Providing Audit Committee Guidance

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2OpjOiT

It has been largely overshadowed by the EU General Data Protection Regulation (GDPR), but the Directive on Security of Network and Information Systems (NIS Directive) has been transposed into law in many European countries.[1] The NIS Directive is the first EU-wide legislation on cybersecurity. The objective of the directive is to achieve a uniformly high level of security of network and information systems across the European Union, through:[2]

- Improved cybersecurity capabilities at the national level
- Increased EU-level cooperation
- Risk management and incident reporting obligations for operators of essential services and digital service providers

Essential services are defined as energy, transport, banking, financial market infrastructures, healthcare, water and digital infrastructure (e.g., top-level domain name registries). Digital service providers are defined as online marketplaces, cloud computing services and search engines.

However, despite the transposition of the directive, there is no requirement for the board members of the operators of essential services or digital service providers to have IT or cybersecurity experience. So what is to be done? Indeed, what can be done for any enterprise where the IT-related risk factors are significant, but the board's experience maybe lacking? I believe it is incumbent on IT audit to educate or, at least, to offer to educate the board in this regard.

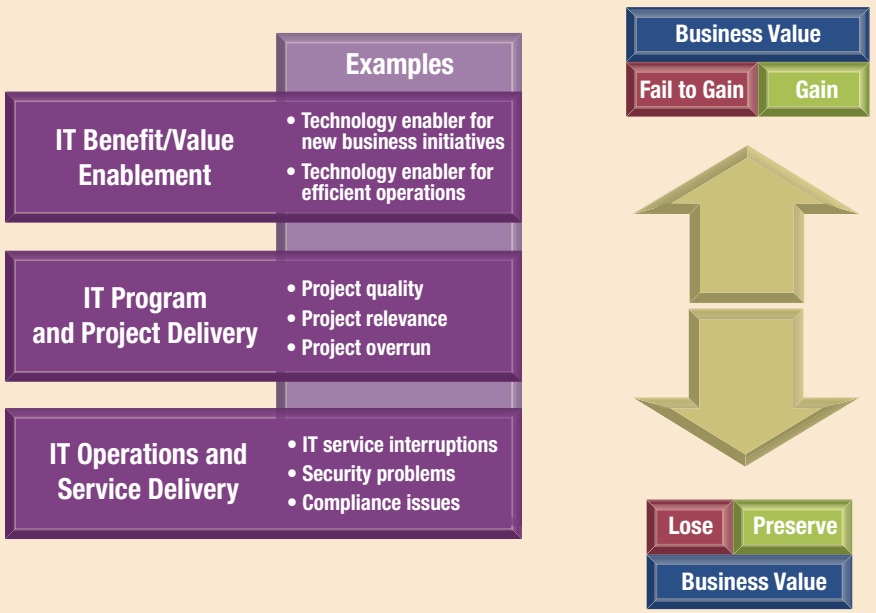
Provide an Overview of IT Risk

IT risk can be categorized (**figure 1**) as:[3]

- **IT benefit/value enablement risk**—Associated with missed opportunities to use technology to improve efficiency or effectiveness of business processes or as an enabler for new business initiatives

Ian Cooke, CISA, CRISC, CGEIT, COBIT Assessor and Implementer, CFE, CIPM, CIPP/E, CIPT, CPTE, DipFM, FIP, ITIL Foundation, Six Sigma Green Belt
Is the group IT audit manager with An Post (the Irish Post Office based in Dublin, Ireland) and has 30 years of experience in all aspects of information systems. Cooke has served on several ISACA® committees and is a past member of ISACA's CGEIT® Exam Item Development Working Group. He is the topic leader for the Audit and Assurance discussions in the ISACA Online Forums. Cooke supported the update of the CISA® Review Manual for the 2016 job practices and was a subject matter expert for the development of ISACA's CISA® and CRISC™ Online Review Courses. He is the recipient of the 2017 John W. Lainhart IV Common Body of Knowledge Award for contributions to the development and enhancement of ISACA publications and certification training modules. He welcomes comments or suggestions for articles via email (Ian_J_Cooke@hotmail.com), Twitter (@COOKEI), LinkedIn (*www.linkedin.com/in/ian-cooke-80700510/*), or on the Audit and Assurance Online Forum (*engage.isaca.org/home*). Opinions expressed are his own and do not necessarily represent the views of An Post.

Figure 1—IT Risk Categories



Source: ISACA®, *COBIT® 5 for Risk*, USA, 2013, figure 5. Reprinted with permission.

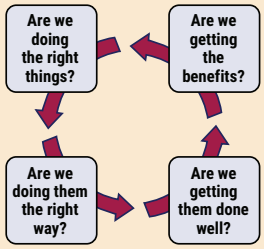
- **IT program and project delivery risk**—Associated with the contribution of IT to new or improved business solutions, usually in the form of projects and programs as part of investment portfolios
- **IT operations and service delivery risk**—Associated with all aspects of the business as usual performance of IT systems and services, which can bring destruction or reduction of value to the enterprise

Another good reference is the Four Ares (**figure 2**).[4] I remember watching in awe as the late Rob Stroud presented on this at EuroCACS in Vienna in 2007 and thinking, "That's it! IT audit has been summed up using four questions." The Four Ares are intended to help manage IT benefit/value enablement risk, but if one considers the questions independently, they are quite insightful. They are great questions for any board member to ask management about any IT initiative or risk.

