SECURE 'T' CAFE

Q2 2023

Menu

QUARTERLY NEWSLETTER

ISACA®
Chennai Chapter

Vanakkam, Namaste 🙏🏻

A warm welcome once again to ISACA Chennai Chapter's Secure 'T' Café.

The spread in this quarter is truly Spicy & Cool... The probable questions on your mind may be....

- Have you added Ice Tea and Mirchi Vada to the menu ?
- How can the content be both Spicy and Cool?
- Spicy & Cool... What would that be like?

Why wait? Read on and check it out yourselves!!!

SECURE STARTERS – Knowledge nuggets on Regulatory Updates

April 24, 2023, the D-day dawned with a brisk start for the entire **Insurance Industry**. Cyber security was the topic of discussion at every nook of Insurance Sector, yes you guessed it right, this quarter's 🌶️ STARTER is on Insurance Regulatory and Development Authority of India (IRDAI) new **Information and Cyber Security Guidelines 2023.**

This is a comprehensive guideline on Cyber Security issued by the Insurance Regulator, as it supersedes all the prior guidelines / circulars issued (for complete list of superseded guidelines and circulars, please refer here).

About the new Guideline

This is a single guideline applicable to all Insurance Industry entities (for e.g. Insurers, Brokers, Web Aggregators, Third Party Administrators, Corporate Surveyors and much more)

The thrust areas in the guideline can be broadly bifurcated as follows:

- Information and Cyber Security Guidelines Document (Guidelines) (175 pages)
- Annexure I to VI (Annexure III has the Audit Questionnaire comprising of 348 points)

The main Guidelines Document elaborates on the following:

- Purpose, Scope, and the overall Objectives of the Guideline
- Governance, defined precise Roles & Responsibilities w.r.t All Functions, not just limited to security (Chief Risk Officer (CRO), Chief Information Security Officer (CISO), Chief IT Security Officer (CITSO), Chief Security Officer (CSO), Chief Human Resource Officer (CHRO), Chief Technology Officer (CTO))
- Committees required (Information Security Risk Management Committee (ISRMC), Control Management Committee (CMC) etc
- Risk Management, Acceptable Usage, Exceptions and the associated processes and approvals surrounding the same
- Manner of Compliance to the Annexure
- Security Domain Policies covering 24 areas – detailing on the practices and review mechanisms required to be deployed by the Entities. The policy requirements may have some additional aspects that have not been specifically dealt with in the 348 audit questionnaire points. Thereby a careful reading is inevitable for ensuring due compliance.
- Each of the 24 Security Domain Policies comprise of a RACI Matrix, to delineate departments which are Responsible, Accountable, to be Consulted and to be Informed

The Annexure to the guideline has 348 Audit Questionnaire points, of which 255 points are classified across Areas based on NIST Cyber Security Framework Sub Chapters 1. Identify (ID) 2. Protect (PR) 3. Detect (DE) 4. Respond (RS) 5. Recover (RC)

The remaining 93 out of 348 Audit Questionnaire points are spread across the following areas: 1. Work from Remote Location (WFRL) 2. Work from Remote Location for Investments Department (WFRL.IN) and 3. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IGDM)

Independent opinion

The Independent Auditors are required to comment both on Control Design and the Effectiveness of Entity's Compliance to the Controls, with Risk marking across High (3 Marks), Medium (2 Marks) and Low (1 Mark) for Non-Compliances. A Certificate is required to be issued to the Audit Committee of the Auditee in the format specified. The Eligibility Criteria for selection of Audit Firms is provided in Annexure IV.

In summary, the IRDAI Information and Cyber Security Guidelines 2023 is both extensive and exhaustive. It lucidly indicates the extent of significance and importance which the regulator places on **Cyber Security.** With specific requirements in terms of Governance & formation of Committees and by assigning Roles to all the departments, the Regulator emphasises that **Cyber Security is an Organisational Responsibility.**

The Insurance Industry and the Auditors are sure to enjoy the spice and flavour which these intense compliance requirements shall bring about, as the only way to sustained growth and success is to dedicatedly ingest the SECURE 'T'!

- The 🌶️ STARTER TOASTED by Ms. Sangeetha N

Chapter Events - over a Cuppa 'T'

ISACA Chennai Chapter's Footprints during the quarter: What makes 2nd Saturdays so special – Ha yes the holiday of course and additionally the ISACA monthly Professional Development Meetings (PDMs) too.

