Professional Opportunities in Cyber Security

CA Narasimhan Elangovan

Partner KEN & Co.

Narasimhan Elangovan

B.Com, FCA, CS, DISA(ICAI), DipIFR(UK), CISA(USA), LLB, CDPSE(USA), ISO 27001 Lead Auditor

Partner
KEN & Co. Chartered Accountants, Bengaluru.

- Practicing Chartered Accountant with specialization in Information System Assurance
- A futurist who specializes in
  - IT Consulting, Information Systems Assurance and InfoSec
  - GDPR & Privacy Law
  - Data Analytics, Implementation and Testing of Internal Financial Controls
  - SOX and SOC (SSAE-16 and 18)
- IS Auditor and Advisor for various BFSI, Sporting Organizations, start-up entities, Tech companies and many more
- Faculty for CISA, DISA and Courses on Blockchain
- Speaker at National & International Forums of IT and Emerging Technologies
- Author
  - "Digitizing CA Practice"
  - Co-author to the Implementation Guide on DCMM 2.0
  - DISA 3.0 – Module 6 on Emerging Technologies
  - Strategic roadmap for CA firms to operate as virtual firms
  - Technical Guide on Internet of Things

Disclaimer

- The views and apps discussed in this session is only for information purpose and are the personal views of the presenter. The presenter is a practising CA and does not have any interest in any of the applications discussed and neither endorses any application.
- The views expressed herein may not be taken to necessarily represent the views of his firm, M/s. KEN & Co. Chartered Accountants.
- Readers are advised to take caution before choosing any of the applications.
- This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment.
- No part of this material shall be construed as a solicitation of services or an invitation of any sort whatsoever from KEN & Co or to create a professional relationship.

Agenda

1. IT Audit
2. Regulatory Frameworks and Standards
3. ITGC
4. SOC / SSAE 3402
5. Third Party Vendor
6. Data Privacy
7. VAPT
8. ISO 27001
9. Virtual CISO
10. Forensics
11. Emerging Technologies

IT Audit

Key features of an automated environment

An automated environment is an ecosystem that **combines people, processes and technology** within an overall business environment.

Automated environments are driven by computer-based systems / information technology systems.

Layers of an automated environment

Databases
- Oracle 12 g, MS-SQL server

Operating systems
- Windows, Linux

Storage devices
- disks, tapes

Network devices
- switches, routers

Networks
- LAN, WAN

Physical environment
- CCTVs, Temperature controls

Regulatory Framework & Standards

Regulatory Requirement for Audit of IT Systems

Companies Act, 2013	Implementation of Internal Financial Controls Audit of IFC
IRDA	All insurers shall have their systems and process audited at least once in 3 years by a CA firm
RBI – Banks / NBFC / Cooperative / RRB	Qualifications such as CISA (offered by ISACA), DISA (offered by ICAI), or CISSP (offered by ISC2), along with two or more years of IS Audit experience, are desirable
SEBI	Intermediaries to be subject to audit based on the Terms of Reference

Guidelines and Procedures – using relevant frameworks and best practices

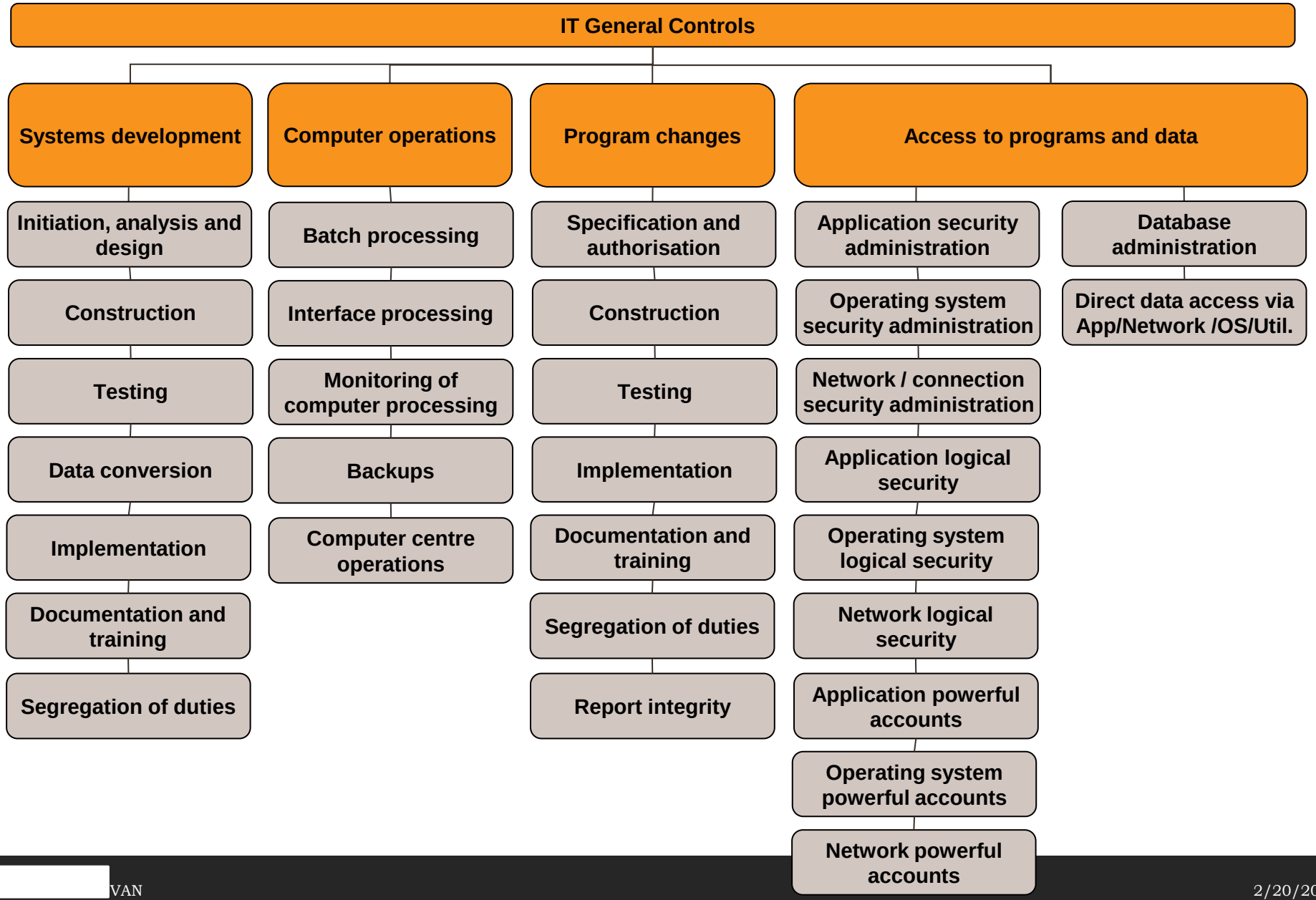
- Standards on Auditing issued by the Institute of Chartered Accountants of India,
- Section 143 of Companies Act
- Guidance Note on Audit of Internal Financial Controls Over Financial Reporting issued by the ICAI.
- Sarbanes Oxley Act of 2002
- ISO 27001:2013 is the Information Security Management System (ISMS)
- ITIL (Information Technology Infrastructure Library) and ISO 20000
- Control Objectives for Information and Related Technologies (CoBIT)
- The Cybersecurity Framework (CSF)
- COSO
- PCIDSS

