Q4 - 2022 ISSUE

ISACA
Bangalore Chapter

InfocITy Auditor

ISACA Bangalore Chapter - News Letter

CONTENTS

ISACA
Bangalore Chapter

InfocITy
Auditor

Q4 - 2022

From The Desk Of The President

Dear Members,

Greetings of the day to you!!!

Year-end is always a time of reflection for all of us - to step back and celebrate the successes, learn from the failures and chart the exciting journey in the year(s) ahead. But the overwhelming emotion is one of gratitude-for the opportunity to be a part of the ISACA Bangalore Chapter, to work with all members whose dedication, passion, and resilience have helped the chapter remain the largest in India and to make a difference in our professional environment, community and society. I was privileged and humbled to be part of the ISACA Bangalore team for several years and I feel even more privileged and humbled today to write my first message as President of the ISACA Bangalore Chapter for the newsletter.

We are witnessing a period of profound change - macroeconomic, geopolitical, social and environmental. Many financial analysts and media outlets have predicted a recession; however, I believe that the cyber security industry is resilient in times of economic turmoil when compared to broader market trends. Now, even as we see some of the larger companies starting to lay off employees, I remain optimistic about the resiliency of the cybersecurity sector and there could be more hidden opportunities moving forward. In the 2008 recession, it created a robust cyber entrepreneurship ecosystem, likewise, it may create great new opportunities for all of us.

Our government launched a pilot project based on the CBDC/ERupee and the draft Data Protection Bill 2022 was open for public comment until December 17th. The draft DPDPB 2022 (Digital Personal Data Protection Bill) appears to be lighter in weight than the PDPB 2019. DPDPB 2022 mostly sails through the February parliamentary session and the detailed regulations are presented subsequently. All these changes will create more demand for ISACA professionals and the CDPSE certification. Based on the demand, the ISACA Bangalore Chapter will soon start its first batch of CDPSE certifications in 2023.

As you are aware, a new team has been appointed following the recent AGM. We have five new members this year and the team has met, identified the goals and is working towards achieving them. We also held an in-person introduction seminar at the Hotel Pai Viceroy in Jayanagar. ISACA BC kicked off CISA review classes with 15 students on December 10th and other certification schedules have been published.

We are pleased to inform you that the sale agreement for the new building authorised during our SGBM in October 2022 has been completed on December 15, 2022. We are now working hard to get the new office up and running as soon as possible. We will keep you posted on the official opening of the new office in the coming months.

If I can leave you with one request, it is that all of you become ISACA Bangalore chapter evangelists in the new year. We all take responsibility for understanding our chapter’s capabilities, promoting our certification review classes and CPE and sharing our stories as broadly and frequently as we can.

As always, we solicit your active participation in the chapter ‘s various events and initiatives, including monthly CPE meetings, newsletter article contributions, reviews, classes for aspiring students, etc.

In closing, I want to wish you and your loved ones all the very best for the holiday season.

Regards,

RAJASEKHARAN K R, CISM, CDPSE, CRISC, PMP, ITIL (E), CSM, SAFe, ISO 27001 LA
President

Message From the Vice President

Dear Friends,

Warmest Greetings

I am delighted to bring greetings in this issue of the ISACA Bangalore Chapter newsletter. I want to start by acknowledging the great team of persons in the Chapter and our Speakers who are making a difference in the lives of our members, in the pursuit of excellence. As a team we have consistently demonstrated a keen attention to support the strategic priorities of our members.

I am happy to recall that our Bangalore Chapter was organized and chartered on 5th January 1996 as the 138th Chapter of ISACA.

Thank you for this fabulous opportunity to serve you in this capacity as we look to the future!!! It is my privilege and honour to serve you all, as the Vice-President of the Bangalore Chapter for the year 2022-2023. It is a matter of great honour for me and I feel humbled to have been given an opportunity to work for you all and on your behalf.

I am optimistically excited about the future prospects of what we will achieve together in the coming years.

I wish you all the best.

Regards,

VIJAYAVANITHA, CISA, CIA, MBA, M.Com
Vice President

Message From Secretary

Greetings Everyone !!

It gives me immense pleasure to communicate with all of you through this newsletter. At the outset let me convey a very hearty, happy and prosperous New Year 2023 to all of you. May this year be a very eventful and engaging year for you and may you reach your goals in professional life during the year.

Last year we were able to purchase new office property for the chapter in the CBD, thereby achieving a longstanding wish of the members since 2011. This achievement is a dream comes true for all the earlier EC members due to whose efforts it was made possible. Also, the Chapter Office will be within reach from all the corners of the city. Now we hope to see more of the members participating in all the meetings planned to be held in the Office. Also, with the acquisition of nearly 2000 sq ft space we will try to hold all the Chapter meetings in the Office premises only. We plan to operationalise the new Chapter office shortly.

It is also heartening to note that since the last 3 years the Chapter has held on to being the largest Chapter in the subcontinent and also being the fourth largest chapter in Asia, after Tokyo, Singapore and Hong Kong chapters. This is all possible due to the active involvement of the previous ECs and the value members find in the activities hosted by the Chapter which we promise to continue. We would request more volunteers to actively participate in the chapter activities like providing articles of interest to the newsletter, sharing of professional knowledge through CPE sessions etc.

I would also call upon all the members to renew their membership at the earliest to keep getting benefits from the ISACA website, where there is treasure trove of Knowledge related to your professional growth. It is disconcerting to note that around 325 members had not renewed their membership last year till December which led to sharp fall in the membership from around 2100 odd to 1800's at the end of the year.

The Chapter is actively trying to remain relevant to the members by organizing various events of interest to the members. The quarterly activity calendar is published and put on the website for the information of the members. As directed by the AGM we are looking out for putting out the Chapter's own website apart from maintaining the engage portal for the benefit of the members.

Till we meet next through these columns, Adios!

Yours Truly,

R S UPADHYA
Secretary

Renewal of ISACA membership for the year 2023

Warm Greetings from ISACA Bangalore Chapter!!!

We thank you for your continued support and commitment to professional excellence by earning one or more of ISACA Certifications.

Use your ISACA® membership and ISACA certification(s) as the platform for your growth by utilizing the opportunities for professional development. As you would have experienced, your ISACA membership and certification(s) increase your advancement opportunities by keeping you informed of standards and good practices in the fields that matter most to you and providing access to leading edge research and knowledge through Journals, Webinars, Blogs, ISACA e-library, local chapter events and many more.

Also, you are aware ISACA Bangalore Chapter provides significant benefits and local networking opportunities to its members. The chapter has been in the forefront and served its members in their quest for acquiring professional knowledge by conducting regular CPE Sessions, Webinars, Conferences and other professional development programs. At the chapter it is our endeavor to bring to the table the most relevant of the current topics and encourage active participation of members.

Visit www.isacabangalore.org for more information.

Now it is time for renewing your ISACA® membership for 2023 if not already done. Please ensure to renew your membership before the PURGE to ensure the benefits arising out of continued membership.

Please click below to renew *(login with your ISACA username and password to renew)*
http://www.isaca.org/renew

In case you need any assistance, please do not hesitate to reach out to Chapter Office at chapter@isacabangalore.org

For your information, the membership dues are indicated here below:

International Membership Dues:	**$135.00**
ISACA Bangalore Chapter Dues:	**$10.00**
Total Dues for 2023 membership renewal:	**US$ 145.00**

Note: ***Apart from the above, certification maintenance dues may apply as per the certifications held.***

Recap of Chapter Programs in Q3, 2022

Annual General Meeting held on 29th October-2022 at Pride Hotel, Richmond Road, Bangalore

Welcome to 26th Annual General Meeting – ISACA Bangalore Chapter
ISACA
Annual General Meeting
Saturday : 29th October 2022
Pride Hotel, Bangalore

Welcome to 26th Annual General Meeting – ISACA Bangalore Chapter
ISACA
Bangalore Chapter
Annual General Meeting
Saturday : 29th October 2022
Pride Hotel, Bangalore

1. **Topic : “Changing Role of Internal Audit - IT Audit Universe & Skills For IT Audit”**
2. **Topic : “Digital Trust”**

   Venue : Pride Hotel, 93, Richmond Road, Langford Gardens, Bengaluru - 560 025.