What commences with a virtual networking in case of online PDMs or the yummy Sweet, Kaaram (savoury) and Coffee – popularly called as SKC by the Tamilians, in physical PDMs, progresses to Security News Roundup, which is a quick digest of the security breaches / best practices from across the world and culminates with a hard-core topic largely associated with the Digital World. The speaker and the topics are hand-picked by a committee of experts. It is truly a delight to watch the rapt attention with which the listeners are absorbed onto the subject... A few SIPs from the monthly PDMs follows on.....

April 2023
A week into the brand-new start of the fiscal year April 2023, the **Future of Data** was discussed at length by our Chapter member **Mr. N C Ananthasayanam** at the virtual PDM on April 8, 2023. The comprehensive contents of the topic right from Data types, tools, different architectures, evolution of data landscapes, challenges thereon, sensitive data compliance, etc., were so well articulated and organically correlated that the most resounding maxims of this decade: 'Data is the new oil', could be appreciated in spirit!!

May 2023
Amidst watch words and catch words like Cyber threat and Cyber risk, the respite is **Cyber Insurance**. The cyber risk scenarios as per the Cert-In report and incisive content on Cyber Insurance was expansively articulated by **Mr. Manoj Vijay Rane** from Alliance Insurance Brokers Private Limited. Practical scenarios in underwriting a cyber liability policy, the proposal form, questionnaire, IS/ IT & BCP policies, were all explained in detail. The steps post a typical breach was diagrammatically presented and elucidated upon. General considerations by insurers while underwriting a cyber liability policy was enlisted and explained – this was truly the cream takeaway of the session.

June 2023
It was a physical PDM for this month in Hotel Maris. **Mr. Girish Rao** from SecureV2 presented about **Protecting Application stacks.** His talk emphasized on how today's cyber-attacks are so sophisticated and get executed in runtime (millisecs) without even accessing the files system of the servers. The importance of successful detection and remediation is key defence against the unknown cyber-attacks.

All our virtual PDMs are attended by **200+ members** on an average and physical PDMs are attended by **120+ members.**

Other Chapter Activities

The chapter restarted physical mode review classes during this quarter in May 2023. **CISA review course** was kicked off on May 28th with weekend classes until 1st week of July with **16 participants**. The chapter is planning for more such review courses and have a watch on our website.

IS0 27701:2019 (Privacy Information Management System) Lead Auditor Program was conducted during May 2023. The Program had **15 participants** and they acquired knowledge on the protection of privacy in the context of processing personally identifiable information (PII), as well as audit techniques. This program was facilitated by Intertek.