ITGC

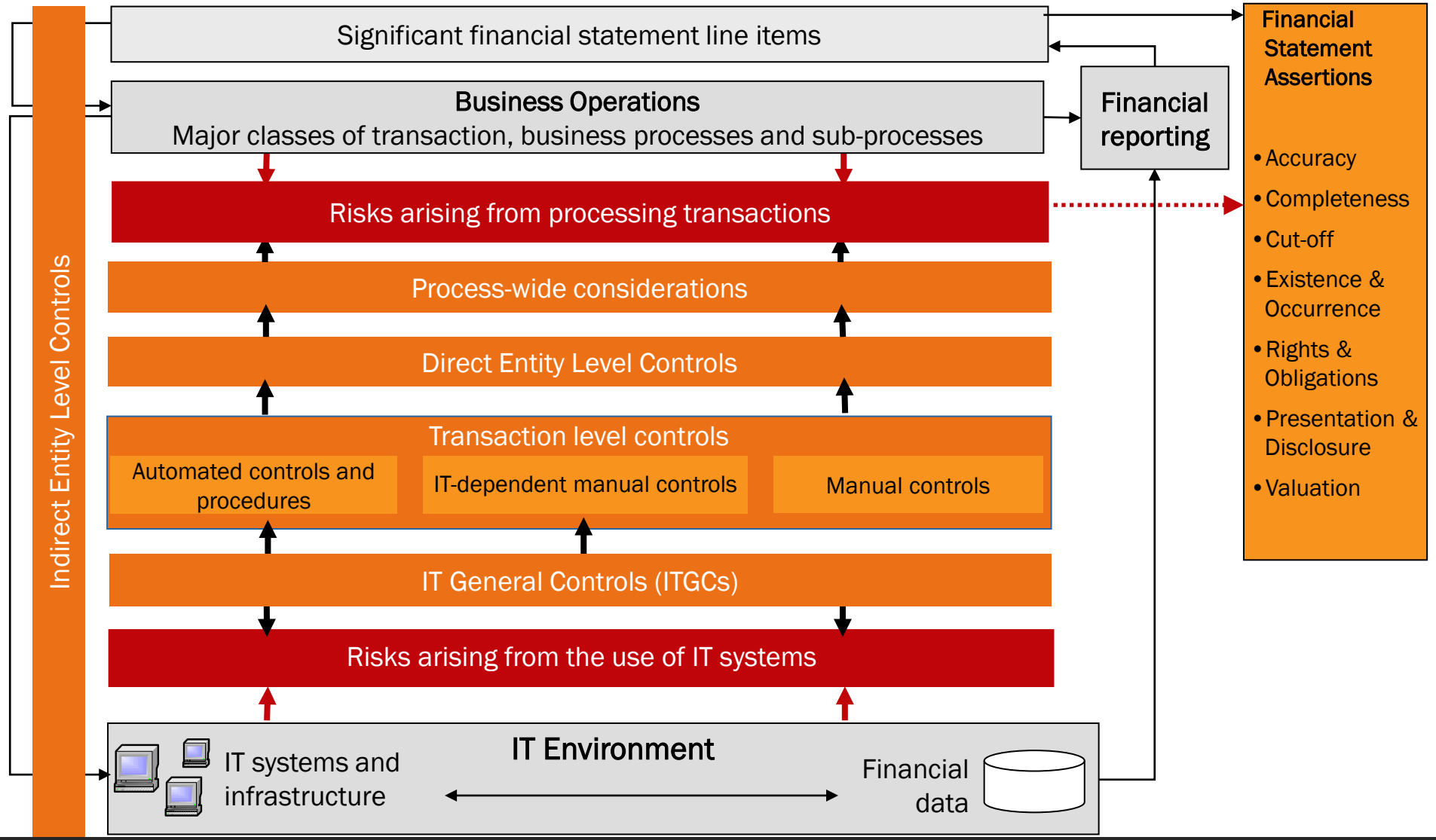
IT General Controls

- General IT Controls: “General IT controls are policies and procedures that relate to many applications and support the effective functioning of application controls. They apply to main frame, mini-frame, and end-user environment.
- General IT-controls that maintain the integrity of information and security of data commonly include controls over the following
  - Data centre and network operations;
  - Program change;
  - Access security;
  - Application system acquisition, development, and maintenance (Business Applications).
- These are IT controls generally implemented to mitigate the IT specific risks and applied commonly across multiple IT systems, applications and business processes.
- General IT controls are known as “pervasive” controls or “indirect” controls