   Date : 15-Oct-2022 (Saturday) Time : 2:00 PM - 4:00 PM IST

   2 CPE Credits offered

Speakers Profile: Mr. Nilakantan, Director Protiviti

Neelakantan is a Director with Protiviti, having more than 12 years of experience in providing information security consulting services to clients in various industry verticals such as Pharma, Financial Services, Manufacturing and IT/ITES. He has worked extensively for clients in India & US and has a varied experience in working with large multinational organizations. He has significant experience conducting information security/ IT compliance assessments including Third Party Vendor Security Assessments. He has also assisted in implementation of Information Security Management System (ISO 27001). He had worked previously with major Big4 firms like PwC, KPMG and Deloitte as part of Risk advisory practice. He also leads India offshore Global Delivery for IT SOX services and supporting various clients across the geographies. In the recent, he leads an IT Compliance audits for one of the largest exchange based out of Chicago.

Mr. CA Narasimhan Elangovan

Mr. Narasimhan Elangovan, a futurist, a GRC Professional, Keynote Speaker. His areas of practice include Data Analytics, Risk Based Audit, Privacy Impact Assessments, Internal Audits, Information Systems Assurance, Internal Financial Controls and SOX Compliance and SOC Audits. He is a regular speaker on Technology at various National and International Conferences of ICAI, ISACA, CII, FICCI etc. He has often addressed the ISACA International conferences at Asia CACS, Europe CACS, Africa CACS, and North America CACS. He is also a member of ISACA Bangalore chapter.

3. **Topic : “APT Attacks - How hackers bypass AV/EDR using advanced evasion Techniques”**

   Venue : Pride Hotel, 93, Richmond Road, Langford Gardens, Bengaluru - 560 025.

   Date : 29-Oct-2022 (Saturday) Time : 10:30 AM - 12:30 PM IST

   2 CPE Credit offered

Speakers Profile:

Mr. Suriya Prakash, Head - DARWIS SFS; Threat Intel API, CySecurity Corp, US.

Mr. J Prasanna - Director, CySecurity Pte Ltd, Singapore.

About the Topic:

Even with corporate, bfsi with antivirus and edr/xdr solution still get infected with Ransomware, spyware, virus and malware. The AV/EDR seems to be in-effective against these attacks. We are sharing how EDR/AV could be bypassed. Can a combination of EDR + Threat Intel API + Honey pot prevent this?

4. **Topic : "ISO 27001:2022. What has changed ?"**
   Venue : Web-based ONLINE session via Zoom Webinar Platform
   Date : 12-Nov-2022 (Saturday) Time : 5:30 PM - 7:30 PM IST
   2 CPE Credit offered

Speaker Profile: Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001

Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001 is a cyber security and privacy expert with 15+ years of experience and his main areas of expertise are information security and privacy management systems, and methodology (ISO27001, ISO27701, GDPR, KATAKRI, COBIT, ISF SOGP, NIST, IAEA guides, PMBOK). Presently Andrew is a Technical Compliance Manager at Finn play.

Topic Summary:

Agenda:

Brief overview of the changes in the new edition of ISO 27001 (Information security, Cybersecurity and privacy protection. Information security management systems. Requirements

- Understand the main changes
- Explore the new Information Security controls
- Plan for improvements to the ISMS

5. **Topic : "A Free in-person Introductory Seminar on ISACA Certifications"**
   Venue : Hotel Pai Viceroy, 3rd Block, Jayanagar, Bengaluru
   Date : 03-Dec-2022 (Saturday)
   45 members attended.

Move Your Career Forward with an ISACA Certification
Get certified and get ahead.

Move Your Career Forward with an ISACA Certification
Get certified and get ahead.

EC Meeting with Workshop on 3rd Dec-2022 at Pai viceroy Hotel, Jayanagar, Bangalore.

6. **Topic : "The Imperative of Cyber Security and Digital Forensics on Auditing Regulatory Compliance"**
   Venue : Web-based ONLINE session via Zoom Webinar Platform
   Date : 10-Dec-2022 (Saturday) Time : 5:30 PM - 7:30 PM IST
   2 CPE Credit offered

Speaker Profile: Nikhil Mahadeshwar, Founder of Cyber Secured India

Mr. Nikhil Mahadeshwar is a renowned Cybersecurity expert and technology-based innovator with more than a decade of experience in the web industry. He is a Digital Forensics Investigator and consultant for various law enforcement and private investigative agencies. He is 'Certified Security Analyst', 'Computer Hacking Forensics Investigator' "ISO 27001:2013 Information Security Management Systems Lead Auditor', and 'Certified Threat Intelligence Analyst'.

He is the founder of Cyber Secured India.

He has also trained more than 50,000 people on cyber awareness and given lectures to entrepreneurs, school & college students, police officials, corporates, etc. He has been awarded as the youngest entrepreneur and was presented as the youngest researcher at the National Conference on Social Media Responsibility.

Topic Summary:

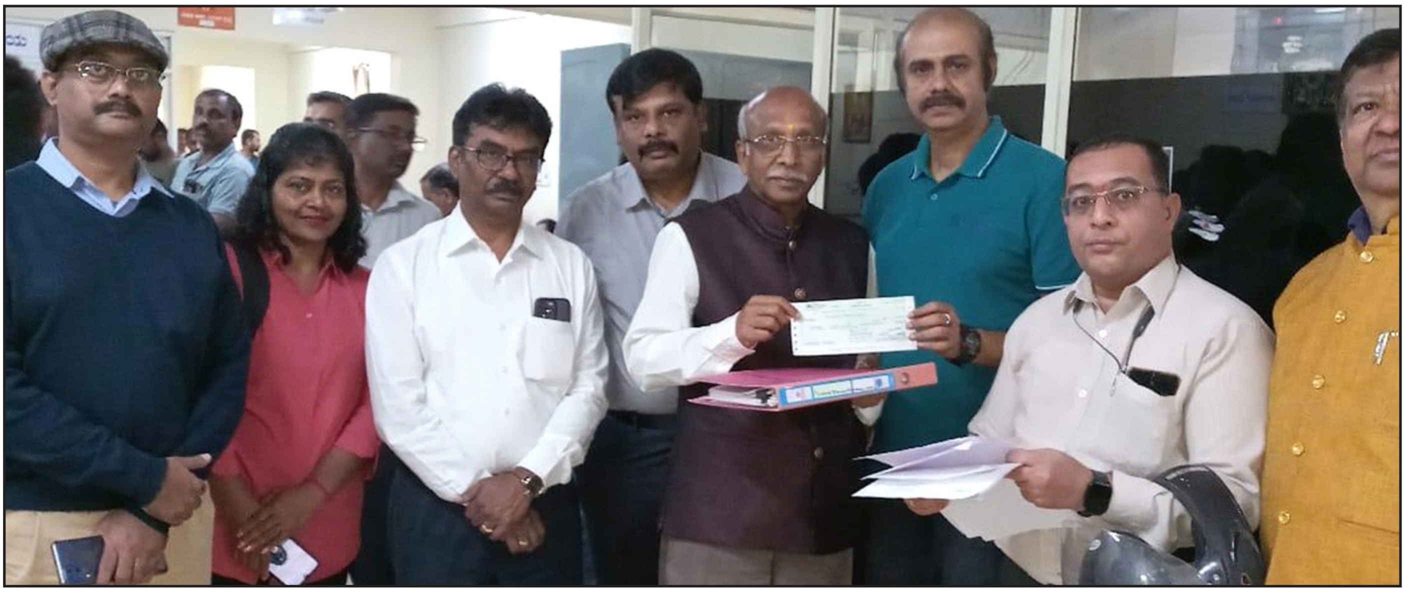
There are several notifications from regulatory bodies, which say a lot about cyber security readiness and digital forensics readiness. While auditing any organization, knowing what to check as an auditor from a technical perspective is really important. Most of the time, we just look at the checklist and compliance certificate. There are important aspects that we may miss out on from the technical perspective. We will cover most of them in the CPE session

ISACA Supported Events :

1. **5-days Information Security Management Systems (ISMS) Virtual Online Lead Auditor Training Course ISO/IEC 27001:2022 (Exemplar Global Approved)**
   Venue : Virtual Online Training
   Date : 26-Dec-2022 (Monday) to 30-Dec-2022 (Friday)
   Time : 9:30 AM - 5:30 PM IST

ISACA New Office Registration

Building Committee completed the procurement and registration of the Solus Jain Heights (B10) Property on December 15, 2022, which was approved in the SGBM on October 15, 2022.