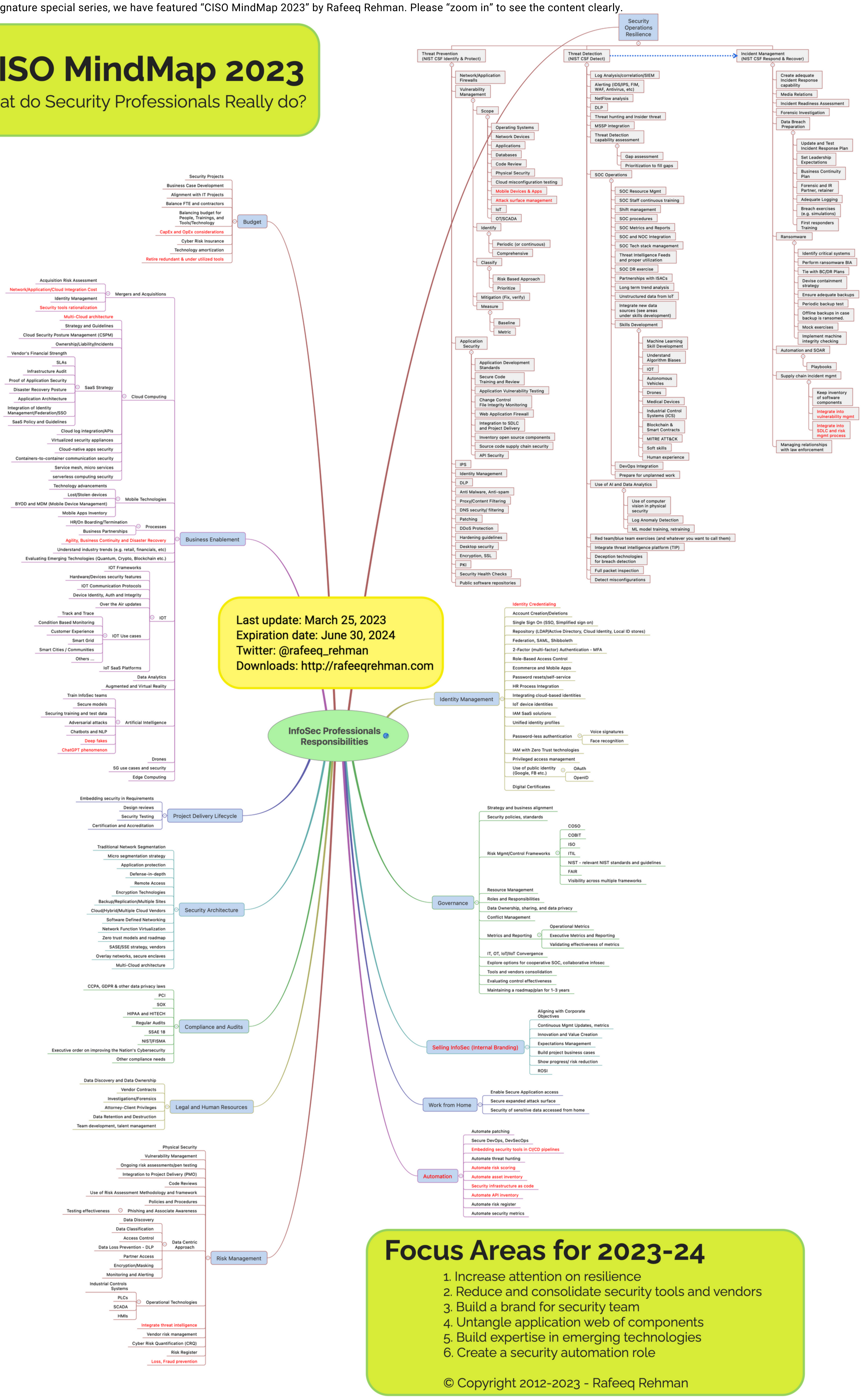
- 'T' brewed by Ms. Sangeetha N and Sripathy Raagav K

SIGNATURE SPECIAL – DIGITALLY YOURS

In our Signature special series, we have featured “CISO MindMap 2023” by Rafeeq Rehman. Please “zoom in” to see the content clearly.

CISO MindMap 2023

What do Security Professionals Really do?



Last update: March 25, 2023
Expiration date: June 30, 2024
Twitter: @rafeeq_rehman
Downloads: http://rafeeqrehman.com

