Auditing Cybersecurity

There are several rites of passage one goes through on the way to becoming an experienced IT auditor. After completing college, one gets a job, although not necessarily in audit. After a while, audit attracts and so one moves into the area and sits and passes the Certified Information Systems Auditor® (CISA®) exam. One then works as part of an audit team before finally progressing to performing solo IT audits. As a practitioner becomes more experienced, he or she will (hopefully) lead a team and become an IT audit director.

However, in recent years, something additional has been added to the rite of passage. Increasingly, IT auditors are being asked to audit cybersecurity. I say increasingly because when I moved into IT audit in 2005 the term was not commonly used.[1] We just audited plain old IT security. Now, it is probably one of the first items in an enterprise's audit universe.

So, what is cybersecurity and how do we audit it? We will, once again, turn to the ISACA® white paper on creating audit programs.[2]

Determine Audit Subject

The first thing to establish is the audit subject. What does cybersecurity mean in the enterprise? ISACA defines cybersecurity as "the protection of information assets by addressing threats to information processed, stored and transported by internetworked information systems."[3] This is quite a wide definition.

In fact, the cybersecurity audit universe includes all control sets, management practices, and governance, risk and compliance (GRC) provisions in force at the enterprise level. In some cases, the extended audit universe may include third parties bound by a contract containing audit rights.[4] Boundaries and limitations to consider for cybersecurity audits include[5]:

- **Corporate sphere of control vs. private sphere of control**—In most enterprises, end users may engage in activities that are only partially covered by the business purpose. This includes the use of private IT devices and nonstandard applications.
- **Internal IT infrastructure vs. external infrastructure**—As a rule, the use of IT extends beyond the internal organizational network, as in traveling use, home-use settings or the adoption of the cloud. While this may create additional cybersecurity risk, it has become common practice in most enterprises.

Further, the audit universe may be extended by reliance on the work of others. Examples include information security management system (ISMS) certification reports, International Standard on Assurance Engagements (ISAE) ISAE 3402 reports or published regulatory review results. IT auditors should identify and categorize audit areas where reliance on the work of others makes sense.[6]

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/2TpXljK

Ian Cooke, CISA, CRISC, CGEIT, COBIT Assessor and Implementer, CFE, CIPM, CIPT, CPTE, DipFM, 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 practice 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.

The key is to consider the cybersecurity-related areas in the enterprise and to determine the audit subject(s). One needs to answer the key question: What is being audited? Given the depth and breadth of the subject matter, it may also be worth creating multiple, individual audit universe items.

Define Audit Objective

Once what is being audited has been decided, the objective of the audit needs to be established. Why is it being audited? From an auditor's perspective, it is advisable to adopt a risk-based view (**figure 1**) and define the objectives accordingly.

The audit objectives should be limited to a reasonable scope and should also correspond to cybersecurity and protection goals as defined by the enterprise (**figure 2**).

Set Audit Scope

Once the objectives for the audit have been defined, the planning and scoping process should identify all areas and aspects of cybersecurity to be covered. In other words, what are the limits to the audit? This could include a specific country, region, division, process area or aspect of cybersecurity. Again, this should be risk based.

Cybersecurity audit scopes are usually more restricted than those for general IT audits due to the higher level of complexity and technical detail to be covered. For an annual or multiyear scope, it is advisable to break down the overall scope into manageable audits and reviews, grouping them by area addressed and by approach.[7]

Perform Pre-Audit Planning

Now that the risk scenarios have been identified (**figure 2**), they should be evaluated to determine their significance. Conducting a risk assessment is critical in setting the final scope of a risk-based audit.[8] The more significant the risk, the greater the need for assurance.

Assurance considerations for cybersecurity have been well documented in the US National Institute for Standards and Technology (NIST) Cybersecurity Framework (CSF).[9] The CSF focuses on using

Figure 1—Cybersecurity Vulnerabilities, Threats and Risk

Vulnerability	Threat	Risk and Impact
Spear phishing	Attackers may gain access through phish payload or combined social-technical follow-up.	Initial data loss or leakage leading to secondary financial and operational impact
Water holing	Attackers may gain control of attractive websites and subsequent control of visitors.	Initial behavioral errors leading to secondary financial and operational impact
Zero-day	Attacks use zero-day exploits to circumvent existing defenses.	Partial or full control of applications and underlying systems/infrastructure leading to secondary operational impact
Excessive privilege	Inside attacks may happen using inappropriate privileges and access rights.	Full and (technically) legitimate control outside the boundaries of organizational GRC; secondary financial, operational and reputational impacts
Social engineering	Attackers exploit social vulnerabilities to gain access to information and/or systems.	Partial or full control of human target(s), subsequent compromise of IT side; secondary impacts on personal/individual well-being
Extended IT infrastructure advanced persistent threats (APT)	Attacks may target the IT infrastructure underlying critical organizational processes.	Full control of infrastructure, risk of extended control, including public infrastructures or business partners
Vendor/business partner exploit	There are attacks on trusted business partners or vendors, compromising key software or deliverables.	Initial attack through organizational IT directed at third parties, with financial, operational and reputational impact

Source: Adapted from ISACA®, *Transforming Cybersecurity*, USA, 2013. Reprinted with permission.