Establishing Enterprise Roles for Data Protection

- Sai Krishnan Mohan, CMC & Ranganath Iyengar, CMC

About the Authors:

SAI KRISHNAN MOHAN | CMC : Is vice president of management information systems (analytics) at Bajaj Auto Ltd. Mohan is a member of ISACA® and the Data Management Association (DAMA) International and can be reached at saikrishnan.mohan@gmail.com and *https://decisionradius.com*.

RANGANATH IYENGAR | CMC : Is director and cofounder of Strategic Interventions India Private Limited. Iyengar is a member of ISACA and the Data Management Association (DAMA) International. Iyengar can be reached at ranga@siiplconsulting.com and *https://www.strategicin.org*.

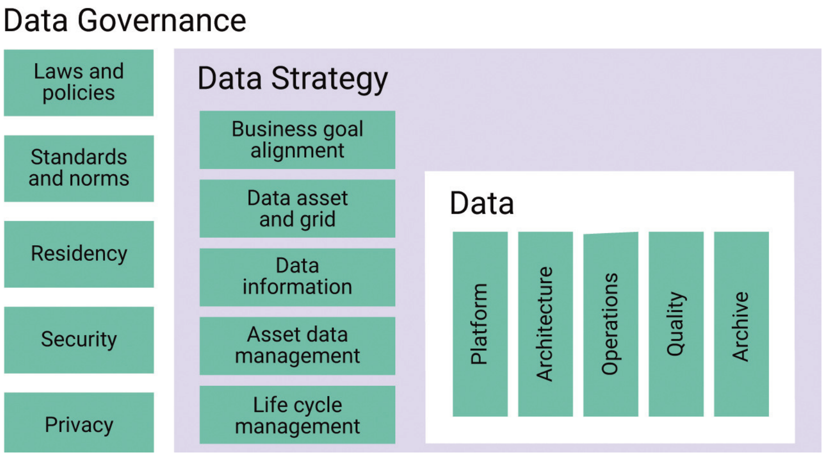
The rise of data sovereignty ideas in various countries, combined with the growing recognition of the utility of data (particularly how data may be used to influence geopolitical events), data residency and localization considerations, is gaining traction in the public sphere. There are clear challenges associated with how specific types of data need to be safeguarded, stored and shared on a need-to-know basis, and data governance mechanisms provide guidelines for these practices. Based on surveys and interviews conducted with senior leaders across industries, an approach for scoping roles, data classification, data governance and decision rights with reference to enterprise data is proposed.

BACKGROUND

The Data Management Association (DAMA) International defines data governance as the “planning, oversight, and control over the management of data, use of data and data-related sources.”[1] Data governance is typically implemented in organizations through policies, guidelines, tools and access controls. If the data are considered information or intellectual assets, the accountability increases. From a practical perspective, there are additional parameters for each concept within data governance **(figure 1).**

FIGURE 1

Enterprise Boundaries—Data Governance, Strategy and Management



Enterprise owners, stakeholders and managers encounter data governance every day as they are challenged to manage data across geographies, business units, teams and individual boundaries. Due to the growing importance of data protection and governance, research was conducted to evaluate the impact of data protection considerations on enterprise risk management (ERM), planning and infrastructure/software portfolio management. The aim was to understand how decision makers and enterprise influencers handle evolving data protection considerations in terms of relative importance/impact, cost and ownership. The research objective was to get wide-ranging inputs from a sample of key decision makers and influencers in the data space across multiple industries, including from enterprises, data (platforms) service providers and third-party system integrators. It is important to consider how to think about data stakeholders in an enterprise and how to define their roles and responsibilities based on different aspects of data governance.

UNDERSTANDING DATA GOVERNANCE

There are four key components of data governance: data residency, security, privacy and compliance.

Data residency is the "storage of personal information within a particular region where data is processed per laws, customs and expectations of that region (country/economic boundary)."[2] As per the International Association for Privacy Professionals (IAPP), information privacy is the right to control how personal information is collected and used.[3] If an organization does not address data residency and privacy, it is at risk of facing potential government enforcement, class action lawsuits, financial penalties and liabilities, damaged reputation, and loss of customer and business partner confidence.[4] Hence, it is critical for the enterprise to get data security and regulatory compliance right.

DAMA defines data security as "the planning, development, and execution of security policies and procedures to provide proper authentication, authorization, access and auditing of data and information assets."[5] Data security can be established through a road map of controls, policies, systems and procedures to protect data from risk[6] including loss, unauthorized access and destruction.

Data compliance refers to the set of practices that ensure that sensitive data are collated, organized and managed in a way that permits organizations to meet their business rule boundaries and legal and governmental regulations.[7] Privacy and security are usually included in the scope of data compliance.

CHALLENGES FOR DATA MANAGEMENT

The International Data Corporation (IDC) has predicted that the amount of worldwide data will grow 61 percent from 33 zettabytes to 175 zettabytes by 2025.[8] This growth creates significant challenges in managing enterprise data flows across systems and lines of business while keeping focus on the alignment between data and business.

Data governance establishes working boundaries for data management, which could operationally include policies, roles and stakeholders, norms for data management operational teams, standards, references or valuation methods. The Profisee 2019 State of Data Management Report identifies four key challenges to data management captured in its survey: compliance, security, analytics and the need for experienced talent.[9]

In 2019, data management strategies focused on alignment of data strategy with enterprise goals, defining the value of professionally managed data and assigning data management responsibility to dedicated staff. In today's context, additional important dimensions include data residency, data privacy, data security and data compliance.

A common challenge for enterprises is managing disparate/distributed data across the life cycle—only then can the data governance boundaries be monitored and controlled. In addition, data risk and compliance requirements can vary by industry. With a 20 percent growth in data every year beyond storage and routine management, automating and prudently managing data are crucial (i.e., tagging, classifying, securing, retaining).[10] For some industries, this is an enormous expense if done primarily using human intervention. Data intelligence and automation help reduce data management risk significantly across an organization.

DATA PROTECTION LAWS

Most countries have laws related to data protection, and their enforcement is often the responsibility of multiple agencies.

The United States has laws such as the Driver's Privacy Protection Act (DPPA) of 1994, Children's Online Privacy Protection Act (COPPA) and Video Privacy Protection Act (VPPA).[11]

In India, the IT Act 2000 Sections 43A and 72A outline compensation rules if personal information is improperly disclosed. Other measures include the Aadhaar Act, an Indian national registration and identification system in which individuals are assigned unique 12-digit numbers that protect confidentiality obligations and the use of personal information by any industry.[12] In addition, the right to privacy is recognized under Article 21 of the Indian Constitution as part of the right to life and personal liberty. A publication by the Indian Ministry of Electronics and Information Technology (MeitY) states that with the transformation of India's economy to a digital economy, "[T]he reality of the digital environment today is that almost every single activity undertaken by an individual involves some sort of data transaction or the other."[13]

The EU General Data Protection Regulation (GDPR) and similar legislative acts point toward a set of principles for the lawful processing of personal data. The UK Information Commissioner's Office (ICO) cites a piece of 2016 EU legislation that represents seven key principles applicable to EU countries for determining basic policies/guidelines on data privacy.[14] The principles are accountability, accuracy, integrity, confidentiality (security), purpose limitation, data minimization, storage limitation and lawfulness, fairness, and transparency. Such principles are useful to boards of directors (BoDs) to set broad frameworks for enterprise governance to address data privacy concerns.

In the context of country-level data protection laws, it is important to understand the differences between data terms to establish focus areas for data protection actions in enterprises:

- Data residency—This is a set of policies, actions and activities pertaining to the geographical location of data storage for regulatory, compliance or policy reasons, including cross-border laws (e.g., tax data and medical records).
- Data sovereignty—This entails protection of data by the location and the laws of a country. It is important as data subjects have different levels of privacy and security protection depending on their data center/hosting location (e.g., email, personal/enterprise data archives). Data sovereignty also defines the stakeholder rights of access to data and national rights and obligations (e.g., government, enterprise, individual, affinity group and social media data).
- Data localization—This is a specific definition purely based on legal obligations, and it is gaining wider acceptance as the entire data life cycle is often managed within a single geographic boundary. It is currently applied primarily to the creation and storage of personal data for audit and traceability since any transactions would require audit, validation or verification.

Data localization and privacy regulations continue to be developed in many countries, and although the data protection principles established by GDPR created a basis for most of them, there are nuances at the country level.

