Doing More With Less

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.

http://bit.ly/2vlJ7be

The Institute of Internal Auditors (IIA) defines internal auditing as an independent, objective assurance and consulting activity designed to add value and improve an organization's operations.[1] However, in many organizations, internal audit is perceived as a (necessary) cost required to ensure compliance with regulations such the US Health Insurance Portability and Accountability Act (HIPAA), the US Sarbanes-Oxley Act of 2002, the European Union Data Protection Directive, or the Payment Card Industry Data Security Standard (PCI DSS). This focus on costs often results in audit staff being kept to a minimum. Even in enterprises with a more progressive view of internal audit, it is often not possible to find people with the right skill set. Nonetheless, the IT auditor is expected to understand innovative technology, understand new regulations and ensure adequate coverage of the audit universe including new applications. So how can IT audit continue to add value? How can we do more with less?

Establish a Data Categorization Scheme

ISACA® defines information security as something that "ensures that within the enterprise, information is protected against disclosure to unauthorised users (confidentiality), improper modification (integrity) and non-access when required (availability)."[2] Therefore, it makes sense (and, indeed, it is commonplace) to categorize the data in accordance with these needs. A short and well-written guide to data categorization is the US Federal Information Processing Standards Publication[3] (FIPS PUB 199) for Security Categorization of Federal Information and Information Systems. A sample data categorization scheme is shown in **figure 1**.

Categorize the Applications

The next step is to categorize the applications based upon the data they process. In effect, one wants to confirm whether each system processes data that are confidential or subject to integrity or availability rules. The best way to do this is to devise a questionnaire and ask the business owner of each application. These questions should be relevant to the enterprise. Sample questions are shown in **figure 2**.

Respondents should be advised that for every question to which they answer "yes," they should indicate the degree of impact: high, medium or low. These ratings, in turn, should be given a numerical weighting. The overall score can then be used to rate the applications (**figure 3**). Again, the scores should be set based upon the needs of the enterprise and the number of questions.

At the end of the process, one should have a list of all the enterprise's applications, each of which is rated as high, medium or low for confidentiality, integrity and availability. These ratings should be

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 current 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 assisted in the updates of the *CISA® Review Manual* for the 2016 job practices and was a subject matter expert for ISACA's CISA Online Review Course. 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 at Ian_J_Cooke@hotmail.com, Twitter (@COOKEI), or on the Audit Tools and Techniques topic in the ISACA Knowledge Center. Opinions expressed in this column are his own and do not necessarily represent the views of An Post.

Figure 1—Sample Data Categorization Scheme

Security Objective	Level 1	Level 2	Level 3
Confidentiality	Loss of access restrictions or unauthorized disclosure would have a **high** impact on enterprise goals.	Loss of access restrictions or unauthorized disclosure would have a **medium** impact on enterprise goals.	Loss of access restrictions or unauthorized disclosure would have a **low** impact on enterprise goals.
Integrity	Improper information modification or destruction would have a **high** impact on enterprise goals.	Improper information modification or destruction would have a **medium** impact on enterprise goals.	Improper information modification or destruction would have a **low** impact on enterprise goals.
Availability	Loss of timely and reliable access would have a **high** impact on enterprise goals.	Loss of timely and reliable access would have a **medium** impact on enterprise goals.	Loss of timely and reliable access would have a **low** impact on enterprise goals.

Figure 2—Sample Questions

Confidentiality—Would unauthorized disclosure…	• affect health and safety? • have a monetary impact (e.g., intellectual property)? • have a reputational impact (e.g., personally identifiable information [PII])? • have a legal/regulatory impact (e.g., PCI DSS)?
Integrity—Would unauthorized modification or destruction…	• affect critical business decisions? • affect health and safety? • have a monetary impact? • have a reputational impact? • have a legal/regulatory impact?
Availability—Would nonavailability…	• have a reputational impact? • affect health and safety? • have a monetary impact? • have a legal/regulatory impact?

used to decide on the controls to be applied. The higher the application rating, the more important the controls are to the enterprise. Therefore, it makes sense to spend more time protecting or, indeed, auditing these applications than the lower-rated ones. Further, the rating will dictate the type of controls. For example, a higher-rated confidentiality application may require that encryption is employed while a higher-rated availability application may require clustering or some sort of failover. It is, of course, possible that an application may be rated high across all three categories.

Figure 3—Sample Scoring Scheme

Security Objective	Level 1—High	Level 2—Medium	Level 3—Low
Confidentiality	45-60	30-45	30 or less
Integrity	45-60	30-45	30 or less
Availability	45-60	30-45	30 or less

Establish the Criteria

The concept of criteria was discussed in my previous column.[4] To recap, “criteria” is defined as the standards and benchmarks used to measure and present the subject matter and against which an IS auditor evaluates the subject matter.[5] An IT auditor will add more value if the criteria used are the same as those already established by the enterprise. If such standards, including a document defining the required baseline controls for all applications—an “application standard,” have not yet been defined, it is highly advisable to audit the second line[6] functions responsible and require that they are set as soon as possible. This document should be agreed to by the first-line functions and subsequently reviewed by internal audit.

