The Evolution of Information Systems Audit

From the early days of electronic data processing (EDP) to modern cybersecurity, IS audits have come a long way. The landscape around information systems has been changing, but as in any journey, an eye on the rearview mirror enables better decision-making and safer travel forward.

By considering the lessons learned and avoiding the mistakes of the past, the world of information systems audit can be shaped and prepared to respond to the future.

Changing Contexts

The factors that play a significant role in information systems audit can be broadly classified into a few contexts, including:

- The business environment
- The technology landscape
- Sociopolitical global trends
- The need for governance

Information systems audits do not live in a world of their own; they are performed in the context of these environments. Understanding the current state of each of these contexts can help the auditors determine how the world of information systems audit needs to change to stay relevant and useful.

The Business Environment

Organizations that dominate the rankings in terms of revenue and market capitalization today are very different from those that were leaders a few decades ago. In fact, many of those former leaders have fallen out of the rankings or even ceased to exist. From a brick-and-mortar world of material things and commodities, the modern global economy now leans heavily on technology and services.

This has caused organizations to prioritize innovation and creativity over functioning and growth. Innovation
and creativity, spanning every function in the organization, can result in amazing new products, business models, methods of acquiring and servicing customers and financing models, and helps create more efficiency in every process.

The organizational ethos has also changed dramatically. A greater focus on inclusion, diversity, empowerment, trust, collaboration, teamwork, outsourcing and gig workers has changed how work is accomplished. In addition, although the digital technologies to enable work from anywhere have been available and practiced by many organizations, the COVID-19 pandemic made the adoption of working from anywhere an urgent and important change for every organization.

The roles of IT and digitalization are significant in every one of these aspects. Organizations that leverage IT and digital technologies are the winners in today’s game.

“The frequency and scale of cybercrimes and the profiles and powers of the actors involved are also changing.”

The Technology Landscape

An aggregation of physical equipment in a glass-enclosed space is no longer the metaphor for IT. An application on a mobile phone is likely a better icon of today’s technologies in this click-and-swipe world.

Over the past few decades, the capabilities of computing power, storage and communication, accompanied by significant advances in programming languages and platforms, have exploded, moving from tedious batch processing to online, real-time processing and responses that yield instant results.

Cloud computing has become pervasive and produces significant computing power, storage and processing tools available to people all over the world. The phenomenal increase in network coverage and speed have made the Internet available to a very large population of the world. Today’s mobile devices pack the punch of large servers of the past and provide dazzling high-resolution touch displays, audio, video, location and communication capabilities that are available anywhere and anytime.

New technologies and tools have also been added to the fold. The Internet of Things (IoT) connects automobiles, appliances, machines and other inanimate objects seamlessly into digital solutions through a combination of sensors, tracking tags and gateway communication devices.

Virtual reality, augmented reality and mixed reality applications are being integrated with engineering, manufacturing and other solutions. Blockchain technology is finding applications in fields such as finance and supply chain. Cryptocurrencies could dramatically change the world of finance; even the world of art is experiencing disruptive technology through nonfungible tokens (NFTs). Artificial intelligence (AI) is benefiting from advances in hardware and software that make it more viable. Powered by big data analytics and machine learning, AI is finding its way into the mainstream and getting embedded in solutions to aid human capabilities and decision-making. Robotic process automation (RPA) is being used to convert routine manual tasks to being completely performed by software, eliminating tedious human effort.

Although digital technologies put convenience and power in the hands of consumers and end users, the backend complexities of how these solutions are created and maintained have increased security considerations exponentially.

The pace at which new technologies and solutions are being developed is mind-boggling and shows no signs of slowing down or stopping. The next major paradigm shift will occur when quantum computing becomes mainstream.

Although it may be impossible for one person to gain expertise in all of these technologies, modern information systems auditors need to perform their work in this landscape.

Sociopolitical Global Trends

Globalization is grappling with the forces of localization. Global and local regulators are requiring organizations to abide by a large set of requirements for complying with regulations by governments and other regulatory bodies. Economic disparities and inequities have widened, leading to an increase
The interconnections and integration between solutions also need to be considered during these audits.

Today, the distinction between an intranet and the Internet has practically disappeared. With many solutions hosted in the cloud, users spread all over the world, and the increased use of mobile devices, the physical segregation is often impossible or impractical.

IT solutions in earlier days assisted the organization in its processes. They were often focused on batch processing and had little interface with end users. Modern solutions do not merely assist in the process but are often the process itself. For example, financial transactions are processed entirely on computer systems, while logistics, transportation, scheduling and manufacturing are all driven, controlled and monitored by computer systems.

The information system auditor’s approach to what to audit will need to change. An isolated audit of one application solution or an infrastructure setup may serve a limited purpose. The interconnections and integration between solutions also need to be considered during these audits.

2. The Nature of the Enemy and Attacks

The cybersecurity landscape is constantly under threat, and the task of keeping systems secure is more complicated than ever. It is often not just a disgruntled employee or a random hacker attacking systems today. State-supported or sponsored cyberattacks are also mentioned in the media. The emergence of various cryptocurrencies as a method of payment has enabled ransomware and other threat-based attacks to find anonymous methods of enrichment. Constant vigilance is required to remain secure and protected from attacks.