RESEARCH METHODOLOGY

Researchers conducted mixed-method research triangulating inputs from qualitative research and literature review. The research followed a sequential exploratory approach with interviews conducted up front to develop focus areas, concepts and hypotheses that were followed by surveys intended to validate the concepts and hypotheses using qualitative methods. Researchers used semistructured interviews and collation and qualitative analysis of the literature available in the public domain, including press releases and disclosures.

Interview participants were selected based on these criteria:

- Decision-making/influencing role with reference to data strategies
- Extensive industry experience (e.g., a senior leadership role)
- Practitioner experience in data management and analytics
- Technologist’s experience with product development and services experience in data management

Researchers sought industry professionals’ opinions on several concepts, including:

- **Enterprise ownership of data governance-**Do IT and associated functions remain the primary owners of data and enterprise data governance, or is enterprise data governance co-owned by all functions, with IT taking a leadership role?
- **Use of formal enterprise data governance frameworks-**Are formal data governance frameworks established and operational in enterprises across industries?
- **Ownership of enterprise data privacy and compliance considerations-**Are data privacy requirements and compliance owned by IT security/enterprise architecture teams, enterprise leaders or legal functions?
- **Data sovereignty trends-**Are data residency (localization) requirements expected to continue increasing globally or decline as economies expand?
- **Choice of tools and technologies to enable data privacy, security and regulatory compliance-**Should the organization adopt cloud-based data storage and governance technologies based on the industry sector of which the organization is a part?

INTERVIEWS

Researchers interviewed seven senior leaders from major multinational/Indian businesses that are global or transnational. Although the interviewees worked in different industries, they shared common concerns about data protection and the evolving regulatory landscape for data privacy, security and residency, and expressed needs including:

- The need for business leaders to develop an awareness of enterprise data governance and evolving regulations that impact roles and responsibilities regarding data storage, location and movement
- The need for increased spending on data privacy, security controls and localization compliance as a proportion of the organization’s overall IT budget

SURVEYS

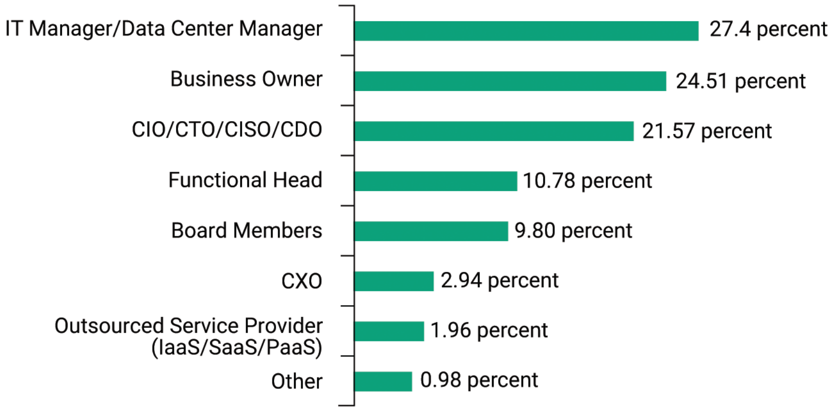
The researchers conducted two surveys from September to November 2021:

1. Survey 1 measured leadership awareness of data privacy, security and residency considerations for enterprises. This survey targeted senior leaders across industry verticals playing global roles in multinational organizations in India.
2. Survey 2 examined enterprise data management and governance practices and tools supporting data privacy, security and residency. This survey targeted senior-level industry practitioners across industry verticals playing global roles in multinational organizations in India.

SENIOR LEADERSHIP SURVEY

FIGURE 2

Responsibilities for Data Management



One hundred two senior professionals participated in the first survey, of which 55 percent were top management in enterprises and more than 92 percent were senior professionals. Most of the respondents (50 percent) had leadership roles in IT/cloud service provider enterprises, and 58 percent of the respondents came from midsize to large organizations (i.e., more than 500 employees). Nearly 48 percent of the respondents believed that ownership of data management is the responsibility of the enterprise, and 49 percent of the respondents believed that ownership of data management lies with IT/ data leaders **(figure 2).**

FIGURE 3

Responsibilities for Data Management

The enterprise architecture/IT team is primarily responsible for awareness and compliance with data localization and storage requirements.	37.25 percent
The legal team is primarily responsible and gives guidance on evolving data localization requirements and helps set data storage policies.	31.37 percent
Enterprise leaders are primarily responsible for awareness and actions related to data localization and storage requirements for respective businesses.	18.63 percent
Country-level leadership teams and their advisory groups are primarily responsible for awareness and actions related to data localization and storage requirements for businesses operating in-country.	11.76 percent
Other	0.98 percent

As shown in **figure 3,** regarding data storage decisions pertaining to multinational business operations, most of the respondents put the onus on respective enterprise architecture and legal teams for compliance with relevant data localization and storage requirements rather than business/country-level leaders. This response is driven by respondents in the IT/cloud services provider industry.

Respondents from manufacturing, professional services and e-commerce industries emphasized business owner and legal team ownership of data storage decisions.

FIGURE 4

Enterprise Awareness of Laws and Regulations Impacting Data Governance

Enterprise/country operations teams share relevant regulatory updates as required with recommended decisions/actions to enterprise leadership.	43.14 percent
The legal team shares relevant updates as required, including recommended decisions/ actions, with enterprise leadership.	31.37 percent
The expectation is for data privacy technology/cloud/tool providers to handle all data governance implications through contractual obligations with low awareness required from enterprise leadership.	14.71 percent
Syndicated (periodic) research updates on the topic from research providers to keep enterprise leadership informed with follow-up insights from analysts/consultants to guide decision-making.	9.80 percent
Other	0.98 percent

The respondents put the onus on local business and legal teams to maintain awareness and understanding of the developing data privacy, security and residency regulations **(figure 4).** These responses indicate a need for practices for business/legal teams to sustain awareness of developing regulations to align the respective enterprise architecture/IT teams when developing the relevant infrastructure and policies for success.

The respondents ranked data management and tool implementation as the leading ways to address enterprise data privacy, security and residency requirements. Respondents from the manufacturing industry placed relatively more emphasis on regional stewardship of business rules related to data privacy/security and residency compliance in data governance solutions **(figure 5).**

FIGURE 5

Leading Ways to Handle Enterprise Data Privacy, Security and Residency Considerations

Maintenance and governance of business rules related to data privacy/security/residency compliance through data governance tools	3.84
Implementation of tools such as One Trust, Privacera, Open Raven, TrustArc, Immuta, Transcend, BigID, Amazon Macie, Dataguise, Okera and Privitar	3.77
Regional stewardship of business rules related to data privacy/security/residency compliance in a data governance solution	3.18
Periodic data privacy/data security impact assessments	2.37
Periodic data residency and localization impact assessments	1.84

FIGURE 6

Perception of Data Sovereignty Trends

Data sovereignty trends will increase with nations developing individual and specific regulations aligned with their national interest	43.00 percent
Convergence to global standard regulations on data privacy, data residency and data security	28.00 percent
Regulations on data privacy, data residency, and data security driven by regional trading agreements or free trade agreements between countries	26.00 percent
Data sovereignty trends reduce as economies open up	3.00 percent
Other	0.00 percent

Most of the respondents (43 percent) believed that the data sovereignty trends developing worldwide will increase with more specific regulations developing around national interests **(figure 6).** Conversely, only a small minority of the respondents (3 percent) believed that data sovereignty trends will decline as global economies expand.

