Auditing the IoT

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/2v5Rm9M

I recently had the honor of being interviewed by ISACA® about my role as an IT auditor as they begin the planning to update the Certified Information Systems Auditor® (CISA®) job practice areas in 2019. At the end of the interview, I was somewhat surprised when I was asked what type of people are attracted to IT audit. When I hesitated, I was asked if they were the "introverted, techie types." Now, I cannot speak for all IT auditors, but I suppose I am.

Certainly, I enjoy technology in all its shapes and forms, including science fiction. I am especially a fan of *Star Trek*, my favorite being *Star Trek: The Next Generation*. However, as an IT auditor, do you ever find yourself watching an episode and wondering, "Who audits that?" Seriously, for example, when Captain Picard[1] asks the replicator[2] for an "Earl Grey, hot," what does "hot" mean? How hot is hot? Does someone validate that it is really Earl Grey?

Of course, the real reason I enjoy *Star Trek* is that it is a predictor of technology. Certainly, the badge communicator, the tricorder,[3] probes, sensors and the replicator predicted the Internet of Things (IoT).[4] Which brings me back to my original question: How do we audit these items?

I must admit I never audited any IoT technologies. I am an experienced auditor, so if I *had* to audit them, I would perform any necessary research and do a reasonable job. However, ISACA's IS Audit and Assurance Standard 1006, Proficiency,[5] requires me to have adequate skills and proficiency and adequate knowledge of the subject matter.

So, what can we do? Another of ISACA's IS Audit and Assurance Standards 1206, Using the Work of Other Experts, requires that IS audit and assurance professionals consider using the work of other experts for the engagement, where appropriate.[6] At EuroCacs 2018, in Edinburgh, Scotland, I attended a session "Auditing the IoT" by R. V. Raghu. Raghu has experience with these technologies, so I reached out to him. Our combined thoughts are framed under the headings of the now familiar ISACA® paper on creating audit programs.[7]

Ian Cooke, CISA, CRISC, CGEIT, COBIT Assessor and Implementer, CFE, 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 community leader for the Oracle Databases, SQL Server Databases, and Audit Tools and Techniques discussions in the ISACA® Knowledge Center. 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), or on the Audit Tools and Techniques topic in the ISACA Knowledge Center. Opinions expressed are his own and do not necessarily represent the views of An Post.

R. V. Raghu, CISA, CRISC
Is director of Versatilist Consulting India Pvt. Ltd. Raghu cofounded Versatilist, which provides consulting, training and auditing services in information security, IT service management, business continuity and enterprise risk management. Raghu has more than 15 years of extensive, hands-on, global experience across various verticals such as engineering; manufacturing; IT; IT-Enabled Services (ITeS); banking, financial services and insurance; chemicals; mining; and telecom. He has provided training, consulting and implementation support for establishing management systems compliant to International Organization for Standardization standards and other frameworks such as CMMI and COBIT®. Raghu is a four-term member of the ISACA Board of Directors. He is a platimun-level member of ISACA and is immediate past president of the ISACA Bangalore Chapter, where he has previously served as director of membership, secretary and vice president.

Determine Audit Subject

The first thing to establish is the audit subject. This is easier said than done as IoT has no universally accepted definition.[8] ISACA has defined IoT as anyone or anything carrying embedded software that enables interaction with other animate or inanimate objects across networks, including the Internet. Interaction entails sharing and processing information to influence decision-making and/or actions with or without human intervention.[9] Examples of commercial or business applications of IoT include:[10]

- Industrial appliances
- Devices for the medical profession
- Devices for agriculture
- Devices and features for the automobile industry

The key is to consider all IoT devices in use at your enterprise and to determine the audit subject(s). You need to answer the key question: What are you auditing?

Define Audit Objective

Once we have decided what we are auditing, we need to establish the objective of the audit. Why are we auditing it? From an auditor's perspective, it is advisable to adopt a risk-based view (**figure 1**) and define the objectives accordingly.

Figure 1—IoT Risk

Risk Category	Examples
Business	• Health and safety • Regulatory compliance • User privacy • Unexpected costs
Operational	• Inappropriate access to functionality • Shadow usage • Performance
Technical	• Device vulnerabilities • Device updates • Device management

Source: Adapted from ISACA, *Internet of Things: Risk and Value Consideration*, USA, 2015. Reprinted with permission.

The technical risk can be further defined as:[11]

- Software updates and patches. The time for a patch to be released may be longer than the typical cycle for non-IoT devices.