Figure 2—Four Ares

The strategic question. Is the investment:
- In line with our vision
- Consistent with our business principles
- Contributing to our strategic objectives
- Providing optimal value, at affordable cost, at an acceptable level of risk

The architecture question. Is the investment:
- In line with our architecture
- Consistent with our architectural principles
- Contributing to the population of our architecture
- In line with other initiatives



The value question. Do we have:
- A clear and shared understanding of the expected benefits
- Clear accountability for realising the benefits
- Relevant metrics
- An effective benefits realisation process over the full economic life cycle of the investment

The delivery question. Do we have:
- Effective and disciplined management, delivery and change management processes
- Competent and available technical and business resources to deliver:
  - The required capabilities
  - The organisational changes required to leverage the capabilities

Source: IT Governance Institute, *The Val IT Framework 2.0*, USA, 2008. Reprinted with permission.

Enjoying this article?

- Read *Getting Started with Risk Management. www.isaca.org/Getting-Started-With-Risk*
- Learn more about, discuss and collaborate on audit and assurance ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Explain the Purpose of Data Classification

All readers of this column will likely be familiar with the concept of data classification and the advantages of same.[5] However, this should be stressed to the audit committee. All data are not created equal, resources are limited and the purpose of performing a data classification is to ensure that the right resources are allocated to the right areas.

Link the Risk Register(s) to the IT Risk Types

If the organization has an enterprise or IT risk register, select the top-five or six IT risk factors (**figure 3**) and, where possible, link them back to the IT risk types as described previously. This will help put the risk in context and reinforce why, for example, a project overrun can affect business value. In addition, if competitors or peer organizations have published their risk scenarios, these should also be reviewed. The purpose is to demonstrate that the enterprise is considering and dealing with similar IT risk. If the risk scenarios are not similar, new or emerging risk may be gleaned from the review.

Explain How Management Manages the IT Risk Scenarios

Next, a high-level overview of the first line management controls[6] should be provided at risk type level or by using the risk scenario categories to provide more concrete examples (**figure 4**). They should include:

- Who is accountable?
- The response to the risk
- Where appropriate, the importance of data classification

List the Independent Sources of Assurance to Mitigate the Identified Risk

An overview of the second and third line functions[7] can provide independent assurance for each risk type (**figure 5**). If the internal audit function does not provide assurance for one or more of the risk types, it should be stressed here. The audit committee should be aware that this information is available to them (if required) and that the enterprise is relying solely on the second-line function.

Figure 3—Sample Risk Scenario Categories by Risk Type

Risk Type	Sample Scenario Category and Risk
IT benefit/value enablement risk	1. Portfolio establishment and maintenance • Selected programs are misaligned with enterprise strategy and priorities. • There is duplication between initiatives.
	2. IT investment decision-making • Business managers are not involved in important IT investment decision-making. • Redundant software is purchased.
IT program and project delivery risk	3. Program/projects life cycle management • Failing projects are not terminated. • There is an IT project budget overrun. • There are excessive delays in outsourced IT development projects.
	4. IT expertise and skills • There is a lack of or mismatched IT-related skills within IT. • There is an inability to recruit IT staff. • There is a lack of training leading to IT staff leaving.
IT operations and service delivery risk	5. Information (data breach: damage, leakage and access) • Sensitive data is lost/disclosed through cyberattacks. • Sensitive information is disclosed through email or social media.
	6. Supplier (selection/performance, contractual and compliance) • There is a lack of supplier due diligence. • Support and services delivered by vendors are not in line with the service-level agreement (SLA).

Source: Modified from ISACA, *Risk Scenarios Using COBIT® 5 for Risk*, USA, 2012, figure 14. Reprinted with permission.

Figure 4—Sample IT Risk Responses	
Sample Scenario Category	**Sample Responses**
1. Portfolio establishment and maintenance	Program and project management office (PMO) Enforce the use of an overall program/project methodology including corporate policy on business case or due diligence.
2. IT investment decision-making	Chief information officer (CIO)/business managers Implement a policy that defines who needs to be involved in investment decisions and the chain of approval.
3. Program/projects life cycle management	Program and PMO Ensure that the true project status is available for decision-makers using common language and methodology.
4. IT expertise and skills	CIO Have a policy for developing, selecting and evaluating IT profiles throughout the entire career.
5. Information (data breach: damage, leakage and access)	IT operations Implement an information security policy approved by the chief information security officer (CISO) (and based upon data classifications) that defines limitations on sharing and using information.
6. Supplier (selection/performance, contractual compliance, termination of service and transfer)	CIO/procurement Implement a procurement policy that provides a formal approach to selecting suppliers including the acceptance criteria by the business.