Segmenting responses by industry vertical, a significant portion of respondents from the manufacturing industry (30 percent) and the services/professional services industries (37 percent) believed that regulations on data privacy, data residency and data security will be driven by regional trading agreements or free trade agreements between countries in the future. The respondents were asked to share any current gaps perceived in enterprise data privacy, security and residency. The gaps mentioned were:

- Cloud data leak prevention security
- Multicloud security
- Employee-level awareness gaps
- Establishment of data management roles and practices focused on privacy, security and residency

PRACTITIONER SURVEY

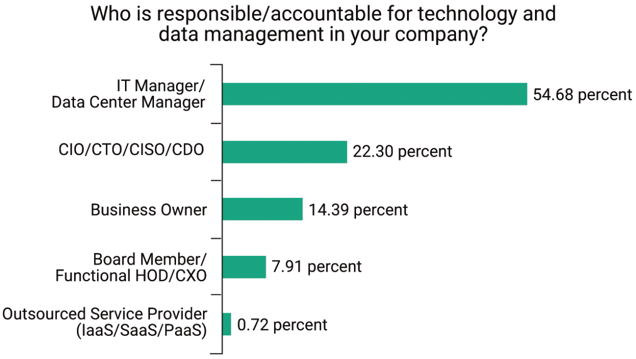
For the second survey, participants were randomly selected, subject to the following shortlisting criteria based on professional experience with data privacy and residency decisions in an enterprise context:

- Active decision makers in enterprises with decision-making authority in IT services or products, maintenance, procurement/buying, IT infrastructure/outsourcing, systems integration, data storage, virtualization, Internet and wireless services, network products and enterprise applications
- Field expertise in product management, medical, legal/law, engineering, market research, finance/accounting, marketing, technology implementation, production, management, technology development hardware, sales/business development, technology development software, operations, procurement and executive leadership

One hundred thirty-seven respondents were qualified based on their awareness and experience as decision makers with data privacy, security and residency considerations in an enterprise context. Out of 157 participants, 89.5 percent (137) were qualified to continue the survey, and the rest (16) were disqualified. The majority of the respondents (57.6 percent) were managers/functional leaders and 23.7 percent were business leaders. Most of the respondents (58 percent) were from the IT/cloud service provider industry, and more than 56 percent of respondents were from mid- to large-sized organizations (500 or more employees). Most of the respondents (55 percent) believed that IT/data center managers are responsible for technology and data management in their organizations **(figure 7).**

FIGURE 7

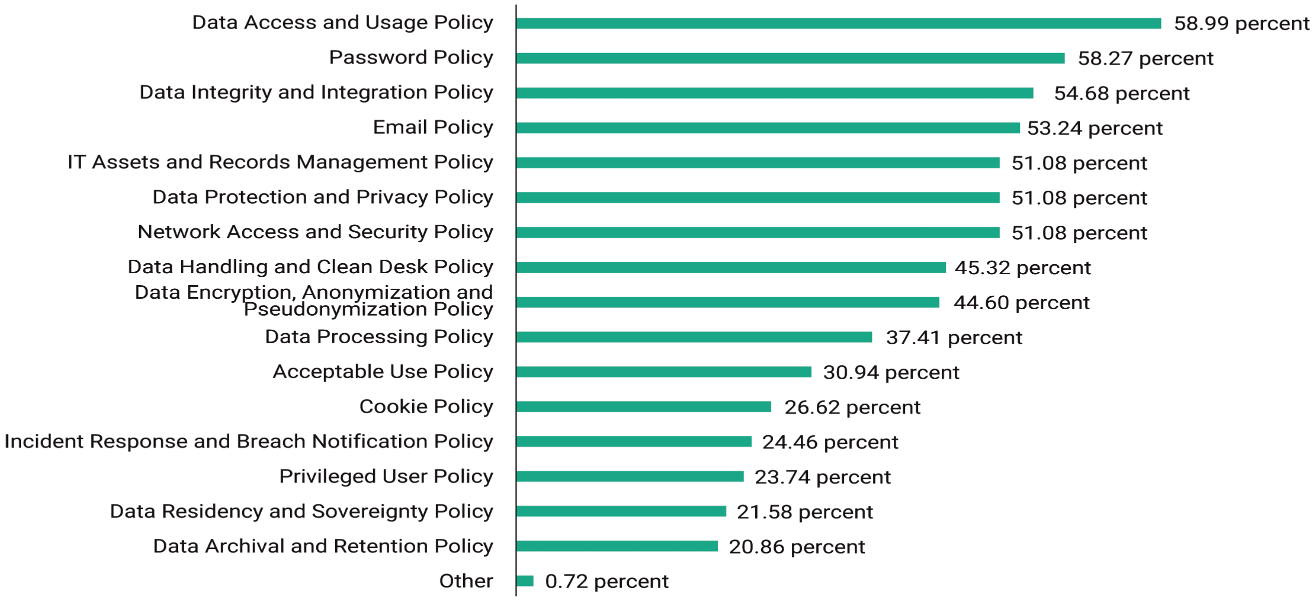
Accountability for Technology and Data Management



Data residency is positioned near the bottom with regard to the types of policies that the organizations ask their employees to follow **(figure 8).**

FIGURE 8

Policy Priorities



Some respondents described organizational practices that risk violating data privacy policies, such as the use of personal storage devices on enterprise hardware even when they are not permitted by policy **(figure 9).**

FIGURE 9

Organizational Practices

Training and orientation on data management practices and privacy	73.38 percent
Website disclaimers on the use of cookies, the capture of personal data	56.12 percent
Changing passwords at regular intervals	55.40 percent
Two-factor authentication (2FA) of login	56.83 percent
Usage of personal hardware, software, mobile and storage devices	47.48 percent
Sharing login IDs for enterprise software with other employees	23.74 percent
Rights and consequences for sharing personal information with the enterprise	45.32 percent
Archiving and checking archived data at regular intervals	41.73 percent
Use of personal storage devices on enterprise hardware	38.13 percent
Regular checking of antivirus, malware and other threats on enterprise devices	47.48 percent
Other	0.72 percent

Virus, malware and phishing attacks topped the list of threats organizations have faced over the last three years, followed by service breaches by IT/cloud service providers **(figure 10).**

FIGURE 10

Leading Threats to Organizations

Identity theft, phishing or spear phishing attacks, social engineering	48.92 percent
Virus, malware, worms, Trojan attacks	48.92 percent
Service breach by cloud service provider (CSP)	46.04 percent
Online financial, bank or credit card fraud	38.13 percent
Hardware, software, data theft	31.65 percent
Theft of employee, enterprise, customer or vendor data	29.50 percent
Service breach by IT	28.78 percent
Web security breach, misconfiguration, authentication, access restriction	27.34 percent
Denial-of-service (DoS) attacks	26.62 percent
Advanced persistent threat (APT) attacks to steal enterprise data	23.74 percent
Router security/domain name system (DNS) attacks	23.74 percent
Cyberespionage	20.14 percent
Other	0.72 percent

Seventy-four percent of respondents used cloud data protection tools in their organization, and approximately 55 percent used data privacy solutions **(figure 11).**

FIGURE 11

Leading Tools for Data Residency, Security and Privacy Compliance

Cloud data protection (CDP) tools	74.10 percent
Data privacy solutions	54.68 percent
Data encryption tools	53.24 percent
Data access governance tools	45.32 percent
Data classification	39.57 percent
Consent/data subject rights management	38.85 percent
Enterprise key management	37.41 percent
Data discovery/flow mapping	32.37 percent
Application-level encryption	32.37 percent
Tokenization tools	23.74 percent
Other	0.72 percent

ESTABLISHING LEADERSHIP AWARENESS

The leadership survey respondents in the first survey put the onus on enterprise architecture/IT and legal teams to handle data protection. Based on the responses, data protection relies on a policy and tool-driven approach. The practitioner survey reveals perceived threats to data security and various tools used in enterprises for data protection. The interviewees shared their reflections that there is a need to improve leadership awareness on the topic of data protection, particularly on evolving laws and regulations that could impact them and their teams' roles and responsibilities. The interviewees also felt that the share of spend on data privacy, security controls and localization compliance needs to be increased.

Based on the surveys and interviews, there is a clear need to enhance enterprise leadership awareness on the topic of data protection and its implications. This leadership awareness is a prerequisite to establishing accountability for data protection in enterprises. Establishing role-based enterprise accountability to handle data protection is a good first step.

ENTERPRISE ACCOUNTABILITY

A good way to establish accountability for data protection is by assigning roles and responsibilities to various aspects of data governance **(figure 12).** An inside-out approach or a set of boundary conditions to define enterprise accountability for data can be used. Traditionally, chief information officers (CIOs) and chief technology officers (CTOs) have been tasked with enterprise accountability for data; however, employees in business and functional roles often create transactional data.

FIGURE 12

Enterprise Role Considerations

Focus Area	Activity Area	Role Considerations
Data governance	• Laws and policies • Standards and norms • Residency • Security • Privacy	Balancing external and internal considerations and risk of data-related decisions with clear accountability at the board level
Data strategy	• Business goal alignment • Data valuation • Information asset management/ enterprise data grid • Data life cycle management	Setting the direction and expectations with enterprise leaders in terms of data ownership, return on investment (ROI), compliance, integrity and business continuity
Data management	• Platform • Architecture • Operations • Quality	Setting the service-level expectations from technology and business teams with clear performance measures

ENTERPRISE DATA RESPONSIBILITIES

Based on the research results, a broad-based approach to responsibilities for handling data governance **(figure 13)** is recommended.