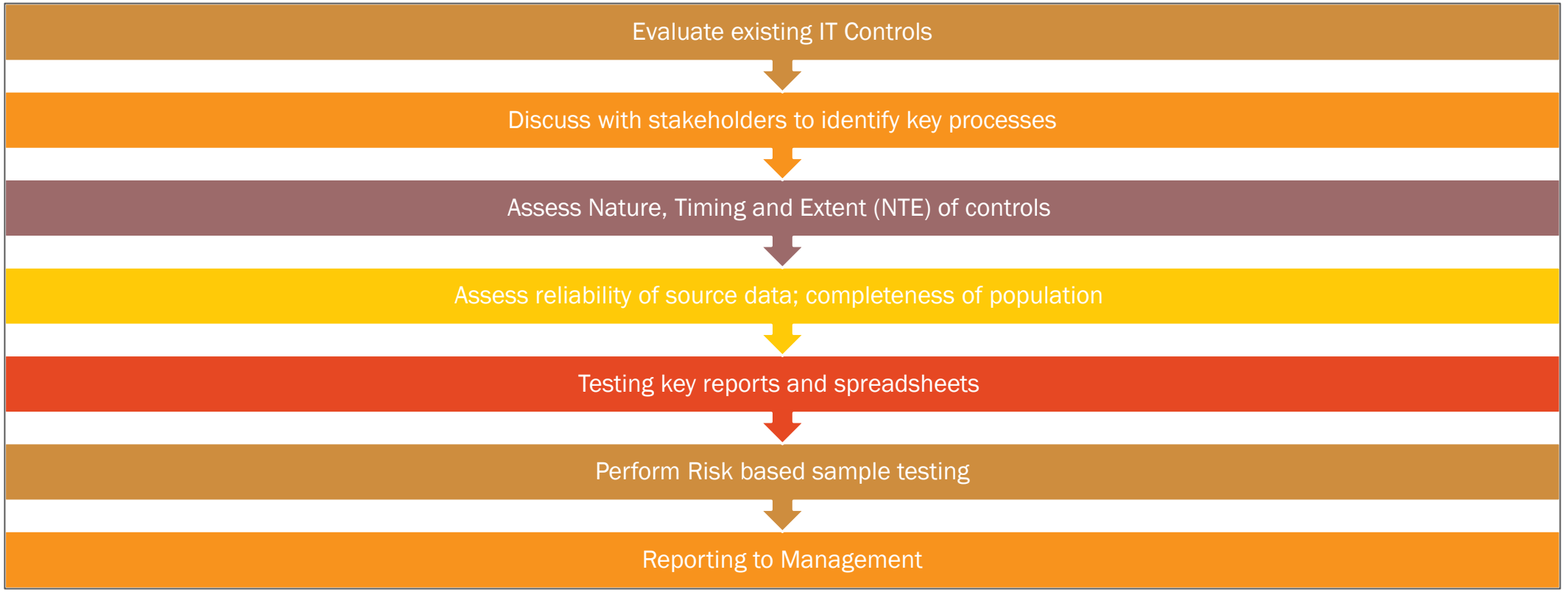
The Complete picture

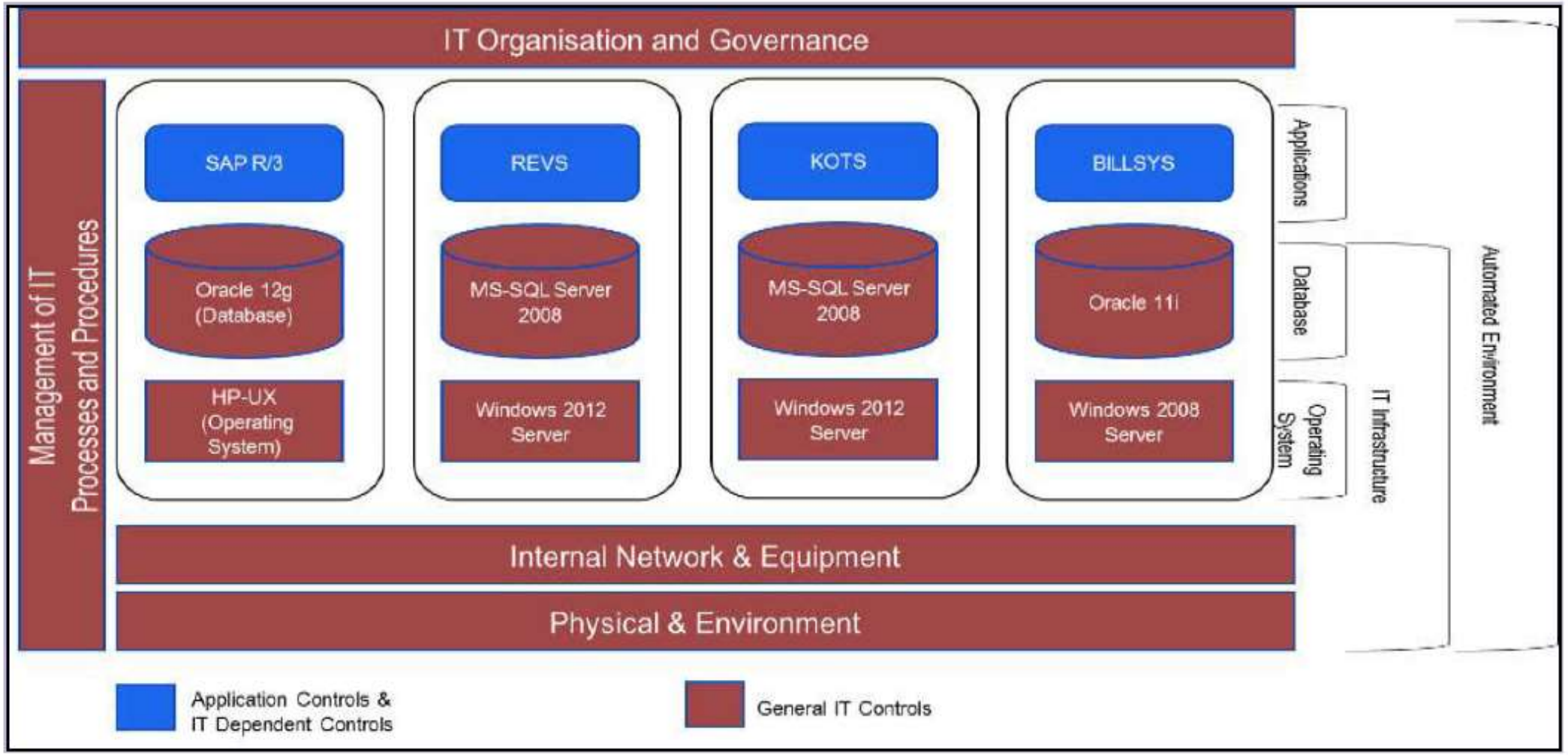


Where Do ITGCs Fit In?



Testing ITGC – Ideal Process




IT Organisation and Governance
Management of IT Processes and Procedures
SAP R/3
Oracle 12g (Database)
HP-UX (Operating System)
REVS
MS-SQL Server 2008
Windows 2012 Server
KOTS
MS-SQL Server 2008
Windows 2012 Server
BILLSYS
Oracle 11i
Windows 2008 Server
Applications
Database
Operating System
IT Infrastructure
Automated Environment
Internal Network & Equipment
Physical & Environment
Application Controls & IT Dependent Controls
General IT Controls

Regulatory Driven

RBI – NBFC

- Master Direction - Information Technology Framework for the NBFC Sector
  - NBFCs with asset size below ₹ 500 crore
    - IT Governance,
    - IT Policy,
    - Information & Cyber Security,
    - IT Operations,
    - IS Audit,
    - Business Continuity Planning and
    - IT Services Outsourcing.
  - NBFCs with asset size more than ₹ 500 crore
- As of January 31, 2021, there were 9,507 NBFCs registered with the RBI.

RBI - Banks

- Similar such requirement for all banks / Co-operatives / RRBs etc
- Domains include :
  - Information Technology Governance
  - Information Security
  - IT operations
  - IT services outsourcing
  - IS Audit
  - Cyber frauds
  - Business Continuity Planning
  - Customer education
  - Legal issues

IRDA - Guidelines

- Asset Management
- Access Control
- Asset Management
- Business Continuity Management
- Cloud Security
- Communication Security
- Compliance
- Compliance with legal requirements
- Cryptography
- Human resource security
- Information security in supplier relationships
- Information security incident management
- Information security policy
- Operations security
- Organization of information security
- Physical Access and Environmental controls
- System acquisition, development and maintenance

