Auditing In IoE & IoT Eco System : Challenges & Opportunities

Internet of Things (ioT) and Internet of Everything (ioE) are going to be the game changer, impacting every sphere of human interface, interaction, the way we live, how we work, how we interact and how do we do business. The questions before the audit professionals are: What is IoT? What is IoE? How do they differ? What are the audit challenges and opportunities while auditing in IoT and IoE IT environment? Read on to know more…

Difference between IoT and IoE

The journey to IoT to IoE is amazingly dazzling with alarming intensity and speed. IoT has been evolving into IoE systems, connecting not only things; but everything including physical things and humans in the omnipresent, omniscient, disrupting technological revolution 4.0. It is an exciting journey in physical space and virtual reality as well with AI, Machine Learning and rubbing shoulder to shoulder with humanoids and robots in a combined IoT and IoE architecture.

K. P. Shashidharan

(The author is a former Director General of the Comptroller & Auditor General of India. He can be reached at kps.ps2013@gmail.com)

IoT connects the Internet things like sensors, devices, computer systems, data, networks, equipment and all things in physical space seamlessly interconnected engaging in continuous data streaming; whereas IoE links everything-not just things; but processes, data, networks, things including everything of IoT and people across the world engaging in data exchange. The IoE system enables human interface to humans, machine to machine communication and human to machine interface in a complex technology driven matrix that connects everything to the super powerful information highway - the Internet. IoE thus takes the auditors for a ride to a dazzling new world of infinite challenges where mind-blowing mind-machine interaction goes on, unfurling into hitherto unknown realms of enormous opportunities.

IoE becomes a complex web of sensors, monitoring automatically mind and body indicators like pulse rates, heart beats, sleep patterns, enabling freeflowing information between man and machine, data-streaming humanoids and robots to machines, linking software and hardware, metamorphosing simple humans into superhuman beings! Advances in Artificial Intelligence and machine learning enables the impossible possible; devices regulate human response making the physical world of networks and computer screens to new avenues of omnipotent virtual realities, new possibilities and opportunities.

Auditing in Disruptive Technological Landscape

Can auditors ignore the risks and challenges of technological disruptions? IoT and IoE are now increasingly being applied in the business as they enable connecting smart systems, mobile apps, devices, monitors, smart equipment, watches, pace makers, people, processes, equipment, smart offices, smart homes, smart cities, computer hardware, software, network, data, processes and everything into the complex web of the mighty information highway offering infinite opportunities with cloud computing, big data along with enormous risks, vulnerabilities, threats, challenges and infinite opportunities.

Making these risks into opportunities is what smart auditors will be looking for. For that, auditors must know enough about the technological applications, associated risks and benefits as well as how to mitigate risks to acceptable levels to increase bottom line.

Internal auditor adds value through management audit and helps the top management in translating business' vision, mission and core values into business strategy and objectives with measurable qualitative and quantitative performance parameters. Enhanced operational performance leads to increased profitability. Management is driven by cutting edge technology to bring operational excellence, cost reduction in operations. Risk management to the level of risk appetite of the business for achieving organisational objectives is a significant value addition internal auditing must aim for by collaborating with the management and thereby integrating the silos for informed decision making process.

Along with operational excellence, bottom line will boom up. Further, the financial reporting must be credible, complying with applicable regulations. Effective internal control system will effectively manage risks to achieve organization goals. Clearly laid down charter of responsibilities, segregation of powers, rules, procedures, systems, controls, supervision, inspection, oversight, monitoring, disruptive ICT solutions like application of IoT, AI, M2M communication, IoE and big data analytics ably complemented and supplemented by internal audit ensure effective control environment for enhanced enterprise risk management for enhanced bottom line.

Internal auditors are providing value added assurance services to business. A good practice for internal audit and assurance functions is the Institute of Internal Auditors' (IIA)'s COSO framework designed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Internal Audit & COSO Framework

Internal auditors are providing value added assurance services to business. A good practice for internal audit and assurance functions is the Institute of Internal Auditors' (IIA)'s COSO framework designed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). COSO is a voluntary private sector initiative of the five non-profit organizations as its sponsors: American Accounting Association (AAA), American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), Institute of Internal Auditors (IIA) and Institute of Managerial Accountants (IMA). The framework helps aligning risk management and fraud deterrence, with business strategy, and performance.

COSO's Internal Audit model addresses five domains: control environment, risk assessment, control activities, information and communication, and monitoring. Sound internal control is established through directed leadership, rules, systems, procedure, Code of Ethics, shared values and culture. Adequate internal control system addresses risk management.