These roles represent various senior stakeholders in the enterprise. They address internal and external governance requirements and balance the risk and controls across stakeholders, which is often the single point of failure leading to breaches, violations or fraud.

FIGURE 13

Roles and Responsibilities of Data Governance

Data Governance Aspects	Role Owner	Responsibility Boundary
Policy and strategy	BoD, Chief risk officer (CRO)	• Policy and strategy • Stakeholder governance
Assurance	Data protection officer	• Compliance with laws • Compliance with organization policies
Integrity	Chief information security officer (CISO) or chief information security and privacy officer (CISPO)	• Data security • Data Privacy
ROI	Chief data officer (CDO), chief financial officer (CFO), chief operating officer (COO), executives	• Master data management • Transaction data integrity • Data life cycle management • Data valuation
Custodian	CIO, CTO	• Business continuity • Technology integrity • IT infrastructure compliance • IT provider compliance

ENTERPRISE DATA BOUNDARIES

Logical boundaries can help clarify decision rights on enterprise data. This includes stakeholder actions covering data governance, data strategy and data management **(figure 12).**

By treating data governance, data strategy and data management as focus areas, activity areas and role considerations can be mapped to each focus area **(figure 12).** These role considerations intersect with the decision aspects and scope described in **figure 14.** From the literature review, surveys and interviews, it can be inferred that the data strategy is connected to data management and that data governance needs to balance external (regulatory and business partner) and internal (enterprise) stakeholder expectations. This approach aligns the BoD's thought process and risk/controls with implementable, quantifiable and actionable measures for various teams and stakeholders. It also provides clear visibility into residency, privacy and security at the BoD level to determine policies and governance mechanisms for execution downstream by teams and leaders.

FIGURE 14

Data Governance Decisions Mapped to Stakeholders

Decision Aspect	Decision Scope	Stakeholders
Location/boundary compliance	Appropriateness of data location	CIO, CTO, executives
Authority/access compliance	Ensuring data security	CISPO, CRO, executives
Privileges/operational compliance	Ensuring data privacy	CDO, CISPO, executives, end users
Data strategy/business compliance	Data strategy governance	BoD, CRO, CFO, executives

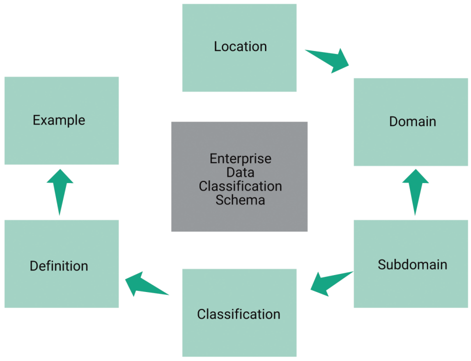
ENTERPRISE DATA CLASSIFICATION SCHEMA

A taxonomy/schematic for enterprise data used by location, as shown in **figure 15,** can be created to guide business/functional stakeholders that must handle active data assets.

This schema can help consolidate and baseline data assets that are in active use or archived, as only an end user of data would have the required degree of visibility. Such taxonomies can then be integrated into an overall enterprise-level data management framework and monitored through an enterprise data grid that tracks all active and archived data assets. This approach also helps enterprise governance stakeholders conduct data use audits to ascertain compliance with various parameters and increase the coverage of such audit exercises across important datasets.

FIGURE 15

Enterprise Data Classification Schema



CONCLUSION

This research examined practitioner perspectives on data protection, including data privacy, data security and data residency/localization considerations. Considering the evolving data regulation landscape and impact to enterprises, it is clear that the responsibility of data protection is not limited to IT/legal considerations; it involves all functions in an organization. Therefore, it is crucial to enhance leadership awareness of data protection and develop a meaningful accountability structure in an organization. Visualizing enterprise data assets in the context of their location, subject area, potential risk, compliance required and data owner/data steward can enable organizations to build a common/cross-functional framework of where to focus on data protection. A structure of roles and responsibilities with decision rights and boundaries can help improve clarity on data ownership and accountability for data protection. Implementing a data classification schema and accountability model for data protection across the enterprise can help reduce threats to data security, data privacy and data residency compliance, thereby reducing enterprise business risk.

AUTHORS' NOTE

The authors would like to thank all interview panelists and survey respondents for their valuable inputs in the primary research.

ENDNOTES

1 DAMA International, DAMA-DMBOK2: Data Management Body of Knowledge, Technics Publications, USA, 2017

2 Day, P.; "Data Across Borders: The Importance of Data Residency," Venture Beat, 3 October 2019,https://venturebeat.com/2019/10/03/data-across-borders-the-importance-of-data-residency

3 International Association of Privacy Professionals (IAPP), "About the IAPP," https://iapp.org/about/what-is-privacy/

4 Ibid.

5 Op cit DAMA International

6 de Groot, J.; "What Is Data Security," Digital Guardian, 12 August 2021, https://digitalguardian.com/blog/what-data-security

7 Reciprocity, "What Is Data Compliance?" 11 January 2020, https://reciprocitylabs.com/resources/what-is-data-compliance

8 Profisee, 2019 State of Data Management Report, USA, 2019, https://go.profisee.com/thank-you-2019-state-of-data-management-report

9 Ibid.

10 Richardson, D.; "Best Practices in Data Governance and Legal Use Cases," Aparavi, https://www.aparavi.com/resources-podcasts/data-governance-best-practices-legal

11 Global Legal Group, Data Protection Laws and Regulations, USA, 2022, https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa

12 Linklaters, "Data Protected: India," September 2022, https://www.linklaters.com/en-us/insights/data-protected/data-protected—india

13 Ministry of Electronics and Information Technology (MeitY), Data Protection in India, India, February 2018,https://digitalindia.gov.in/writereaddata/files/6.Data%20Protection%20in%20India.pdf

14 UK Information Commissioner's Office (ICO), "The Principles," https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

This article is published from ISACA Journal's online-exclusive content for the benefit of Members.

Link to access the article online: https://www.isaca.org/resources/isaca-journal/issues/2022/volume-6/establishing-enterprise-roles-for-data-protection

Artificial Intelligence in Auditing

- *CA Narasimhan Elangovan*
Partner, KEN & Co.

About the Author:

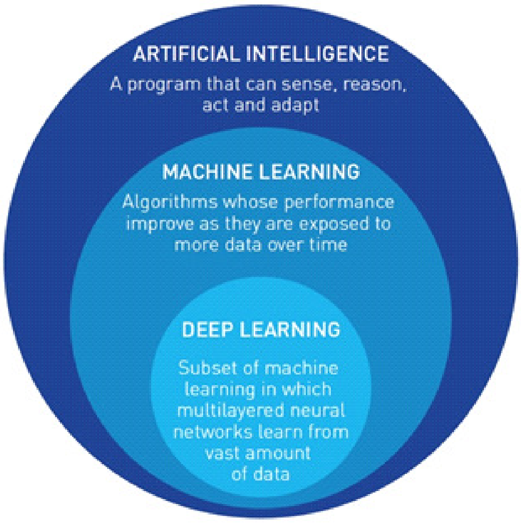
The author is a practising CA and partner KEN & Co. He is a GRC Professional, a Digital transformation catalyst and an author. He believes in the power of technology to solve everyday problems. He can be reached at narasimhan@ken-co.in

Special Mention

The author would like to recognise the efforts of George Sunny in contributing towards this article.

Artificial Intelligence (or AI for short) is the simulation of human intelligence by machines. Machine learning is a subset of artificial intelligence that can learn automatically through experience and exposure to data. These sound like fancy statements but what is AI really?

Simply put AI is statistics on steroids. It is a powerful tool that allows us to deal with huge quantities of data and be reasonably assured that the inferences drawn are accurate. AI has proven to be useful in a variety of areas like medicine, driverless cars, speech recognition, and of course in audit.