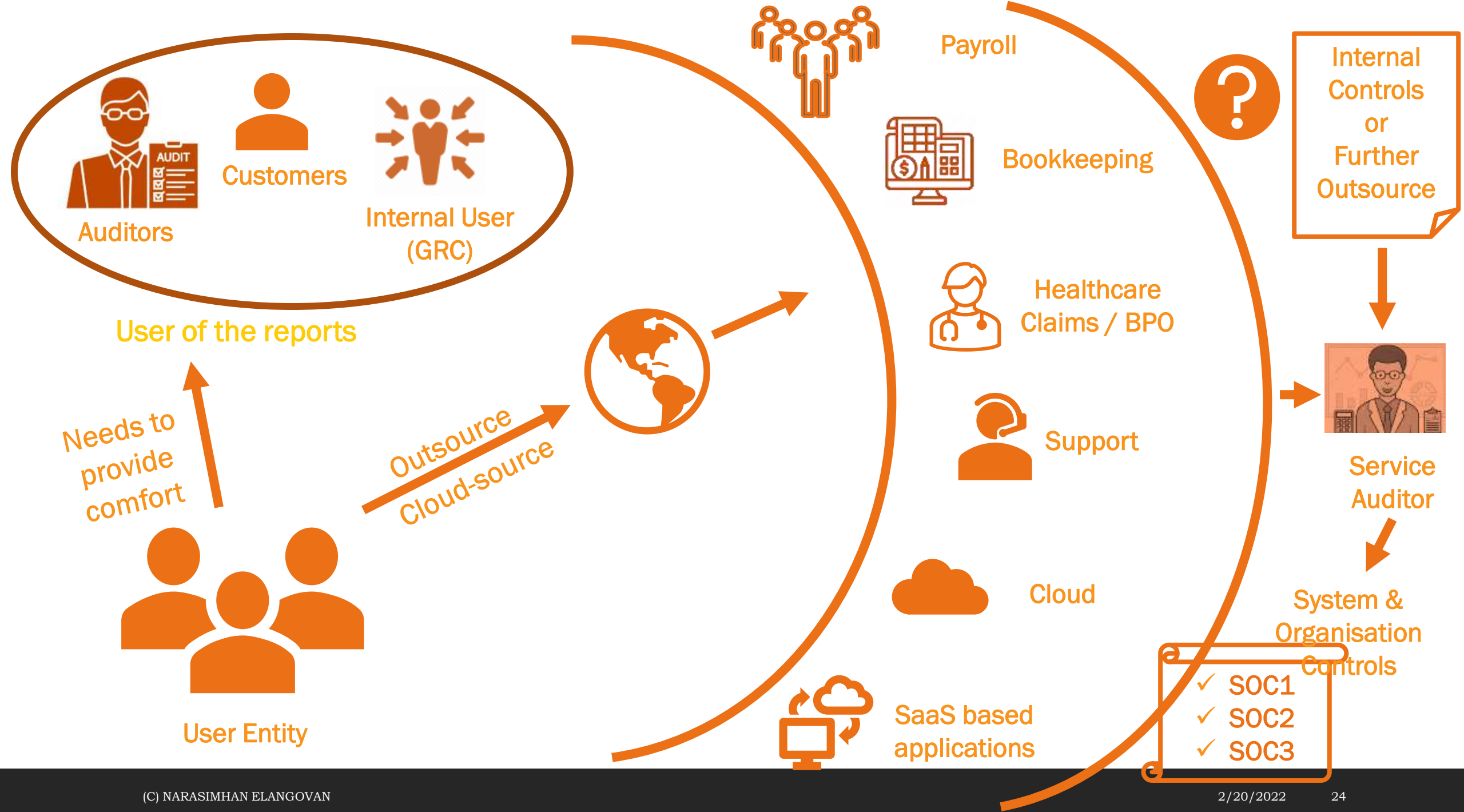
IRDA - ISNP (E-Commerce on Insurance Self-Network Platform) Audit

- Online offering
- Internet Website and mobile app
- Disclosures
- Pre-sale solicitation
- Information sharing with Prospect
- Products
- Pricing
- Commission or remuneration to the Insurance Self-Network Platform
- Proposal Form
- Compliance to KYC/ AML norms
- Creation of e-Insurance Account
- Payment of premium
- Issuance of e-Insurance policies
- Servicing of Policies
- Privacy of personal information and data security
- Display
- Grievances
- Fraud
- Maintenance of records
- Standard Operating Procedure
- Supervision and Control
- Compliance
- Reporting requirements
- Other issues
- Further powers of the Authority.