Figure 2—Cybersecurity Goals and Audit Objectives	
Cybersecurity Goal	**Audit Objective**
Emerging risk is reliably identified, appropriately evaluated and adequately treated.	1. Confirm the reliability of the risk identification process.
	2. Assess the risk evaluation process, including tools, methods and techniques used.
	3. Confirm that all risk is treated in line with the evaluation results.
	4. Verify that treatment is adequate or formal risk acceptances exist for untreated risk
Cybersecurity policies, standards and procedures are adequate and effective.	5. Verify that documentation is complete and up to date.
	6. Confirm that formal approval, release and enforcement are in place.
	7. Verify that documentation covers all cybersecurity requirements.
	8. Verify that subsidiary controls cover all provisions made in policies, standards and procedures.
Cybersecurity transformation processes are defined, deployed and measured.	9. Verify the existence and completeness of the transformation process and related guidance.
	10. Verify that the transformation process is implemented and followed by all parts of the enterprise.
	11. Confirm controls, metrics and measurements relating to transformation goals, risk and performance.
Attacks and breaches are identified and treated in a timely and appropriate manner.	12. Confirm monitoring and specific technical attack recognition solutions.
	13. Assess interfaces to security incident management and crisis management processes and plans.
	14. Evaluate the timeliness and adequacy of attack response.

Source: Adapted from ISACA, *Transforming Cybersecurity*, USA, 2013. Reprinted with permission.

business drivers to guide cybersecurity activities and considering cybersecurity risk as part of the organization's risk management processes.[10] One of the strongest features of the CSF is the Framework Core (**figure 3**). This core is a set of cybersecurity activities, desired outcomes and references from industry standards, guidelines and practices.[11]

Figure 3—Functions of the NIST CSF Core				
Identify	**Protect**	**Detect**	**Respond**	**Recover**
Develop the organizational understanding to manage cyberspace risk to systems, assets, data and capabilities.	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.	Develop and implement the appropriate activities to take action regarding.	Ensure appropriate activities to maintain plans for resistance and to restore any capabilities or services that were impaired due to a cybersecurity event.
ASSET MANAGEMENT	ACCESS CONTROL	ANOMALIES AND EVENTS	RESPONSIVE PLANNING	RECOVERY PLANNING
BUSINESS ENVIRONMENT	AWARENESS AND TRAINING	SECURITY CONTINUOUS MONITORING	COMMUNICATIONS	IMPROVEMENTS
GOVERNANCE	DATA SECURITY	DETECTION PROCESSES	ANALYSIS	COMMUNICATIONS
RISK ASSESSMENT	INFORMATION PROTECTION PROCESSES AND PROCEDURES		MITIGATION	
RISK MANAGEMENT STRATEGY	MAINTENANCE		IMPROVEMENTS	
	PROTECTIVE TECHNOLOGY			

Source: National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0*, USA, 2014. Reprinted with permission.

Enjoying this article?

- Read *Evaluating Risk and Auditing Controls*. *www.isaca.org/auditing-cyber-security*
- Learn more about, discuss and collaborate on audit and assurance ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Each defined function, for example, "Identify," is broken down to defined categories, for example, "Asset Management." These, in turn, are broken down to sub-categories, which are mapped to informative references (**figure 4**).

This is powerful, as it allows the IT auditor to focus on areas that may require assurance. For example, if the enterprise under review has successfully implemented International Organization for Standardization (ISO) ISO 27001 *Information security management systems*, there may not be a need to confirm that physical devices and systems are inventoried if one relies on the work completed by the ISO auditor.

Determine Audit Procedures and Steps for Data Gathering

At this stage of the audit process, the audit team should have enough information to identify and select the audit approach or strategy and start developing the audit program.[12] However, the testing steps do need to be defined.