As well as adding more value, auditing to the same defined standards will also result in a lot less friction with auditees and should avoid the age-old argument of “We do not apply that standard here.” Further, if the auditees are aware of the standard, they are much more likely to be compliant with it.

Perform a Control Self-Assessment Based Upon the Criteria

ISACA defines control self-assessment (CSA) as an assessment of controls made by the staff of the unit or units involved. It is a management technique that assures stakeholders, customers and other parties that the internal control system of the organization is reliable.[7]

Since the enterprise now has a defined application standard and is looking to increase the assurance provided by internal audit, it makes good sense to build a CSA questionnaire based upon the standard.

The CSA should require the auditee to answer questions on the application standard, providing a percentage score for each answer (the higher the score, the more satisfied the respondent is with the control in question). Further, each question should be flagged as baseline (i.e., all applications require this) or related to confidentiality, integrity or availability.

This should result in a list of applications with percentage scores for each of the security areas (**figure 4**).

Audit the Gap

The resultant gap between a perfect score (100 percent) and the actual score may be small in numerical terms, but could represent a significant risk to the enterprise. For example, Application C may have been categorized as high for confidentiality, and 22 percent does not appear to be an overly large deficiency, but it could represent failures in important controls such as the use of a deprecated encryption protocol. It is, therefore, important that this gap is assessed. This could be

Figure 4—Sample Application Standard Scores

Application	Overall	Confidentiality	Integrity	Availability
Application A	93%	96%	95%	83%
Application B	87%	80%	84%	98%
Application C	84%	78%	85%	94%

done by internal audit performing a short, sharp, focused audit on the control(s) in the question. Recommendations (if any) should then be made and followed up[8] on in the normal way. Confirmed implementation of these recommendations should, of course, result in an increased score the next time the application goes through the CSA process.

Report to the Audit Committee

When several applications have gone through the CSA process, it would be good practice to report the CSA results to the audit committee. This provides transparency and allows the IT auditor to give an opinion on the overall control environment. Further, as the CSA is repeated, applications' scores can be tracked, showing improved scores as controls are implemented and risk mitigated or a decrease in scores as emerging risk arises.

> **“When several applications have gone through the CSA process, it would be good practice to report the CSA results to the audit committee.”**

Audit a Percentage of the Applications Annually

There is always a risk with a CSA that results are inaccurate or that, over time, the auditees become a little complacent. This can result in CSA results that are not reliable. To counterbalance this, I recommend performing a full audit on a defined percentage of the applications on an annual basis. This should help to keep the CSA honest.

Conclusion

Categorizing applications by confidentiality, integrity and availability allows an IT auditor to ensure that limited resources are directed at the right risk factors at the right time. Further, performing CSAs to agreed-on criteria increases assurance coverage and helps ensure that all three lines of defense are pulling in the same direction. Finally, reporting the results to the audit committee increases transparency and allows an IT auditor to give an opinion on the overall control environment. Together, these items add real value to the enterprise.

Author's Note

The author wishes to acknowledge Frank Ennis and Paul Rochford, CISA, CRISC, CISSP, CISSP-ISSAP, of An Post for their contribution to many of the concepts used in this article.

Endnotes

[1] The Institute of Internal Auditors, About Internal Auditing, *https://global.theiia.org/about/about-internal-auditing/pages/about-internal-auditing.aspx*

[2] ISACA®, *COBIT® 5 for Information Security*, USA, 2012, p.19, *www.isaca.org/COBIT/Pages/Information-Security-Product-Page.aspx*

[3] National Institute of Standards and Technology Computer Security Division, *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standards (FIPS) Publication 199, USA, February 2004, *http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf*

[4] Cooke, I.; “Audit Programs,” *ISACA® Journal*, vol. 4, 2017, *www.isaca.org/Journal/archives/Pages/default.aspx*

[5] ISACA, Information Technology Assurance Framework (ITAF), *www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Pages/ObjectivesScopeandAuthorityofITAudit.aspx*

[6] Chartered Institute of Internal Auditors, Governance of Risk: Three lines of Defence, *https://www.iia.org.uk/resources/audit-committees/governance-of-risk-three-lines-of-defence/*

[7] ISACA, *CISA® Review Manual 26th Edition*, USA, 2016

[8] Cooke, I.; “Enhancing the Audit Follow-up Process Using COBIT 5,” *ISACA Journal*, vol. 6, 2016, *www.isaca.org/Journal/archives/Pages/default.aspx*