- Hardware lifespan. IoT devices have their own life cycle, often with built-in obsolescence. Components such as nonreplaceable batteries in IoT devices require life cycle planning and asset management processes specific to IoT.
- User IDs and passwords to control access either do not exist or are hard coded.
- IoT devices can be hacked quickly but take days or weeks to rectify. The wider consequences remain unknown because it is difficult to know what has been seen, modified or stolen.
- Cybercriminals can plant back doors for future automated attacks in or from IoT devices; typical attacks include botnet distributed denial-of-service (DDoS) attacks.
- Hackers can use IoT devices as an entry point to an enterprise's networks.
- Hacking smart heating, ventilation and air conditioning (HVAC) systems and energy meters can destroy critical infrastructure by jamming and manipulating controls.

Set Audit Scope

When the objectives of the audit have been defined, the scoping process should identify the actual IoT devices that need to be audited. In other words, what are the limits to the audit? This is easier said than done, as the devices are not just the sensors and include supporting infrastructure such as the connectivity and data collection methods, the cloud or other storage means, and the algorithms used for processing the data.

> “IT IS IMPORTANT TO REITERATE THAT IOT HAS NO UNIVERSALLY ACCEPTED DEFINITION; THEREFORE, THERE ARE NO UNIVERSALLY ACCEPTED STANDARDS FOR QUALITY, SAFETY OR DURABILITY.”

Perform Pre-Audit Planning

Now that the risk scenarios have been identified, they should be evaluated to determine their significance. Conducting a risk assessment is critical in setting the final scope of a risk-based audit.[12] Assurance considerations for the IoT include:[13]

- How will the device be used from a business perspective? What business processes are supported and what business value is expected to be generated?
- What is the threat environment for the device? What threats are anticipated and how will they be mitigated?
- Who will have access to the device and how will their identities be established and proven?
- What is the process for updating the device in the event of a published attack or vulnerability?
- Who is responsible for monitoring for new attacks or vulnerabilities pertaining to the device? How will they perform that monitoring?
- Have all risk scenarios been evaluated and compared to anticipated business value?
- What personal information is collected, stored or processed by the IoT devices and systems?
- Do the individuals about whom the personal information applies know that their information is being collected and used? Have they given consent to such uses and collection?
- With whom will the data be shared/disclosed?

Finally, the auditee should be interviewed to inquire about activities or areas of concern that should be included in the scope of the engagement.

Determine Audit Procedures and Steps for Data Gathering

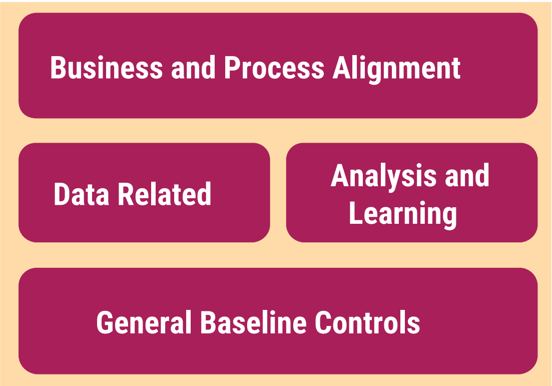
At this stage of the audit process, the audit team should have enough information to identify and select the audit approach or strategy and start developing the audit program.[14] However, the testing steps do need to be defined.

It is important to reiterate that IoT has no universally accepted definition; therefore, there are no universally accepted standards for quality, safety or durability.[15] Similarly, there are no universally accepted audit/assurance programs.

It is, therefore, proposed to review the distinct aspects of IoT by considering (**figure 2**):

- **General baseline controls**—Minimum controls that need to be applied to all aspects of the technology
- **Data-related controls**—Such as controls that apply to the data forming a key part of IoT
- **Analysis and learning-related controls**—Applied to ensure that the analysis is ethical and enables trusted use of the data and that outcomes of analysis can be applied to business decision-making
- **Business and process alignment**—Related aspects which ensure that the IoT implementation is aligned to business needs and that business benefits are delivered as required

Figure 2—Proposed to IoT Audit Framework



Applicable sources of assurance for each of the previously mentioned are defined in **figure 3.** Some of these relate directly to the IoT while others are more generic and should be applied to relevant IoT components.