The auditor needs to evaluate how the enterprise is geared to face these threats. Whether strategies for incidence emergency response, disclosures, recovery from disasters, communication management and reputation recovery are in place and tested should be verified by the auditors.
3. The Significance of Privacy

Every system that captures, stores and processes personally identifiable information (PII) has to operate under regulations that protect privacy and remain within that framework with respect to consent, protection and nondisclosure.

Hence, the auditor needs to identify the specific privacy regulations that impact the solutions and include a verification of how the solutions comply with the privacy requirement pertaining to that region in their audits.

“Powerful big data analytics are helping auditors find anomalies and patterns of wrongdoing—sometimes before the event occurs.”

How the Audit Function Responds to This Change

The audit function can address these significant changes across several dimensions, including collaboration, education and training, standards and guidelines, regulations, and technology.

Independence and Collaboration

The audit function inherently needs to be independent, unbiased and influenced only by objective review and reporting. In an organizational context, the reporting structure, resourcing and management of the audit function must remain free from influence by the technology or business functions, and the team should have access to top management and the board.

However, given that the information systems audit function requires significant technology and business skills, collaboration and teamwork are essential. The challenge is to obtain the needed skills by working together without compromising independence.

Collaboration and teamwork without compromising independence can only be achieved through a mature approach and learning mindset. These are the elements of information systems audit that are under the most stress—digital solutions and modern business processes are continually evolving and high-velocity, high-volume transactions are being processed in real time. In this scenario, the information systems audit cannot focus only on reactionary activity. Security and controls need to be built into the environment during the design, build and maintenance stages. Mature organizations that find a way to include this constructive collaboration will set themselves up for a secure future.

Education and Training

The COVID-19 pandemic has expanded the digital world. Today, digital learning courses on audit and emerging technologies are available to people all over the world. Information systems auditors must prioritize learning, develop a systematic plan and make the effort to learn. The management of the audit function should include learning as an important criterion in the evaluation of their teams.

Standards and Guidelines

Although technology has evolved rapidly, many organizations are working hard to implement standards and guidelines to make themselves secure. Frameworks for the secure implementation of many of the technologies are available either from the manufacturers themselves or from professional entities.

For example, based on the emerging world of the Internet of Things (IoT), the US National Institute of Standards and Technology (NIST) released draft cybersecurity guidance for manufacturers of IoT devices and equipment. Guidelines for securing and auditing IoT, cloud and AI have been developed by industry bodies. Information systems auditors would benefit from studying these types of frameworks, standards and guidelines.

Regulations

Regulatory bodies are working to keep pace with emerging technologies. Requirements cover many aspects of cybersecurity and privacy. This is a big driver for compliance and has spurred the creation of products and service providers who consult in those areas.

It is important for the auditor to be aware of the jurisdiction of each of these regulations and how they impact the solutions an organization in different parts of the world can implement,
considering where they are hosted and where their users reside. Noncompliance with regulatory requirements can cost organizations plenty in terms of fines and punishments.

Technology

Like the rest of the business, the auditors also need to embrace technology for their work. New technologies that drive innovative solutions are helping to better secure those solutions. Big advances are being made in encryption and transmission of data. Two-factor authentication is gaining acceptance, and systems using biometrics are more efficient and more reliable than ever. This results in more secure and controlled access.

AI is being built into more products and can watch for patterns in traffic and identify attacks before they cause harm. Powerful big data analytics are helping auditors find anomalies and patterns of wrongdoing—sometimes before the event occurs.

Computer-assisted audit techniques (CAAT), as they were previously known, are evolving. Continuous monitoring is being built into the digital solutions themselves, with the goal of autodetecting harm and self-healing systems.

It is up to the auditor to remain up to date and take advantage of new technology to assist in information systems audits and ensure that organizations build effective security programs and remain secure.

Conclusion

Changes in business, technology and sociopolitical environments have increased the need for a force to safeguard organizations, including assets, data and systems. The information security or cybersecurity function must be well organized, well staffed, properly implemented and effectively operated. Every organization needs a competent, relevant and effective information systems audit function to verify, report and offer guidance about the efficient functioning of the cybersecurity function. This includes:

• The technology capabilities of the IS audit function need to keep pace with the evolution of new digital technologies.
• IS audit cannot be a discrete, periodic activity. Given that the digital solutions of today are running the enterprise and continuously upgrading and evolving, audit should include continuous assurance and proactive monitoring. It should also focus on the processes that manage the technology development and implementation. An IS audit should focus on the governance and management aspects of technology and cybersecurity as much as it does on specific focus areas of the audit.5

• IS audit needs to be cognizant of business imperatives and align with the aspirations of the organization, including being agile and innovative and adopting technologies at a rapid pace. IS audit’s integration with business management and technology management should increase and improve without compromising independence.

Endnotes