InfoSec Professionals Responsibilities

- Security Operations Resilience
  - Threat Prevention (NIST CSF Identify & Protect)
    - Network/Application Firewalls
    - Vulnerability Management
      - Scope
        - Operating Systems
        - Network Devices
        - Applications
        - Databases
        - Code Review
        - Physical Security
        - Cloud misconfiguration testing
        - Mobile Devices & Apps
        - Attack surface management
        - IoT
        - OT/SCADA
      - Identify
        - Periodic (or continuous)
        - Comprehensive
      - Classify
        - Risk Based Approach
        - Prioritize
      - Mitigation (Fix, verify)
      - Measure
        - Baseline
        - Metric
    - Application Security
      - Application Development Standards
      - Secure Code Training and Review
      - Application Vulnerability Testing
      - Change Control File Integrity Monitoring
      - Web Application Firewall
      - Integration to SDLC and Project Delivery
      - Inventory open source components
      - Source code supply chain security
      - API Security
    - IPS
    - Identity Management
    - DLP
    - Anti Malware, Anti-spam
    - Proxy/Content Filtering
    - DNS security/ filtering
    - Patching
    - DDoS Protection
    - Hardening guidelines
    - Desktop security
    - Encryption, SSL
    - PKI
    - Security Health Checks
    - Public software repositories
  - Threat Detection (NIST CSF Detect)
    - Log Analysis/correlation/SIEM
    - Alerting (IDS/IPS, FIM, WAF, Antivirus, etc)
    - NetFlow analysis
    - DLP
    - Threat hunting and Insider threat
    - MSSP integration
    - Threat Detection capability assessment
      - Gap assessment
      - Prioritization to fill gaps
    - SOC Operations
      - SOC Resource Mgmt
      - SOC Staff continuous training
      - Shift management
      - SOC procedures
      - SOC Metrics and Reports
      - SOC and NOC Integration
      - SOC Tech stack management
      - Threat Intelligence Feeds and proper utilization
      - SOC DR exercise
      - Partnerships with ISACs
      - Long term trend analysis
      - Unstructured data from IoT
      - Integrate new data sources (see areas under skills development)
      - Skills Development
        - Machine Learning Skill Development
        - Understand Algorithm Biases
        - IOT
        - Autonomous Vehicles
        - Drones
        - Medical Devices
        - Industrial Control Systems (ICS)
        - Blockchain & Smart Contracts
        - MITRE ATT&CK
        - Soft skills
        - Human experience
      - DevOps Integration
      - Prepare for unplanned work
    - Use of AI and Data Analytics
      - Use of computer vision in physical security
      - Log Anomaly Detection
      - ML model training, retraining
    - Red team/blue team exercises (and whatever you want to call them)
    - Integrate threat intelligence platform (TIP)
    - Deception technologies for breach detection
    - Full packet inspection
    - Detect misconfigurations
  - Incident Management (NIST CSF Respond & Recover)
    - Create adequate Incident Response capability
    - Media Relations
    - Incident Readiness Assessment
    - Forensic Investigation
    - Data Breach Preparation
      - Update and Test Incident Response Plan
      - Set Leadership Expectations
      - Business Continuity Plan
      - Forensic and IR Partner, retainer
      - Adequate Logging
      - Breach exercises (e.g. simulations)
      - First responders Training
    - Ransomware
      - Identify critical systems
      - Perform ransomware BIA
      - Tie with BC/DR Plans
      - Devise containment strategy
      - Ensure adequate backups
      - Periodic backup test
      - Offline backups in case backup is ransomed.
      - Mock exercises
      - Implement machine integrity checking
    - Automation and SOAR
      - Playbooks
    - Supply chain incident mgmt
      - Keep inventory of software components
      - Integrate into vulnerability mgmt
      - Integrate into SDLC and risk mgmt process
    - Managing relationships with law enforcement
- Budget
  - Security Projects
  - Business Case Development
  - Alignment with IT Projects
  - Balance FTE and contractors
  - Balancing budget for People, Trainings, and Tools/Technology
  - CapEx and OpEx considerations
  - Cyber Risk Insurance
  - Technology amortization
  - Retire redundant & under utilized tools
- Business Enablement
  - Mergers and Acquisitions
    - Acquisition Risk Assessment
    - Network/Application/Cloud Integration Cost
    - Identity Management
    - Security tools rationalization
  - Cloud Computing
    - Multi-Cloud architecture
    - Strategy and Guidelines
    - Cloud Security Posture Management (CSPM)
    - Ownership/Liability/Incidents
    - SaaS Strategy
      - Vendor's Financial Strength
      - SLAs
      - Infrastructure Audit
      - Proof of Application Security
      - Disaster Recovery Posture
      - Application Architecture
      - Integration of Identity Management/Federation/SSO
      - SaaS Policy and Guidelines
    - Cloud log integration/APIs
    - VIrtualized security appliances
    - Cloud-native apps security
    - Containers-to-container communication security