Figure 3—Sources of Assurance Documentation

Area	Source of Assurance
General baseline controls	• Open Web Application Security Project (OWASP) IoT Security Guidance[16] • Global System for Mobile Communications Association (GSMA) IoT Security Assessment[17] • Future Proofing the Connected World[18] • US Department of Defense Security Technical Implementation Guide (STIG)[19] • CIS Benchmarks[20]
Data related	• OWASP IoT Security Guidance[21] • GSMA IoT Security Assessment • Future Proofing the Connected World[22] • *COBIT® 5: Enabling Information*[23] • US Health Insurance Portability and Accountability Act (HIPAA) Audit/Assurance Program[24] • *ISACA® Privacy Principles, Governance and Management Program Guide*[25] • *Auditing Data Privacy*[26] • General Data Protection Regulation (GDPR) Readiness, Assessment and Compliance[27]
Analysis and learning	• OWASP IoT Security Guidance[28] • GSMA IoT Security Assessment • Future Proofing the Connected World[29] • *ISACA Privacy Principles, Governance and Management Program Guide*[30] • *Auditing Data Privacy*[31] • General Data Protection Regulation (GDPR) Readiness, Assessment and Compliance[32] • Bias Testing for Generalized Machine Learning Applications[33]
Business and process alignment	• COBIT® 5[34]

Conclusion

IoT is not science fiction and is very much here to stay and can bring great business value. Unfortunately, as is often the case with technology, it has developed ahead of many of the desired controls, including sources of assurance. It is, therefore, advisable to adopt a generic auditing model and to select the applicable controls from the available documentation. In our enterprises, it is up to each of us to "make it so."[35]

Endnotes

1 Star Trek Database, Picard, Jean-Luc, *www.startrek.com/database_article/picard-jean-luc*

2 Star Trek Database, Replicator, *www.startrek.com/database_article/replicator*

3 Raidió Teilifís Éireann, "Star Trek-Type Medical Tricorder a Step Closer," 7 June 2018, *https://www.rte.ie/news/2018/0607/968778-tricorder/*

4 ISACA, *Assessing IoT*, USA, 2017, *www.isaca.org/Knowledge-Center/Research/Documents/Assessing-IOT_res_eng_1217.PDF*

5 ITAF, Information Systems Audit and Assurance Framework, USA, 2014, p. 18

6 *Ibid.*, p. 33

7 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*

8 ISACA, *Assessing IoT Upsides, Downsides and Why We Should Care About Them*, USA, 2017, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Assessing-IoT.aspx*

9 *Ibid.*

10 *Ibid.*

11 *Ibid.*

12 ISACA, *Audit Plan Activities: Step-By-Step*, USA, 2016, *www.isaca.org/Knowledge-Center/Research/Documents/Audit-Plan-Activities_res_eng_0316.pdf*

13 ISACA, *Internet of Things: Risk and Value Considerations*, USA, 2015, *www.isaca.org/knowledge-center/research/researchdeliverables/pages/internet-of-things-risk-and-value-considerations.aspx*

14 *Op cit, Audit Plan Activities: Step-By-Step*

15 *Op cit Assessing IoT Upsides, Downsides and Why We Should Care About Them*

16 The Open Web Application Security Project (OWASP), IoT Security Guidance, *https://www.owasp.org/index.php/IoT_Security_Guidance*

17 GSM Association, IoT Security Assessment, *https://www.gsma.com/iot/iot-security-assessment/*

18 Cloud Security Alliance, Future Proofing the Connected World, *https://cloudsecurityalliance.org/download/future-proofing-the-connected-world/*

19 Information Assurance Support Environment, STIGs Master List (A-Z), *https://iase.disa.mil/stigs/Pages/a-z.aspx*

20 Center for Internet Security, CIS Benchmarks, *https://www.cisecurity.org/cis-benchmarks/*

21 *Op cit* OWASP

22 *Op cit* Cloud Security Alliance

23 ISACA, *COBIT® 5: Enabling Information*, USA, 2013, *www.isaca.org/COBIT/Pages/COBIT-5-Enabling-Information-product-page.aspx*

24 ISACA, HIPAA Audit/Assurance Program, USA, 2017, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/HIPAA-Audit-Assurance-Program.aspx*

25 ISACA, *ISACA Privacy Principles, Governance and Management Program Guide*, USA, 2016, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/ISACA-Privacy-Principles-and-Program-Management-Guide.aspx*

26 Cooke, I.; "Auditing Data Privacy," *ISACA® Journal*, vol. 3, 2018, *www.isaca.org/archives*

27 ISACA, General Data Protection Regulation (GDPR) Readiness, Assessment and Compliance, *https://www.isaca.org/info/gdpr/index.html*

28 *Op cit* OWASP

29 *Op cit* Cloud Security Alliance

30 *Op cit ISACA Privacy Principles, Governance and Management Program Guide*

31 *Op cit* Cooke

32 *Op cit* ISACA General Data Protection Regulation (GDPR) Readiness, Assessment and Compliance

33 GitHub, Bias Testing for Generalized Machine Learning Applications, *https://github.com/pymetrics/audit-ai*

34 ISACA, COBIT® 5, USA, 2012, *www.isaca.org/COBIT/Pages/default.aspx*

35 "Make it so" is the phrase *Star Trek*'s Captain Picard uses when he wants an order implemented.