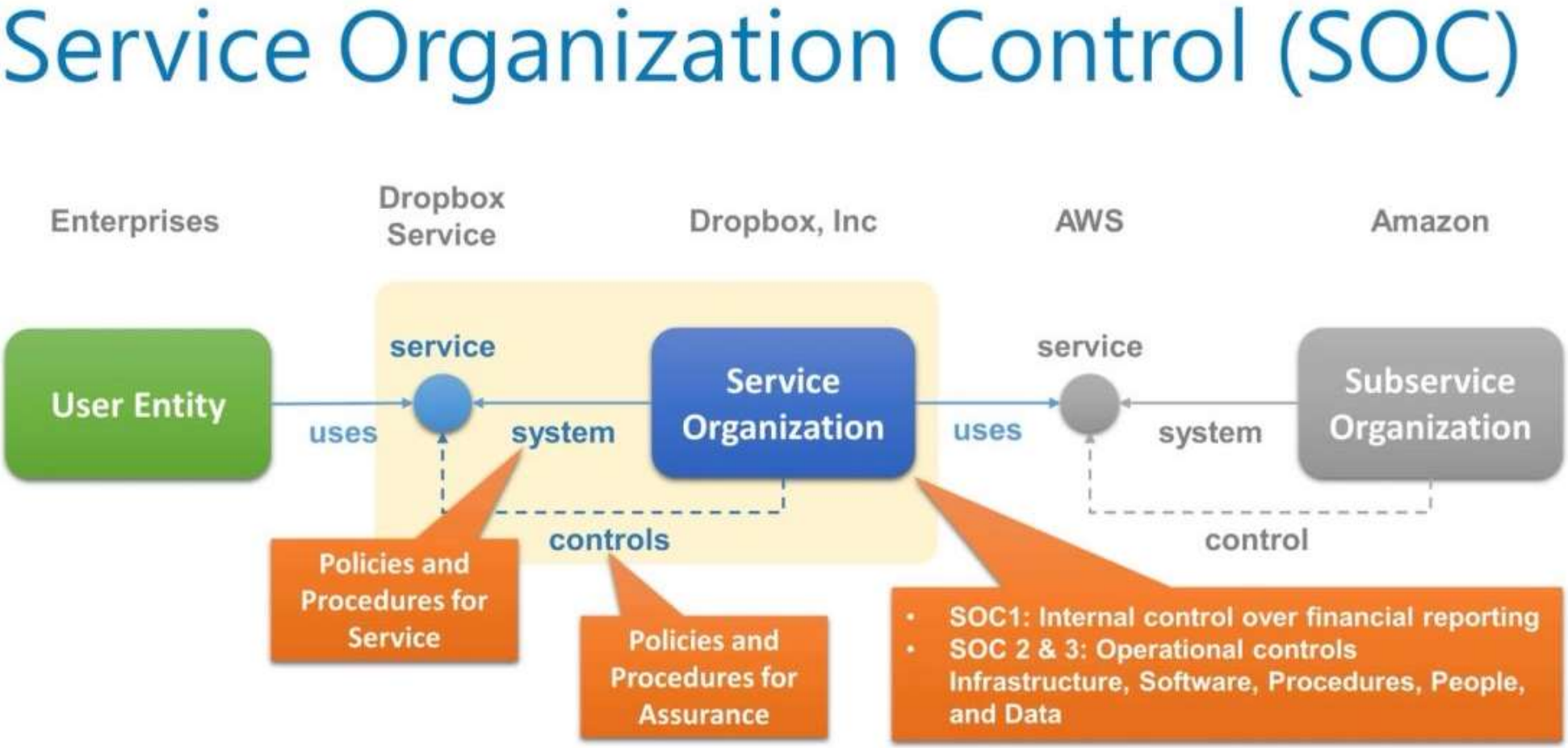
SEBI - Cyber Security & Cyber Resilience framework

- Governance
- Protection
- Access Controls
- Physical Security
- Network Security Management
- Data Security
- Hardening
- Patch Mgmt.
- VAPT
- Monitoring and Detection
- Sharing Information
- Vendor Mgmt.


SOC


Auditors
Customers
Internal User (GRC)
User of the reports
Needs to provide comfort
User Entity
Outsource
Cloud-source
Payroll
Bookkeeping
Healthcare Claims / BPO
Support
Cloud
SaaS based applications
Internal Controls or Further Outsource
Service Auditor
System & Organisation Controls
SOC1
SOC2
SOC3

An Illustrative Case



What is SOC?

SOC stands for System and Organization Controls.

An SOC report is published by an audit firm and documents their independent opinion on the **design and/or operating effectiveness of internal controls relevant to the services provided to their customers.**

Per the Sarbanes–Oxley Act of 2002, USA, public companies are made responsible for the maintenance of an effective system of controls over financial reporting.

Internal control reports on the services provided by a service organization providing valuable information that users need to assess and address the risks associated with an outsourced service

SAE 3402

SAE 3402

SAE 3402 deals with the assurance engagement that provides a service relevant to the user entities' internal control as it related to financial reporting.

This standard applies only when the service organizations are responsible for, or otherwise make an assertion about the suitable designs of control.

SAE 3402 is effective for service auditor's assurance reports covering periods ending on or after April 1, 2011.

Objective

Obtain reasonable assurance in all material aspects of the service organization's description-

- Systems are designed and implemented throughout the specified period
- System’s control objectives are suitably designed throughout the specified period
- Controls were operated effectively in accordance with the control objectives

Report on the above matters in accordance with the service auditor’s findings

What is Third Party Risk?