In 2016, ISACA released an audit/assurance program based upon the NIST CSF,[13] which defines testing steps for cybersecurity. As always, audit/assurance programs should be considered a starting point and adjusted based upon risk and criteria that are relevant to the organization being audited. Failure to do so can result in a checklist approach, which can lead to the auditor recommending controls that are not applicable to the organization. This, in turn, can damage the auditor's reputation with the auditee and, ultimately, with senior management.[14] It is, therefore, worth spending the time considering the identified audit objectives and need for assurance (**figure 5**).

Conclusion

Cybersecurity risk affects an organization's bottom line. It can drive up costs and affect revenue. It can harm an organization's ability to innovate and to gain and maintain customers.[15] The proliferation, complexity and, dare one say it, near ubiquity of cyberattacks means that all IT auditors will be required to develop cybersecurity audit capabilities. As a leading advocate for managing this risk, ISACA has made several developments in this area including white papers, an audit program based upon the NIST CSF and a cybersecurity audit certification.[16] All IT auditors should utilize these tools to help protect enterprises from cybersecurity risk.

Figure 4—Sample CSF Core Mapping

Function	Category	Subcategory	Informative References
Identify (ID)	**Asset Management** (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried.	**CIS CSC 1** **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** 7, 8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried.	**CIS CSC 2** **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** 7, 8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped.	**CIS CSC 12** **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are cataloged.	**CIS CSC 12** **COBIT 5** APO02.02, APO10.04, DSS01.02 **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53 Rev. 4** AC-20, SA-9

Source: National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0*, USA, 2014. Reprinted with permission.

Figure 5—Audit Objective to Audit Program Mapping			
Emerging risk is reliably identified, appropriately evaluated and adequately treated.	1	Identify	Asset vulnerabilities are identified and documented.
	2	Identify	Threats, vulnerabilities, likelihoods and impacts are used to determine risk.
	3	Identify	Risk responses are identified and prioritized.
	4	Protect	Protection processes are continuously improved.
Cybersecurity policies, standards and procedures are adequate and effective.	5	Identify	Organizational information security policy is established.
	6	Protect	Organizational information security policy is established.
	7	Identify	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.
	8	Protect	Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).
	9	Protect	Response plans incorporate lessons learned.
Cybersecurity transformation processes are defined, deployed and measured.	10	Protect	Response strategies are updated.
	11	Detect	Impact of events is determined.
	12	Detect	Detected events are analyzed to understand attack targets and methods.
Attacks and breaches are identified and treated in a timely and appropriate manner.	13	Respond	Personnel know their roles and order of operations when a response is needed.
	14	Respond/ Recover	Recovery plans incorporate lessons learned.

Endnotes

1 Merriam Webster, cybersecurity definition, *https://www.merriam-webster.com/dictionary/cybersecurity.* Interestingly, according to Merriam-Webster, the first known use of the term was in 1989.
2 ISACA®, *Information Systems Auditing: Tools and Techniques, Creating Audit Programs,* USA, 2016, *www.isaca.org/Knowledge-Center/Research/Documents/IS-auditing-creating-audit-programs_whp_eng_0316.PDF*
3 ISACA Glossary, Cybersecurity, *https://www.isaca.org/Pages/Glossary.aspx*
4 ISACA, *Transforming Cybersecurity*, USA, 2013, *www.isaca.org/knowledge-center/research/researchdeliverables/pages/transforming-cybersecurity-using-cobit-5.aspx*
5 *Ibid.*
6 *Ibid.*
7 *Ibid.*
8 ISACA, *Audit Plan Activities: Step-By-Step*, USA, 2016, *www.isaca.org/Knowledge-Center/Research/Documents/Audit-Plan-Activities_res_eng_0316.pdf*
9 National Institute for Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, USA, 2018, *https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf*
10 *Ibid.*
11 ISACA, *Implementing the NIST Cybersecurity Framework Using COBIT® 5*, USA, 2017, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Implementing-the-NIST-Cybersecurity-Framework-Using-COBIT-5.aspx*
12 *Op cit* Audit Plan Activities: Step-By-Step
13 ISACA, *IS Audit/Assurance Program, Cybersecurity: Based on the NIST Cybersecurity Framework*, USA, 2017, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cybersecurity-Based-on-the-NIST-Cybersecurity-Framework.aspx*
14 Cooke, I.; "Audit Programs," *ISACA® Journal*, vol. 4, 2017, *https://www.isaca.org/journal/archives*
15 *Op cit*, Framework for Improving Critical Infrastructure Cybersecurity
16 ISACA, Cybersecurity Audit Certificate, *https://www.isaca.org/Education/on-demand-learning/Pages/cybersecurity-audit-certificate-exam-and-certificate-details.aspx*