    - Service mesh, micro services
    - serverless computing security
  - Mobile Technologies
    - Technology advancements
    - Lost/Stolen devices
    - BYOD and MDM (Mobile Device Management)
    - Mobile Apps Inventory
  - Processes
    - HR/On Boarding/Termination
    - Business Partnerships
  - Agility, Business Continuity and Disaster Recovery
  - Understand industry trends (e.g. retail, financials, etc)
  - Evaluating Emerging Technologies (Quantum, Crypto, Blockchain etc.)
  - IOT
    - IOT Frameworks
    - Hardware/Devices security features
    - IOT Communication Protocols
    - Device Identity, Auth and Integrity
    - Over the Air updates
    - IOT Use cases
      - Track and Trace
      - Condition Based Monitoring
      - Customer Experience
      - Smart Grid
      - Smart Cities / Communities
      - Others ...
    - IoT SaaS Platforms
  - Data Analytics
  - Augmented and Virtual Reality
  - Artificial Intelligence
    - Train InfoSec teams
    - Secure models
    - Securing training and test data
    - Adversarial attacks
    - Chatbots and NLP
    - Deep fakes
    - ChatGPT phenomenon
  - Drones
  - 5G use cases and security
  - Edge Computing
- Project Delivery Lifecycle
  - Embedding security in Requirements
  - Design reviews
  - Security Testing
  - Certification and Accreditation
- Security Architecture
  - Traditional Network Segmentation
  - Micro segmentation strategy
  - Application protection
  - Defense-in-depth
  - Remote Access
  - Encryption Technologies
  - Backup/Replication/Multiple Sites
  - Cloud/Hybrid/Multiple Cloud Vendors
  - Software Defined Networking
  - Network Function Virtualization
  - Zero trust models and roadmap
  - SASE/SSE strategy, vendors
  - Overlay networks, secure enclaves
  - Multi-Cloud architecture
- Compliance and Audits
  - CCPA, GDPR & other data privacy laws
  - PCI
  - SOX
  - HIPAA and HITECH
  - Regular Audits
  - SSAE 18
  - NIST/FISMA
  - Executive order on improving the Nation's Cybersecurity
  - Other compliance needs
- Legal and Human Resources
  - Data Discovery and Data Ownership
  - Vendor Contracts
  - Investigations/Forensics
  - Attorney-Client Privileges
  - Data Retention and Destruction
  - Team development, talent management
- Risk Management
  - Physical Security
  - Vulnerability Management
  - Ongoing risk assessments/pen testing
  - Integration to Project Delivery (PMO)
  - Code Reviews
  - Use of Risk Assessment Methodology and framework
  - Policies and Procedures
  - Phishing and Associate Awareness
    - Testing effectiveness
  - Data Centric Approach
    - Data Discovery
    - Data Classification
    - Access Control
    - Data Loss Prevention - DLP
    - Partner Access
    - Encryption/Masking
    - Monitoring and Alerting
  - Operational Technologies
    - Industrial Controls Systems
    - PLCs
    - SCADA
    - HMIs
  - Integrate threat intelligence
  - Vendor risk management
  - Cyber Risk Quantification (CRQ)
  - Risk Register
  - Loss, Fraud prevention
- Identity Management
  - Identity Credentialing
  - Account Creation/Deletions
  - Single Sign On (SSO, Simplified sign on)
  - Repository (LDAP/Active Directory, Cloud Identity, Local ID stores)
  - Federation, SAML, Shibboleth
  - 2-Factor (multi-factor) Authentication - MFA
  - Role-Based Access Control
  - Ecommerce and Mobile Apps
  - Password resets/self-service
  - HR Process Integration
  - Integrating cloud-based identities
  - IoT device identities
  - IAM SaaS solutions
  - Unified identity profiles
  - Password-less authentication
    - Voice signatures
    - Face recognition
  - IAM with Zero Trust technologies
  - Privileged access management
  - Use of public identity (Google, FB etc.)
    - OAuth
    - OpenID
  - Digital Certificates
- Governance
  - Strategy and business alignment
  - Security policies, standards
  - Risk Mgmt/Control Frameworks
    - COSO
    - COBIT
    - ISO
    - ITIL
    - NIST - relevant NIST standards and guidelines
    - FAIR
    - Visibility across multiple frameworks
  - Resource Management
  - Roles and Responsibilities
  - Data Ownership, sharing, and data privacy
  - Conflict Management
  - Metrics and Reporting
    - Operational Metrics
    - Executive Metrics and Reporting
    - Validating effectiveness of metrics
  - IT, OT, IoT/IIoT Convergence
  - Explore options for cooperative SOC, collaborative infosec
  - Tools and vendors consolidation
  - Evaluating control effectiveness
  - Maintaining a roadmap/plan for 1-3 years
- Selling InfoSec (Internal Branding)
  - Aligning with Corporate Objectives
  - Continuous Mgmt Updates, metrics
  - Innovation and Value Creation
  - Expectations Management
  - Build project business cases
  - Show progress/ risk reduction
  - ROSI
- Work from Home
  - Enable Secure Application access
  - Secure expanded attack surface
  - Security of sensitive data accessed from home
- Automation
  - Automate patching
  - Secure DevOps, DevSecOps
  - Embedding security tools in CI/CD pipelines
  - Automate threat hunting
  - Automate risk scoring
  - Automate asset inventory
  - Security infrastructure as code
  - Automate API inventory
  - Automate risk register
  - Automate security metrics

