2012) identifies 39 Threat Categories).
- For the initial set-up of a solid risk management process, this standard details the following stages:
  - Context establishment: understanding the business environment you are operating in. This helps to value the impact of certain threats, were they to occur. It also helps you to identify the right threats in the first place.
  - Risk assessment: identifying threats, estimating vulnerability and impact.
  - Risk treatment: implementing measures to mitigate risk, to monitor, to plan, and to act.

Regarding information risk management, this quantification is not supported by hard figures that make it possible to quantify risks. However, the IRM function needs a uniform method to quantify risk. If risk is defined as the result of Threat level, Vulnerability level and Impact level, then IRM needs a method to assign numbers to these levels. This will be one of the most challenging aspects of IRM in the coming years. To make it even more challenging, the levels constantly change, due to increased threat assessments, compliance failures, or newly discovered vulnerabilities or re-assessed impact levels.

The risk quantification, feeding the risk register, will also allow managers to steer towards sustainable IRM improvement programs. Based on the risks in the Risk Register, a project portfolio plan can be drafted to identify projects and programs that aim at improving the risk treatment in a sustainable way. With this intelligence, organizations can spend their resources on those risks that matter, resulting in a rationalized risk remediation.

Conclusion

Even though the IT landscape has changed dramatically since the '60s and '70s, IRM methodologies have not changed all that much. True, IRM processes have successfully identified new risks arising in our current environment, but the process and the tooling that is used to achieve this is largely unchanged . Accurate and timely insight into Risk Levels is still hard to achieve, but under the right circumstances it is definitely achievable.

This article mentioned the key capabilities that are needed to realize the potential of the 2020-IRM manager. Inspired by Martin Luther King's famous speech "I have a dream," we should be looking forward to these possibilities, instead of only running behind and fixing the disasters after the fact. In large organizations it will be possible that the person who is ultimately accountable for risk management has a real-time overview of current risks, aggregated to a comprehensive level. Exceeding tolerable thresholds will automatically lead to alerts, where it will be possible to drill down to the harmed asset(s) or business entities and identify the localized problem. Designing new projects or programs will be facilitated by simulating threats or overruns, to better defend against malicious entities or spontaneous events.

Realizing these possibilities requires a structural approach, starting with embedding the key capabilities mentioned earlier and knowing where you are heading. By determining how far you are from the goal, you can design a program to go forward and attain that goal. As always, without change there is no progress.

References

ISF report September 2012: "You could be next, learning from incidents to improve resilience."

ISO/IEC 27001:2005 Information security management systems.

ISO/IEC 27005:2011 Information security risk management.

The Standard of Good Practice for Information Security (ISF 2012).

About the authors

J. A.M. Hermans is partner at KPMG Advisory N.V. He heads the Information Security Services of KPMG in the Netherlands, focusing on topics such as IT-GRC, Cybersecurity, Cloud Computing and Identity & Access Management. He has worked for numerous organizations in most industry sectors, such as Financial Services, Oil & Gas, Government and others, and was involved in more than 100 national and international information security projects around the world. His major involvements were in assisting clients in their strategy, building the business cases and performing program management activities as well as quality assurance activities.

A.C. van der Harst is a director at KPMG Advisory N.V. He has 15+ years' experience in the field of IT Audit (RE), project management (Prince2 Practitioner), information security and support of Financial Statement Audits. He has specific experience in risk management, controls design and embedding, minimizing the "control burden" and creating capabilities for monitoring compliance on an ongoing basis. Main clients are in the fields of Oil & Gas, Building and Construction, and the engineering-to-order businesses.

P.R. de Meijer is a manager at KPMG Advisory N.V., specializing in Information Protection and Business Resiliency, and IT audit. He has been involved in several assignments concerning information security and security-related controls. He performed these assignments both as an auditor and an advisor, and is a certified ISO 27001 auditor as well as a certified ISO 27005 Risk Manager. He has experience in Information Security engagements in both the private as well as the public sector, with a focus on the Oil & Gas, and Building and Construction sectors. In addition to his focus on information risk management, he is managing KPMG's global COBIT IT Assessment tool.

S.R. Verkaart is a manager working at KPMG Advisory N.V. He joined KPMG in 2004 to work in IT audit and advisory practice. In the past years he has built up experience in a number of areas: IT Attestation engagements based on international standards ISAE 3000 and ISAE 3402, IT project ERP implementation reviews and quality assurance roles, and set-up and audit of Information Security control frameworks based on industry standards COBIT and ISO27001. He has specific experience in the field of developing and evaluating business process and IT controls required to meet business objectives. His focus is mainly on clients in the Oil & Gas, Energy, Construction and Communications sectors.