COSO's ERM framework defines the key components, objectives and categories of ERM management: Strategic, Operations, Reporting and Compliance. ERM focuses on the risk identification and management by introducing effective internal controls. The boards of directors find the framework useful for risk management and formulation of business strategy.

Key Thought Terrains

COSO provides thought leadership on internal control, enterprise risk management, fraud deterrence, improved oversight for organizational performance. COSO framework for Internal Audit and the updated Enterprise Risk Management (ERM) models are benchmarked practices. ERM integrates business strategy and business performance. Stakeholders are seeking greater transparency and accountability. Managers need to think strategically about how to manage the increasing volatility, complexity, and ambiguity:

Some of the key issues are:

- Big data proliferation with unprecedented speed need better analytical tools to structure in new ways. Advanced analytics and data visualization tools can only analyse and understand impact of risks.
- Artificial intelligence, Machine to Machine communication and automation are applied for enterprise risk management practices with critical information to managing risk.
- Business executives are driven by the cost effective risk management, compliance, and control activities and governance.
- Business strategy aims at bringing competitive edge in business operations by adopting and adapting cutting edge technological solutions.

ISACA's COBIT Framework

The Information Systems Audit and Control Association (ISACA)'s COBIT - Control Objectives for Information and Related Technology - framework for Information Technology is designed, developed and updated keeping in pace with rapidly changing technological landscape in the audit ecosystem to ensure effective IT governance and management, IT, audit and assurance professionals. COBIT aims at marriage of business objectives with IT goals and ICT applications in business strategy and processes for optimising the enterprise objectives focusing on four critical domains: Plan and Organize, Acquire and Implement, Deliver and Support and Monitor and Evaluate IT related architecture for achieving organizational strategic goals.

Big data proliferation with unprecedented speed need better analytical tools to structure in new ways. Advanced analytics and data visualization tools can only analyse and understand impact of risks. Artificial intelligence, Machine to Machine communication and automation are applied for enterprise risk management practices with critical information to managing risk.

COBIT covers 34 essential processes and 320-odd key controls of responsibility centres help to manage IT related risks to address compliance, internal control, risk management and governance issues. COBIT integrates Enterprise Risk Management and Internal Control developed by the Committee of Sponsoring Organization of the Treadway Commission (COSO); the Information Technology Infrastructure Library for IT service management (ITIL); standards for quality management of International Organization for Standardization (ISO 27000 series); Capability Maturity Model Integration (CMMI), The Open Group Architecture Framework (TOGAF) and the Project Management Body of Knowledge (PMBOK) for improvement in business processes and performance.

While scrutinising the enterprise documentation, the IT auditor should look for evidence of deployment of the best practices for systems development lifecycle (SDLC) by using the maturity model. The risk, compliance and governance-based methodology can provide data security, database integrity, and continuous vigilance on information architecture.

The framework is constantly updated taking into account emerging disruptive technological applications by organizations for better outcome. It equips the IT auditors with dynamic concepts, techniques, processes and structures for transition to change management, with detailed control centric audit checklists and possible sources of evidence gathering, for giving assurance regarding the effectiveness of controls. While scrutinising the enterprise documentation, the IT auditor should look for evidence of deployment of the best practices for systems development lifecycle (SDLC) by using the maturity model. The risk, compliance and governance-based methodology can provide data security, database integrity, and continuous vigilance on information architecture. The framework must enable the auditor to conduct effective IT audit and provide assurance that the IT systems are completely fine-tuned to maximise business objectives and targeted outcome.

Key Risks

IoT and IoE become omnipresent in the business terrain adding value, complexity and risks significantly. ISACA wants companies to ask the following nine critical questions:

1. *How will the device be used from a business perspective, and what business value is expected?*
2. *What threats are anticipated, and how will they be mitigated?*
3. *Who will have access to the device, and how will their identities be established and proven?*
4. *What is the process for updating the device in the event of an attack or vulnerability?*
5. *Who is responsible for monitoring new attacks or vulnerabilities pertaining to the device?*
6. *Have risk scenarios been evaluated and compared to anticipated business value?*
7. *What personal information is collected, stored and/or processed by the IoT device?*
8. *Do the individuals whose information is being collected know that it is being collected and used, and have they given consent?*
9. *With whom will the data be shared?*

Organizations while using IoT and IoE, must be able to manage the risks and safeguard the business interests. ISACA's Internet of Things: Risk and Value Considerations" guidance provides (www.isaca.org/internet-of-things) dos and don'ts for the IoT security, privacy, compliance and assurance issues.