Third Party Risk

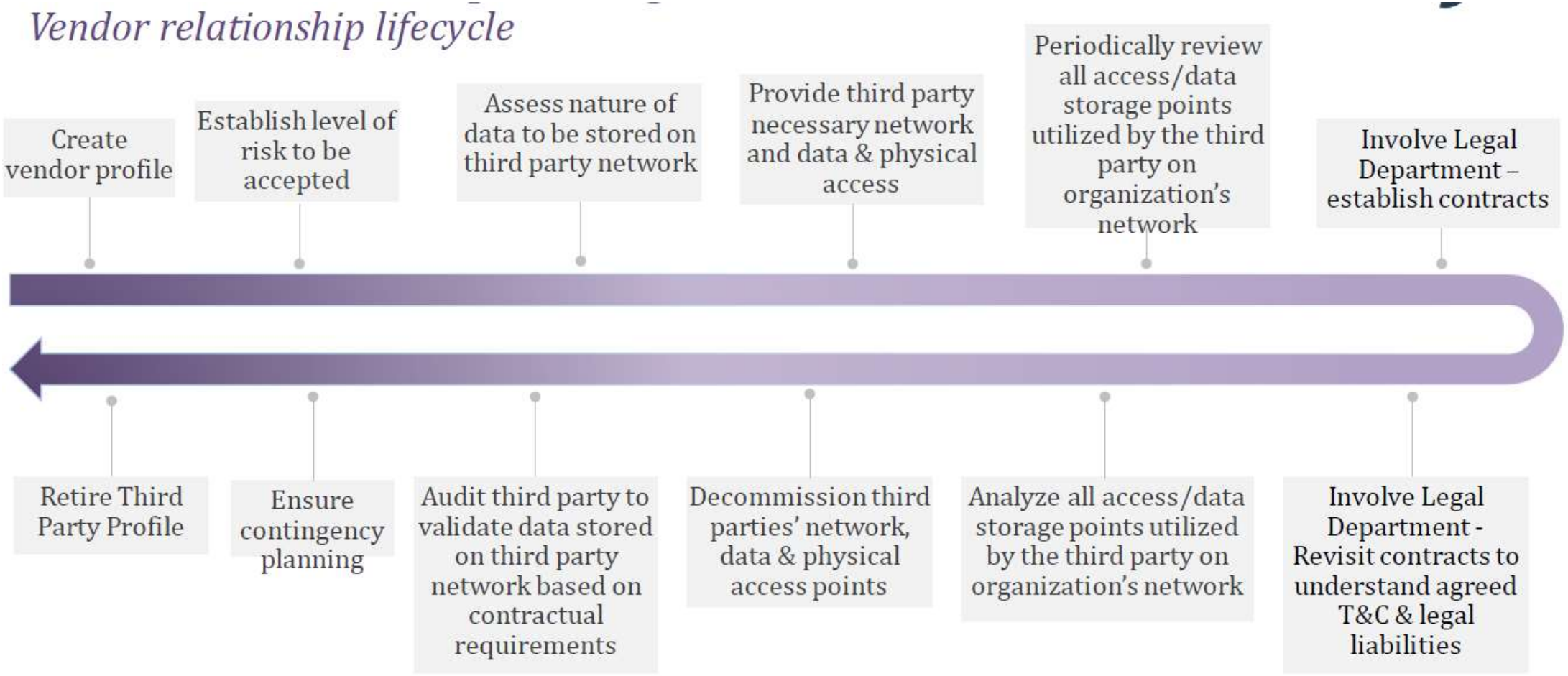
- Used to define suppliers, vendors, sub-contractors etc.
- A 'third party' is defined as any entity that a company does business with. This may include suppliers, vendors, contract manufacturers, business partners and affiliates, brokers, distributors, resellers, and agents.
- Third parties can be both 'upstream' (suppliers and vendors) and 'downstream', (distributors and re-sellers) as well as non-contractual parties.

Reference : As defined in Office of the Comptroller of the Currency (OCC), US, OCC Bulletin 2013-29 on Third-Party Relationships: Risk Management Guidance