Focus Areas for 2023-24

1. Increase attention on resilience
2. Reduce and consolidate security tools and vendors
3. Build a brand for security team
4. Untangle application web of components
5. Build expertise in emerging technologies
6. Create a security automation role

How to use CISO MindMap?
There are different ways people use the CISO MindMap. Following are some of the ways this MindMap is quite helpful:

- Have you been asked what you really do as a security professional? The CISO MindMap explaining the complexity of a CISO job, especially to a business audience.
- A means for guiding conversation with other technology professionals.
- SANS Institute uses it as part of the Security Leadership Poster.
- Designing and refining security programs.
- Some security vendors use the MindMap for awareness.
- CISO group discussions and/or community meetings.
- For aspiring security professionals, understand the landscape and decide their career path.
- An educational and awareness tool.

The stress on people who have these responsibilities is real. If nothing else, this MindMap should help leaders recognize that stress and do something about it.

Recommendations for 2023-2024:
Every year, the Author makes recommendations as a practitioner and based upon conversations with infosec leaders. These are not “predictions” of the future but rather “what is needed now” to strengthen security programs.

1. **Increase Attention on Resilience** – Evaluate ransomware defences, detection and response capabilities, perform a business impact analysis and identify critical processes, applications and data. Test ability to restore systems and data within an acceptable time frame. Understand that merely having a backup is not enough. Ability to rebuild impacted systems and restore backups in a timely manner is crucial to bring business back to normal operating conditions after security incidents.
2. **Reduce and Consolidate Security Tools** – More security tools don’t necessarily reduce risk but do add the need for maintaining expertise on security teams. While deciding which tools to keep or retire, think about functionality overlap, future direction, innovation on the part of vendors.
3. **Build a Brand for Security Team** – While the message is important, the credibility of the messenger is also crucial. To serve business better, train security team staff on business acumen, value creation, influencing people without authority, and human experience. This recommendation was in the list last year as well and we need to keep focus on the fact that information security teams don’t live in a vacuum and have to enable business and interact with others.
4. **Untangle Application Web of Components** – Modern applications have become a web of interconnected components, APIs, multiple cloud and data centers, open source libraries, third party services like DNS, email, content delivery vendors, and so on. Even when you purchase a commercial off the shelf application/software, it may rely on third party APIs and services. Understand how business applications work, take an inventory of all components that they rely on, and make it part of your vulnerability management program
5. **Build Expertise in Emerging Technologies** – By now everyone has heard about ChatGPT and competing technologies from other vendors. Build team expertise in technology fields including machine learning (ML) models, model training, API security, service mesh, containers, DevSecOps.
6. **Create a Security Automation Role** – Managing security program cost and working at “machine speed” requires automation. This is a new section added to CISO MindMap this year. Automate maintaining a risk register, asset (hardware, software, APIs, etc.) inventory, scanning and testing. Many tools used in CI/CD pipelines as part of DevOps are useful for automation. However, simple scripting goes a long way in reducing overhead of routine tasks. Automating security metrics such that you can see the current state of your security program anytime you need to, almost in real time. It is not an easy task but it is doable and some organizations do it on scale.

Source: https://rafeeqrehman.com/ciso-mindmap/
Note: We have obtained author’s permission to use the mind map in our newsletter.