ISACA cautions that risk management must aim at attaining the company's objectives. An entity can accept certain level of risks, eliminate certain risks, share some risks, mitigate and control certain risks and transfer some risks by insuring as well. Control system must be assigned according to the risk levels. It can be detective, preventive, or corrective measures: detecting incidents where preventive controls must be put in place. A detective control may identify inactive accounts and suspicious activities for monitoring.

Preventive security systems include intrusion prevention systems, firewalls, antivirus software; access controls that guide sensitive system resources and data from unauthorized sources. Correcting omissions, errors, or incidents involve correcting wrong data entry to removing illegal users/software from networks to recover from disruptions. IT controls of governance, application, and technology are relevant to know how higher-level controls to be developed.

Internal control oversight by the board can ensure governance framework including monitoring information principles, processes, policies, management, ensuring that they are performing correctly. Management must ensure that the IT controls are meeting the objectives and reliable. The technical controls framework lays the foundation for reliance on information security including its authenticity, integrity of data and evidence of changes if any. Some of these controls include database controls, operating system controls, logging, and encryption.

IoT & IoE Ontology

The IoT security risk ontology covers risk identification control mechanisms suitable for heterogeneous IoT devices. IoT and IoE risks span the physical environment to the virtual Internet. Key security issues include ensuring confidentiality, authentication, access control, privacy and the management of trust in IoT and IoE ecosystem.

Organizations while using IoT and IoE, must be able to manage the risks and safeguard the business interests. ISACA's Internet of Things: Risk and Value Considerations" guidance provides (www.isaca.org/internet-of-things) dos and don'ts for the IoT security, privacy, compliance and assurance issues.

Access control, authentication, data anonymization and privacy are challenging due to scalability and heterogeneity of devices. Confidentiality can be achieved with encryption. IoE exchanges data with other services with third parties, such as service providers and control centres, data transmission must not be tampered. This can be achieved with identity management tools such as Message Authentication Codes. IoE services must be available from anywhere at any time for which different measures may have to be adopted. Service must be accessible to only authentic users by an authentic source by deploying authentication devices. A home with an IoT service, without proper access control, could lead to disclosure of a user's information. Such critical user information must be provided to only by the authorized people. There are very sensitive healthcare services for which trustworthiness of sensors and data is extremely important. Malicious sensor nodes and non-trustworthy sensor data can lead to a safety disaster.

Audit tools for IoT & IoE Ecosystems

IT audit tools and software solutions are yet to be designed to enable effective audit of IoT and IoE landscape. There are security issues relating to the four pillar of IoE system: hardware, software, network and cloud. Malwares and ransomware target IoT and IoE systems. However, Industry, corporate, banking and financial services go for IoE systems for added benefits with increasing speed. IoT and IoE have many risks. IT auditors must be competent to audit IoT applications, encompassing the security risks of IoT and IoE applications.

Risks in IoE environments are the probability of an event occurring and damaging the control measures. IoE applications are exposed to numerous types of risks. IT auditors must assess the risks and suggest appropriate governance approach. Adoption of any technology, processes or business methods may increase risk. IoT risks needs to be evaluated from an organizational, operational, and technical angle.

Organizational risk affects safety within an organization. Privacy of businesses and their customers is organizational risk. IoT enables large amounts of personal data; unauthorized access to this data must be prevented. Noncompliance of applicable regulations like Sarbanes-Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA), Basel II, or SEBI or MCA in India can cause serious regulatory risk.

Operational risk during a machine to machine communication must be secured. Technical risks are associated with IoT devices connected to the Internet. Keeping all these devices secure is challenging as they are exposed to potential threats to hacking or infection with malware or ransomware. Mirai botnet is a powerful botnet to execute denial-of-service (DoS) attacks affecting IoT devices.

There can be five possible attacks cybercriminals can launch on the Internet of Everything (IoE) are given below:

I. Sniffer Attack involving a program called a "sniffer," sniffs out any unencrypted information passing through a network and then steals it.

II. Denial of Service Attack cripples the use of networks, devices or systems.

III. Compromised-Key Attack aims at stealing the key to encrypted communication and uses it to interpret the encrypted data.

IV. Password-Based Attack breaks into a network by guessing or stealing its password.

V. Man-in-the-Middle Attack targets to steal the data being transmitted between two parties and/or devices.

Ensuring Cyber Security

Auditors must know what controls are to be used to mitigate these possible attacks. It is important to enable all security features on all smart devices provided by manufacturers.

IoE-enabled products can be used to update product firmware regularly. Inherent flaws and vulnerabilities in the system must be addressed by firmware updates to patch them to make it more secure.