ARTIFICIAL INTELLIGENCE
A program that can sense, reason, act and adapt
MACHINE LEARNING
Algorithms whose performance improve as they are exposed to more data over time
DEEP LEARNING
Subset of machine learning in which multilayered neural networks learn from vast amount of data

Key Applications of AI in Audit

The following are the domains where one could use AI in audit:

a. **Helping you understand the behavior / pattern**

AI is good at digesting large amounts of data quickly and identifying patterns or finding anomalies or outliers in that dataset. The objective is to identify whether a given data point fits within an existing pattern or if it is an outlier or anomaly. An example could be, identifying transactions which are more than 3 to 4 times of the average or standard deviation.

b. **Digging deeper**

AI can help in discovering unknown patterns,which perhaps the human mind may not have thought of. It can run multiple simulations on the data thereby making it more probable or likely to identify newer trends. It can perform macro and micro analysis there by helping you to dig deeper. A classical instance would be using AI in fraud detection patterns and using it real-time to prevent frauds.

c. **Automating Routine Tasks**

The boring and monotonous comparisons and reconciliation of data can be automated with a lot of rules and little bit of intelligence, thanks to AI. Most of our work in audit including performing of operating effectiveness testing, compliance and substantive procedures can be automated. It can also help in automating time-consuming documentation processes.

d. Performing risk analysis

With growing volumes in data,it is increasing becoming a challenge to analyze the entire population for doing risk assessments. AI comes to the rescue. With built in intelligence AI solutions can reveal how unusual sales reversals occur post month or quarter end for specific locations or specific accounts. Using these insights auditors can change the processes deployed in audit.

e. Predicting

AI powered with statistical models can help in identifying patterns which are likely to follow in the days to come. These act like early warning signals and help prevent possible frauds or lapses in internal control systems.

f. Analyze structured and unstructured data

Most of the current audits are focused on analyzing the structured data. However, AI powered solutions analyze the complete volume of structured and unstructured data that come from financial records by parsing data in detail.

A few practical use cases

- **Reviewing of Contracts -**The most common use case of AI in audit procedures is contract reviews such as leases. With the help of AI, an auditor can continuously analyze a larger number of contracts in real-time.

  Using AI, auditors can automatically extract data from contracts with tools such as Natural Language Processing (NLP) and identify relevant clauses for accounting treatment such as lease commencement date, payment amount, renewal, and termination options and so on. Thanks to these findings, auditors can evaluate and assess risks in the contract more effectively.

- **Spotting material misstatements in general ledger -**Factors such as the large volume of data, insufficient time and inherent limits of internal control systems and accounting, have limited auditors to have to be content with the “reasonable assurance” motto. Auditors examine a subset of data rather than the entire data set hence the risk of material misstatement increases.

  Use of machine learning improves the testing of ledger data by analyzing the entire dataset in a short period of time to identify material misstatements based on risk analysis rather than traditional audit rules. This allows AI-based tools to flag transactional data based on how far they differ from the standard setallowing for the spotting of patterns and anomalies within unstructured data with ease, a feat that was previously difficult at best, if not impossible.

- **Automating expense audits -**Another area where AI automates an audit process is with expenses. AI-powered tools can help businesses to detect duplicates, out-of-policy spendings, incorrect amounts, suspicious merchants or attendees, and excessive spending.

Benefits of AI in Audit

- **Reduces the workload on auditors:** Auditors do not have to go-back-forth for asking questions to the client as much as in traditional audit.
- **Reduction of cost:** Using AI reduces the cost involved in manual hours of research and analysis.
- **Audit Quality:** Good AI systems continuously learn and adapt to datasets so that they can better detect anomalies as more data is processed. Therefore, use of AI/machine learning increases the audit quality.
- **Enhance focus:** Using AI to power audits can help auditors focus on key aspects which require more attention and there by target key risks.

Limitations of AI

Powerful as it is, AI is still just a tool for use. AI is not a magic box that will supplant human beings from all areas of their usefulness. The truth is that AI needs humans significantly more that humans need AI.

AI may be able to scan through terabytes of data at speeds unthinkable for humans, but it is not able to interpret this data and draw meaningful conclusions. It may be able to identify patterns that we would miss but it is incapable to understanding the meaning behind those patterns and its implication in real life. At the end of the day, AI is only as powerful and the person using it.

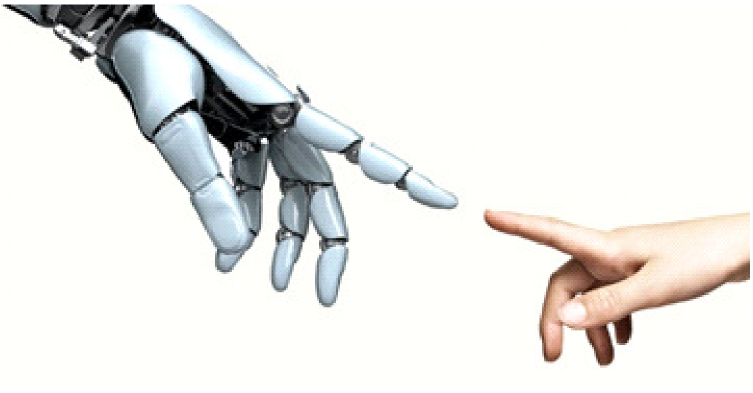
How to get started?

While much has been spoken on how AI can move the work of audit, the real question is where does one get started? Below are a few tools and solutions which is worth exploring:

- Botkeeper can automate accounting power by Machine Learning.
- iManage can review 1000s of contracts and extract specific requirements using AI.
- Home grown company, Zoho's ZIA is an AI assisted tool which can bring in automated analysis of data and acts as a second pair of eyes. It can be used extensively in Zoho Books and Zoho Analytics
- mindbridge.ai is analytics powered by AI and can help you demystify the complicated numbers and assess risk
- Not to forget, Microsoft Excel's "Ideas" now called as "Analyze Data" uses AI to provide interesting, automated insights.
- teachablemachine.withgoogle.com helps you have fund with AI

Conclusion

We have seen the many wonderful uses that AI can have in the field of auditing.We have also seen why AI by itself is insufficient in



many important ways. This leads us to an obvious conclusion. The greatest results are achieved when AI is used to augment the capabilities of humans and facilitate our actions.

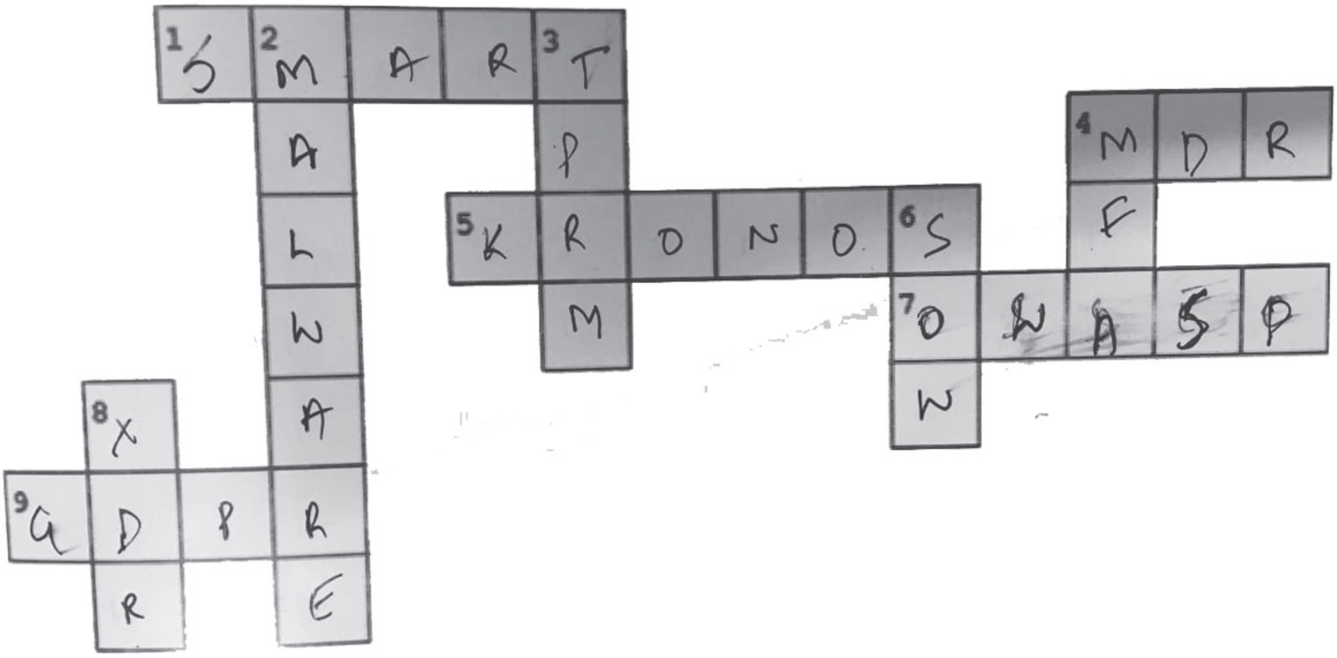
Disclaimer

The tools and solutions mentioned are purely for educational purposes and the author does not have any interest in them or endorse them.