~~Milk~~ Handshake – Member Delight Series

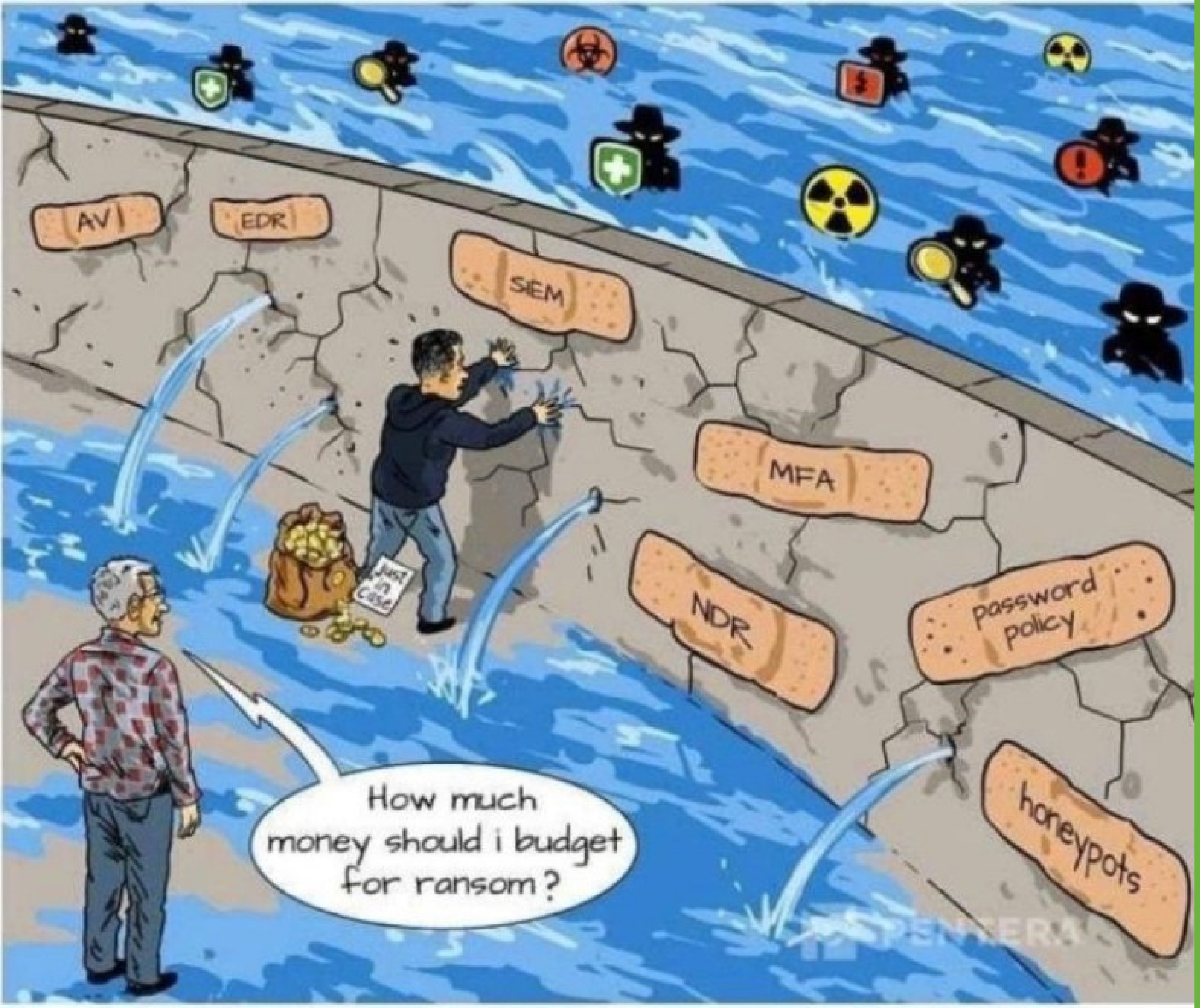
Get to know of a Chapter member and his/her Journey with the ISACA Chennai Chapter - This time it is a Tete-a-Tete between our Chapter Members Mrs. Choodamani Vasudevan and Ms. Sangeetha N – Sometimes a 'HANDSHAKE' is all it takes to initiate a Communication Session. This podcast covers volunteering experiences of Mrs. Choodamani with our Chapter and she also talks about Environmental Sustainability and Governance (ESG) – specially on the 17 Sustainable Development Goals (SDG) defined by the United Nations and how can organizations achieve them. Grab your ear pods and listen in to the podcast below.

Access the Podcast here

Note: The views expressed here are the individual views of the respective members and are not representative of any organization or any certification bodies to which they are affiliated to.

Stress Test - Try Desserts - Laught out Loud n Reflect too!! 🤣

"........to manage risk on accidental shredding, suggest you to take a photocopy before we start......."



I CHANGED ALL MY PASSWORDS TO "INCORRECT".
SO WHENEVER I FORGET, IT WILL TELL ME "YOUR PASSWORD IS INCORRECT."

Source: LinkedIn and Google

~~PAAN~~ PAM SUPARI – a good achievement (meal) should last forever!

In this section, we pass on our appreciatiation to ISACA exam passers and share their success stories as well.