Smart device must be checked properly to ensure proper encryption, its firmware updates and network communications. Googling the device model can find possible historical security issues. Use secure passwords with a complex combination of letters, numbers, punctuation marks, mathematical symbols and the like with at least eight characters with upper and lower-case characters.

Smart device must be checked properly to ensure proper encryption, its firmware updates and network communications. Googling the device model can find possible historical security issues. Use secure passwords with a complex combination of letters, numbers, punctuation marks, mathematical symbols and the like with at least eight characters with upper and lower-case characters. Reusing the passwords or using the same password across devices is risky. The manufacturer's guide on how to manage their device vulnerabilities must be followed. IoE-enabled products enable regular updating of product firmware. Inherent vulnerabilities in the system must be addressed by firmware updates and patches.

Key Audit Concerns

The goal of auditing an IoT and IoE systems is to ensure data confidentiality, integrity, and availability as these fundamentals determine the quality of information security within an organisation. Risks can be associated in the processes displaying sensitive information to unauthorized users. Integrity of data ensures accuracy, reliability, and completeness of information. Risks can, be arising out of technological dysfunctions, incorrect data input, or the intentional manipulation of data. Availability of information flow is the life blood of informed decision making in business. Risks can lead to loss of data and unavailability of data damaging the existence or continuity of the business.

CIA principles include identity management to enable the right persons to access the right resources at the right times and for the right reasons; access control restricting access to unauthorised persons; authentication specifies access rights to resources as an access policy; privacy assurance focus on the correct collection, storage, and usage of personally identifiable data and other sensitive information; non-repudiation ensures the validity of a unique individual within a system; and, context awareness, determines how certain processes of a device operate.

The compliance frameworks include personal data protection acts; data breach notification obligations, the Sarbanes Oxley Act, Basel II, and the Health Insurance Portability and Accountability Act and the applicable acts, rule and regulations. Auditors use COBIT 5, NIST 800-53, and ISO 27001 frameworks in IT audit. Information Systems Audit and Control Association (ISACA), the Dutch Association of Chartered EDP Auditors (NOREA), and the Open Web Application Security Project (OWASP) provide guidance for IT audit. IT audit practices assist IT auditors in designing controls for risk management.

Need for Robust Internal Controls

The objective of IT audit of IoT and IoE system is to evaluate the system's internal capabilities and control design, including security protocols. Security personnel must put in place the controls correctly and they are effective to prevent security breach. IT audit aims at examining the information systems, their inputs, outputs, and processing with a view to assess the internal controls systems that are in place to protect a company's information.

IT auditors and management need to understand that IoT and IoE ecosystem and their interfaces, devices in the loop and the users. Improper controls for the risks lead to disastrous consequences. IT auditors need to update skills to track vulnerabilities in IoT and IoE systems to suggest proper controls. Controls can be put in place to monitor whether IoT is working as it should be correctly logged and resolutions are recorded in a timely manner.

Businesses must go for sound auditing practices for effective risk management. Audits should be capable to detect risks and address them before any damage is done. They should understand how IoT operates to be able to develop methods to perform audit tests on system-specific functionality. Internal audits must be competent to protect IoT and IoE system, exposed to attacks from hackers and cybercriminals.

The management must introduce appropriate policies, procedures and actions. IoT systems can also pose life and safety risks to people, including pacemakers, defibrillators and assembly line robots at manufacturing facilities. IT auditors must ensure that IoT and IoE systems have undergone testing and upgrades, patches and changes are made to IoT systems. Sensitive data needs protection from hackers.

The goal of auditing an IoT and IoE systems is to ensure data confidentiality, integrity, and availability as these fundamentals determine the quality of information security within an organisation. Risks can be associated in the processes displaying sensitive information to unauthorized users.

How Auditors Add Value?

Internal audit, management audit, financial statement audits, IT audit and other assurance services ensure adequacy of internal controls, risk management to enable the business to achieve its strategic goals. Audit brings credibility and investor confidence. Independent auditors are trusted expert intermediaries between the business and the customers. Auditors' assurance service helps business to adopt best business practices, operational excellence, reliable financial reporting by using right accounting standards and reporting practices. Entities are legally mandated to obtain independent attestation by an audit professional validating the financial and operational information sent to regulators. Evaluation of internal control systems for effective risk management for ensuring business outcome is assured by effective internal audit. Besides, regulatory audits oversee compliance with applicable regulations and prudential financial standards enhancing trust and credibility of business reporting to stakeholders. ■