References

1. ACCA Global
2. Corpgov.law.harvard.edu
3. AICPA

Answers for Q3, 2022 Crossword



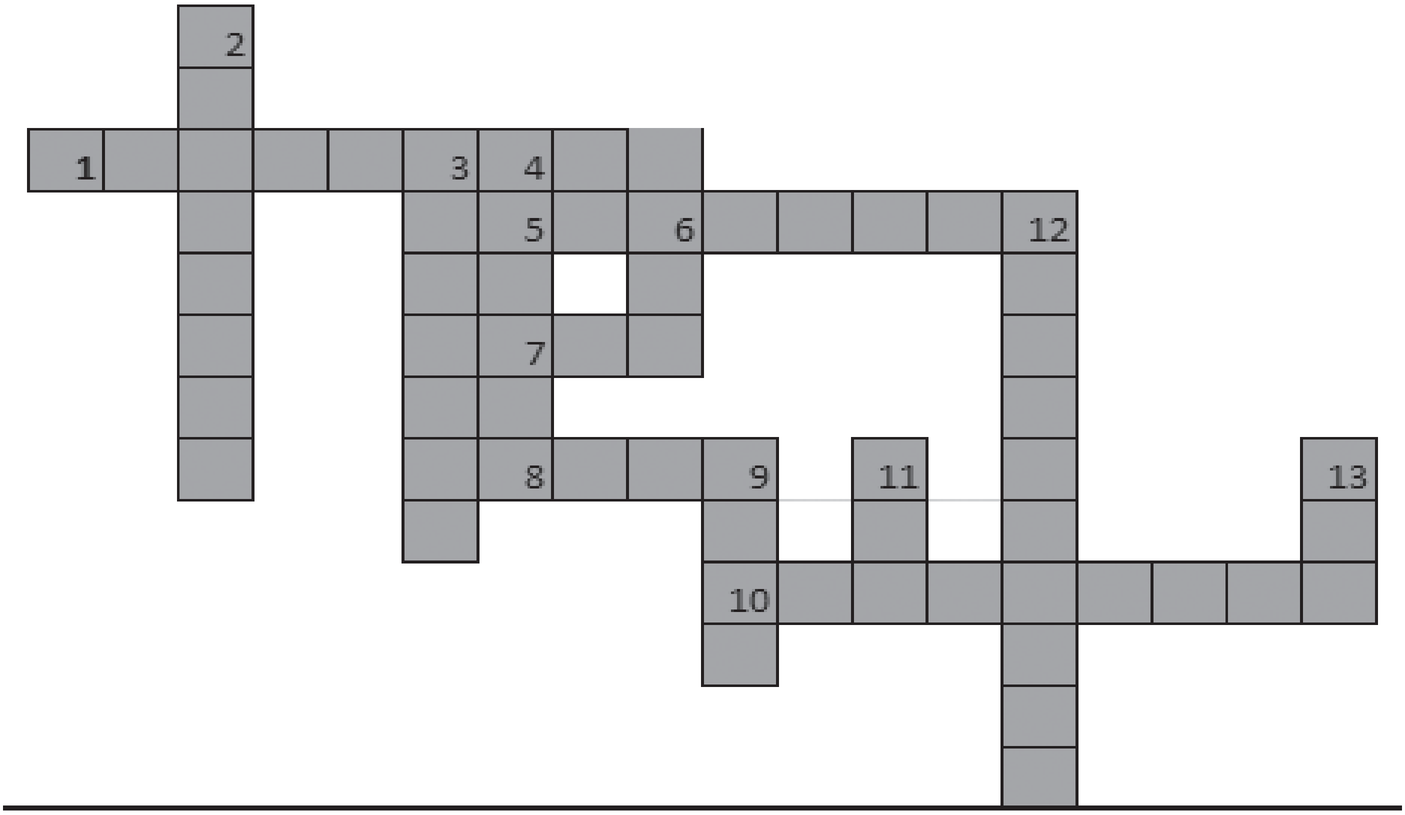
Winners of Q3-2022 Crossword Context:

1. Chandrashekar S - Membership ID: 1626867

Congratulations to the winners...!!

Each winner will get a gift voucher worth of Rs.500 each. ISACA Bangalore Chapter team will contact the winners.

ISACA BANGALORE CHAPTER CROSSWORD CONTEST - Q4, 2022



Across

1 The attribute that uses asymmetric cryptography for digital signatures in order to prove that the message was not altered after it was digitally signed by the creator?

5 Which identifies the mail server for a domain.

7 Object Automatically assign security settings to systems through Active Directory

8 Solutions aggregate and correlate log entries that are received from a wide variety of sources

10 Unidirectional gates that prevent more than a single person fromentering a facility at a time

Down

2 Technique to Digitally label data and indicate ownership.

3 Slowest and most intrusive biometric scan technique

4 The most common application of steganography is hiding information under

6 The amount of time that it is acceptable for a system to be down prior to recovery during a disaster

9 The amount of time that typically take to restore service after a failure

11 The Metric used to measure the frequency at which the system admits a person who should not be admitted.

12 Strong magnetic fields to a storage device in order toremove the data that is stored magnetically on that device

13 Dictionary provides a centralrepository of security vulnerabilities

Crossword Created by Director - Newsletter, ISACA Bangalore Chapter

Three lucky winners will be awarded Rs.500 gift voucher each.

All the responses will be sent to chapter manager email address (chapter@isacabangalore.org).The responses should contain the photo / scanned copy of the filled crossword, Member name, ISACA ID, email and contact phone number.

Last date for sending the crossword results is March 15th, 2023.

Terms & Conditions:

a. This contest is only for ISACA Bangalore Chapter members only. Other ISACA chapter members and non-members are not eligible to participate in the contest.

b. In case if there are only one or two winners from the total entries then the vouchers will be given only to them. If there are no winners then no gift vouchers will be given.

c. ISACA Bangalore Chapter Executive committee reserves all rights to drop / change this program, modify the gift vouchers value

Contributions to ISACA Bangalore Chapter Newsletter

Dear Members,

The ISACA Bangalore Chapter Quarterly Newsletter covers the updates on chapter events, technical articles and whitepapers related to the areas of emerging technologies, IT Governance, Audits and Cybersecurity. In this regard, we encourage our chapter members to send your technical articles and whitepapers to us.

You can send your articles / whitepapers to our chapter email address: chapter@isacabangalore.org

Regards,

CA. Chandra Prakash Jain T, FCA, CS, CISA
Director - Newsletter, ISACA Bangalore Chapter

Support from ISACA Bangalore Chapter

Website: https://engage.isaca.org/bangalorechapter/home

Chapter Office Address:
S/13, 2nd Floor, Priya Chambers
Dr. Rajkumar Road, Opp. St. Theresa’s Hospital,
2nd Stage, Rajajinagar, Bangalore- 5600 10.

T: 8050030042 / 98865 08515 / 080-23377956

Email: communications@isacabangalore.org & chapter@isacabangalore.org

Telegram Channel: https://t.me/joinchat/AAAAAEt42QAUpWHucyNyJA

LinkedIN: https://www.linkedin.com/company/isacabc/

YouTube: https://www.youtube.com/channel/UCTdsKxe3t3BDCVGNrcUFhjg

Facebook: https://www.facebook.com/ISACABC/3

383
30
495
31.4K

Book Post

If undelivered please return to :

ISACA®
Bangalore Chapter

S-13, 2nd Floor, Priya Chambers
Dr. Rajkumar Road, Opp. St. Theresa's Hospital,
2nd Stage, Rajajinagar, Bangalore- 5600 10.
Ph. : 080-23377956 Email: chapter@isacabangalore.org

Printed @ Cauvery Ent. ✆ 22128682

Chapter Reg No : 433/2002-2003