Source: Modified from ISACA, *Risk Scenarios Using COBIT® 5 for Risk*, USA, 2012, figure 14. Reprinted with permission.

Figure 5—Source of Assurance	
Risk Type	**Sample Source of Assurance**
IT benefit/value enablement risk	• Risk management • Financial control • Compliance • Internal audit
IT program and project delivery risk	• Risk management • Compliance • Internal audit
IT operations and service delivery risk	• IT security • External audit • International Organization for Standardization (ISO) auditor • Payment Card Industry Data Security Standard (PCI DSS) Qualified Security Assessor (QSA) • Privacy office • Compliance • Quality • Suppliers • Internal audit

Figure 6—Sample IT Risk and Assurance Available	
Sample Scenario Category	**Assurance Available**
1. Portfolio establishment and maintenance	• PMO management reports • Risk management reports • Compliance management reports • External reviews • Internal audit reviews
2. IT investment decision-making	• Business cases, the cost and return on investment of IT initiatives (business managers or representatives) • Risk management reports • Compliance management reports • External reviews • Internal audit reviews
3. Program/projects life cycle management	• Program and project status reports (PMO) • Risk management reports • Compliance management reports • External reviews • Internal audit reviews
4. IT expertise and skills	• Human resource reports • External reviews • Internal audit review
5. Information (data breach: damage, leakage and access)	• IT management reports or presentations • Partner reviews • ISO 27001—*Information Security Management Reports* (ISO auditor) • Cloud Security Alliance (CSA) Consensus Assessments Initiative Questionnaire (CAIQ) (cloud suppliers) • CSA Cloud Controls Matrix (CCM) Report (cloud suppliers) • PCI DSS Reports (QSA) • Service organization controls (SOC) reports (suppliers) • US Privacy Shield • Privacy office reports • Internal audit reports • External audit reports
6. Supplier (selection/performance, contractual compliance, termination of service and transfer)	• Procurement management reports or presentations • ISO 27001—Certifications • CSA CAIQ (cloud suppliers) • CSA CCM Report (cloud suppliers) • PCI DSS Certificate of Compliance • SOC reports (suppliers) • US Privacy Shield • Internal audit reports • Service levels • Questionnaire responses, attestations (suppliers)

Provide Mapping Between the Identified Risk and the Assurance Available

Finally, a mapping of the identified risk and the assurance available from all three lines of defense is next (**figure 6**). The assurance items in the figure are rather generic because it is only an illustration of where they come from; however, they should be as specific as possible. Internal audit reviews are included for each example; however, as previously noted, this may not be the case in every enterprise. The committee should be made aware of this should it become part of the IT audit plan,[8] or are they happy to rely on the assurance provided?

This mapping is key and why we have taken the time to build to this stage. The committee should be made aware of the importance of the assurance

provided. For example, the International Organization for Standardization (ISO) standard ISO 27001 provides assurance over the Information Security Management System (ISMS) and may also be a key business enabler—other enterprises require it before they do business. The committee should, therefore, understand that when the internal audit report in front of them says that application A is not in compliance with ISO 27001, that this is something they should question.

Conclusion

I am aware that in more mature enterprises much, if not all, of the information discussed here will be available in a risk register. Nonetheless, audit committee members are typically busy people and, unless IT experience is mandated, are often generalists. By drawing a line between accepted IT risk types, the importance of data classification, the information available and the assurance provided by internal audit, the committee should be in a position to take the next generation of IT risk (e.g., the NIS directive), categorize them and understand the likely sources of assurance. The committee members should be able to understand the answers when they ask, are we doing the right things? Are we doing them the right way? Are we getting them done well? Are we getting the benefits? And I strongly believe that this can only help internal audit.

Endnotes

1 European Commission, State-of-Play of the Transposition of the NIS Directive, Belgium, 2018, *https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive*

2 European Commission, "Questions and Answers: Directive on Security of Network and Information Systems, the First EU-Wide Legislation on Cybersecurity," Belgium, 2018, *http://europa.eu/rapid/press-release_MEMO-18-3651_en.htm*

3 ISACA®, *COBIT® 5 for Risk*, USA, 2013, *www.isaca.org/COBIT/Pages/Risk-product-page.aspx*

4 IT Governance Institute, *The Val IT Framework 2.0*, USA, 2008, *www.isaca.org/Knowledge-Center/Val-IT-IT-Value-Delivery-/Pages/Val-IT-Publications.aspx#framework*

5 Cooke, I; "Doing More With Less," *ISACA® Journal*, vol. 5, 2017, *https://www.isaca.org/archives*

6 Institute of Internal Auditors, *The Three Lines of Defense in Effective Risk Management and Control,* USA, 2013, *https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf*

7 *Ibid*.

8 Cooke, I.; "Defining the IT Audit Plan Using COBIT 2019," *ISACA Journal*, vol. 3, 2019, *https://www.isaca.org/archives*