HELP
SOURCE
Q&A

Q I recently joined a new organization in the risk management department. I observed that the process followed is different than the previous organization in which I was employed. Does the IT risk management process differ from organization to organization?

A Risk management forms the foundation of any organization. Typically, the process for risk management follows these steps:

- Identification of risk
- Analysis, assessment and evaluation of risk
- Determine risk response
- Implement risk response
- Monitor risk

Organizations may adopt different frameworks to establish risk management within the organization; however, whatever the framework may be, at a high level, these steps are commonly used. The difference in risk management processes used by different organizations may be due to various reasons such as:

- **Standards or frameworks adopted**—Although risk management is an established discipline, IT risk management standards have evolved recently. There are a numerous standards such as the European Union Agency for Cybersecurity (ENISA) Octave,[1] Management of Risk (M_o_R),[2] Standards Australia AS/NZS 4360,[3] US National Institute of Standards and Technology (NIST) Special Publication (SP)800-30,[4] International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) ISO/IEC 27005[5] and ISO 31000.[6] While implementing standards, organizations need to develop a framework for the organizational risk management process. There are few frameworks organizations can use such as NIST SP 800-37[7] or ISACA's *COBIT® 5 for Risk*.[8] Organizations can adopt and adapt these frameworks to develop their own risk management framework.

  Processes suggested by these frameworks, although similar, might vary in details, for example, ISO/IEC 27001:2005 *Information technology—Security techniques—Information security management systems—Requirements*[9] suggests an asset-based approach for IT risk management.

> "ALTHOUGH RISK MANAGEMENT IS AN ESTABLISHED DISCIPLINE, IT RISK MANAGEMENT STANDARDS HAVE EVOLVED RECENTLY."

- **Risk assessment: qualitative or quantitative**—Implementing quantitative risk analysis might require detailed study to determine the appropriate method. Comparatively, implementing a qualitative risk assessment might be considered easier since accurately measuring risk is difficult. However, organizations may adopt an approach to arrive at indicative quantified risk impact.
- **Business priorities**—Organizations may define risk management processes depending on the needs and nature of business.

Sunil Bakshi, CISA, CRISC, CISM, CGEIT, ABCI, AMIIB, BS 25999LI, CEH, CISSP, ISO 27001 LA, MCA, PMP
Has worked in IT, IT governance, IS audit, information security and IT risk management. He has 40 years of experience in various positions in different industries. Currently, he is a freelance consultant in India.

- **Risk identification methods**—Risk identification methods adopted by organizations can be different. For example, some risk managers may focus on identifying threats and vulnerabilities first; other risk managers may focus on risk scenario development. Although the outcome is the same, the process may be different.
- **Risk assessment and review**—Organizations use different methods for risk assessment by risk owners. Some organizations follow the workshop method wherein risk owners are facilitated to identify, assess and determine the response for risk, whereas other organizations adopt a survey method. Depending on the method, the process may change.
- **Integration with enterprise risk**—Many organizations still consider risk associated with use of IT as a separate area and isolate risk management from enterprise risk management (ERM). This approach requires additional processes to aggregate IT-related risk and interpret them in business terms.

Therefore, although it may appear that there are different risk management processes, the objective and the outcome are the same.

Endnotes

1 European Union Agency for Cybersecurity, Octave, *https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_octave.html*
2 Axelos, "M_o_R Risk Management," *https://www.axelos.com/best-practice-solutions/mor*
3 Standards Australia, Welcome to AS Standards, *www.asnzs.org/*
4 National Institute of Standards and Technology, *Special Publication (SP) 800-30 Risk Management Guide for Information Technology Systems*, USA, 2012, *https://csrc.nist.gov/publications/detail/sp/800-30/archive/2002-07-01*
5 International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) ISO/IEC 27005:2011 *Information technology—Security techniques—Information security risk management*, Switzerland, 2011, *https://www.iso.org/standard/56742.html*
6 International Organization for Standardization (ISO) ISO 31000 *Risk management—Guidelines*, Switzerland, 2018, *https://www.iso.org/iso-31000-risk-management.html*
7 National Institute of Standards and Technology, *Special Publication (SP) 800-37 Rev. 2 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, USA, 2018, *https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final*
8 ISACA®, *COBIT® 5 for Risk*, USA, 2013, *www.isaca.org/COBIT*
9 International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 27001:2005 *Information technology—Security techniques—Information security management systems—Requirements*, Switzerland, 2005, *https://www.iso.org/standard/42103.html*