CISA
Certified Information Systems Auditor.
An ISACA Certification

- Thomalakrishnan Selvakumar
- Lokesh Kabeerdoss
- Vivek Kumar Ranjan
- Jeyalakshmi K
- Hariharan Vijayan Nair
- Vasanth Nagarajan
- Kumar SSSK
- Hariharaputhran Venkateshwaran
- Ashish Yadav
- Kanagarajan v
- Anshuma Sharma
- Durga Sundheer

CISM
Certified Information Security Manager.
An ISACA Certification

- Stephen Emmanuel
- Vigirtheeswaran G. T.
- Abhijit Mishra
- K. Arthi
- Vivek Samiaiya
- Venkatesan Kesavan
- Anuscia Joscie Anand
- Vivek Samiaiya

CRISC
Certified in Risk and Information Systems Control.
An ISACA Certification

- Revathy Natarajan
- Navien P S S
- Parthasarathy

If you're aspiring to be a Infosec manager this is certainly an exam that you must work towards.
-- Stephen Emmanuel - Passed CISM

What I felt that the questions were straight through and not much tricky. All the options looks similar but if we are strong in the concepts, we will be able to rule out the wrong options. Time is sufficient in the exam. Instead of find correct answer, I took the approach of eliminating wrong option one by one and I was able to get the best answer. I took online video course and went through it in detailed multiple times. I attempted 20 mock tests in one month and prepared notes for last day revision. With all these efforts, I was able to sail through the exam.
-- Vivek Kumar Ranjan - Passed CISA

It was fully loaded and well balanced exam, which requires technical and management based approach to solve the real life real time issue. After passing the exam, it is imperative that we continuously update ourselves to stay focused and fulfils all information security management related requirements of the business.
-- Ashish Yadav - Passed CISA

For me early morning preparation was comfortable. I relied on only ISACA study materials. I took notes on all the concepts while reading page by page of CISM manual and revisited with ISACA's video manual which helped me to recollect all the concepts. The practice tests and the mock test help me to understand my strength and weaknesses. I have learnt from my first attempt and cracked the 2nd. Local chapter training will give the glimpse and road map for the preparation.
-- Vigirtheeswaran G. T. - Passed CISM

I attended training at the Chennai Chapter and read the book every day for two hours and I passed my exam. Thanks to my mentor who supported me for exam preparation.
-- **K. Arthi - Passed CISM**

During my preparation of the CISM exam, I did learn the basics and background of the information security program management, it helped me hone my skills as a manager, and did aid my thinking in terms of designing and leading an information security function. Not just the certification adds value to one’s profile, it improvises and fine tunes one’s skills. I see ISACA certifications as a trust-worthy path to up-skill myself and learn the nuances.
-- Anuscia Joscie Anand - Passed CISM

ISACA
Chennai Chapter

Trust you all enjoyed our delicious spread @ Chennai Secure 'T' Café
Do drop by @ this space each quarter for more interesting feeds Menu

Give us your esteemed feedback @ https://forms.office.com/r/qjiYn0FAMU. It takes less than 2 minutes to complete the form.

Newsletter Editors:
Sangeetha N and Sripathy Raagav K (ERT group members)
Newsletter Editorial Review:
Jayasree Chandrasekaran and Vaidyanathan Chandramouli

ISACA CHENNAI CONFERENCE 2023

Conference Dates
September 8 & 9, 2023

Pre-Conference Workshop
September 7, 2023

Venue
Le Royal Meridian
Guindy, Chennai - 600032

Diamond and Title Partner

Raksha TECHNOLOGIES 360° Cyber Security

HCLSoftware · txOne networks · VARONIS · SentinelOne · pagEntra

Knowledge Partner (Platinum)

SkillsDA® Center for advance training

Gold Partners

VAULT INFOSEC YOUR SECURITY, OUR VOW · SOPHOS · TÜV SÜD · CYBLE · Qualys. · इंडियन बैंक Indian Bank इलाहाबाद ALLAHABAD

Silver Partners

sify · TMB Tamilnad Mercantile Bank Ltd Be a step ahead in life · Finstein Unleashing Cybersecurity Brilliance, the Einstein Way! · Sukra Infotek FUTURISTIC SOLUTIONS · intertek Total Quality. Assured. · WHITESWAN IDENTITY SECURITY

Associate partners

Risk · Pro · rezilyens

Pre-conference workshop partners

SkillsDA® Center for advance training · Finstein Unleashing Cybersecurity Brilliance, the Einstein Way! · CYSECURITY