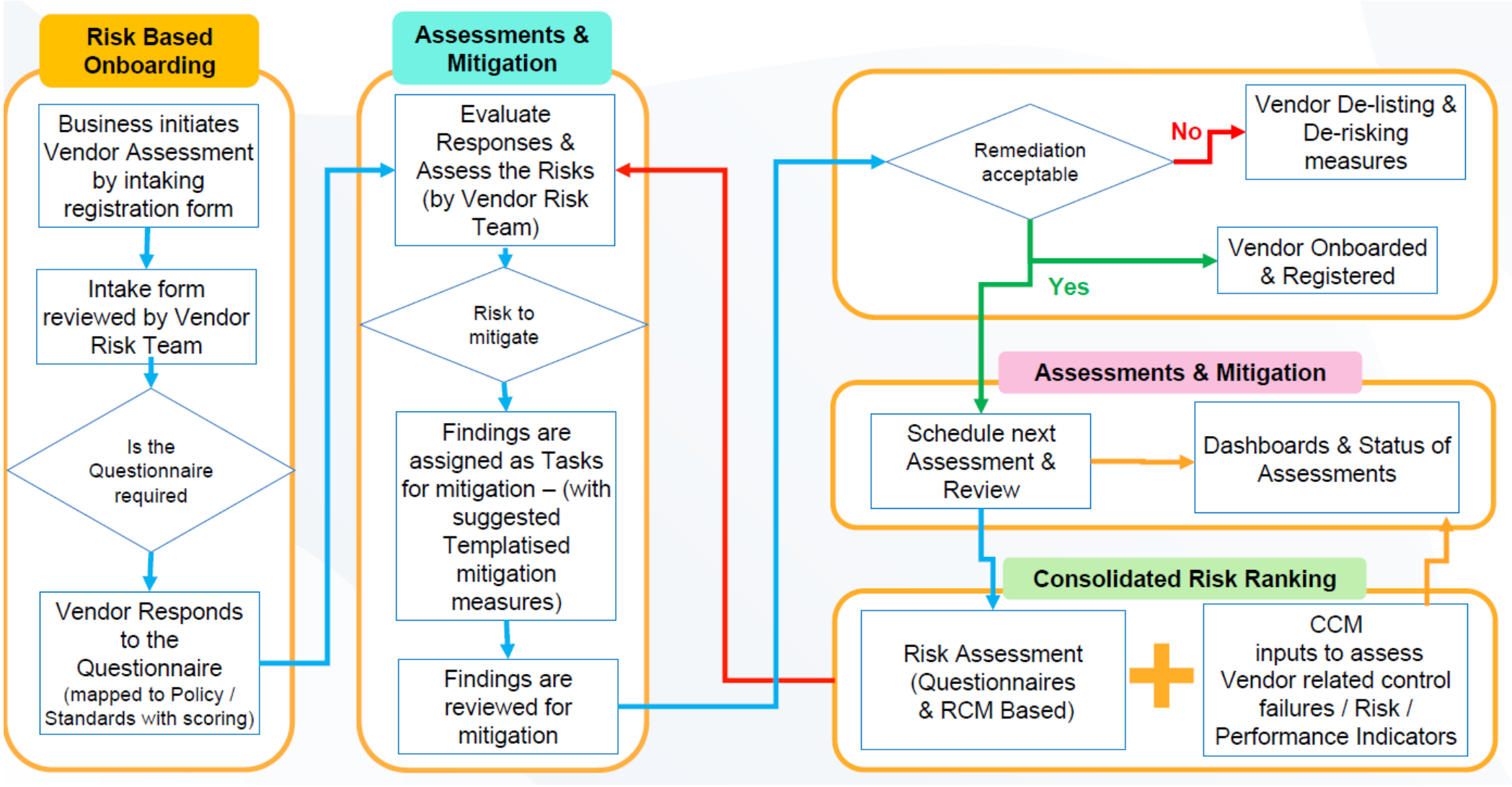
Supply Chain Technology Risk

- When companies began extensive outsourcing and globalizing the supply chain, they did so without understanding the risks suppliers posed.
- Lack of supplier attention to quality management could compromise the brand and business.
- From logistics to environmental, pandemic to geo-political there are many risks which could impact business.
- Technology & digitalization of supply chain has opened up new technology risks. With the global increase in cyber attacks, cybersecurity threats has become a major business risk.

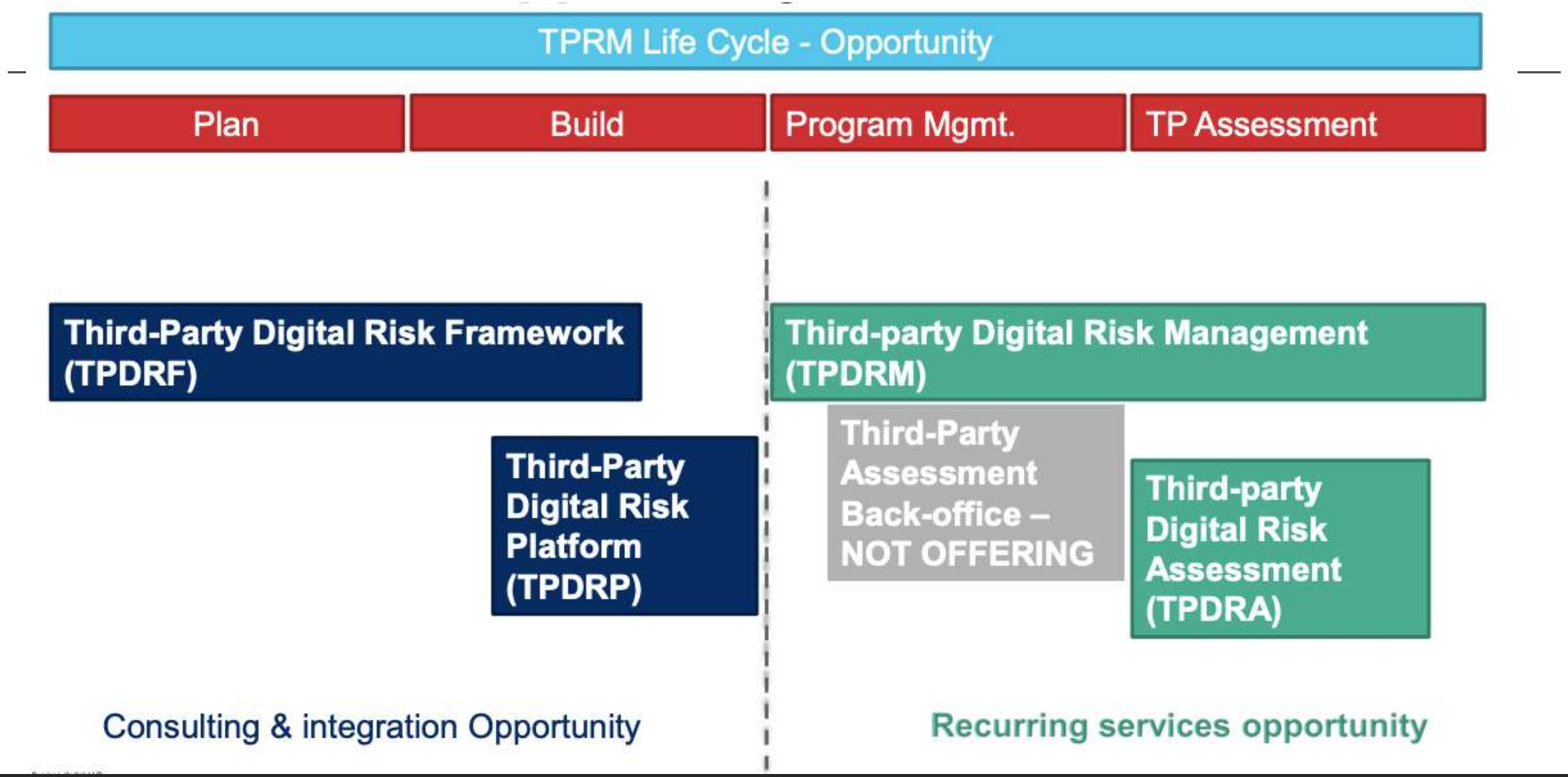
Vendor relationship lifecycle



Typical Cycle



TPRM Services - Opportunity

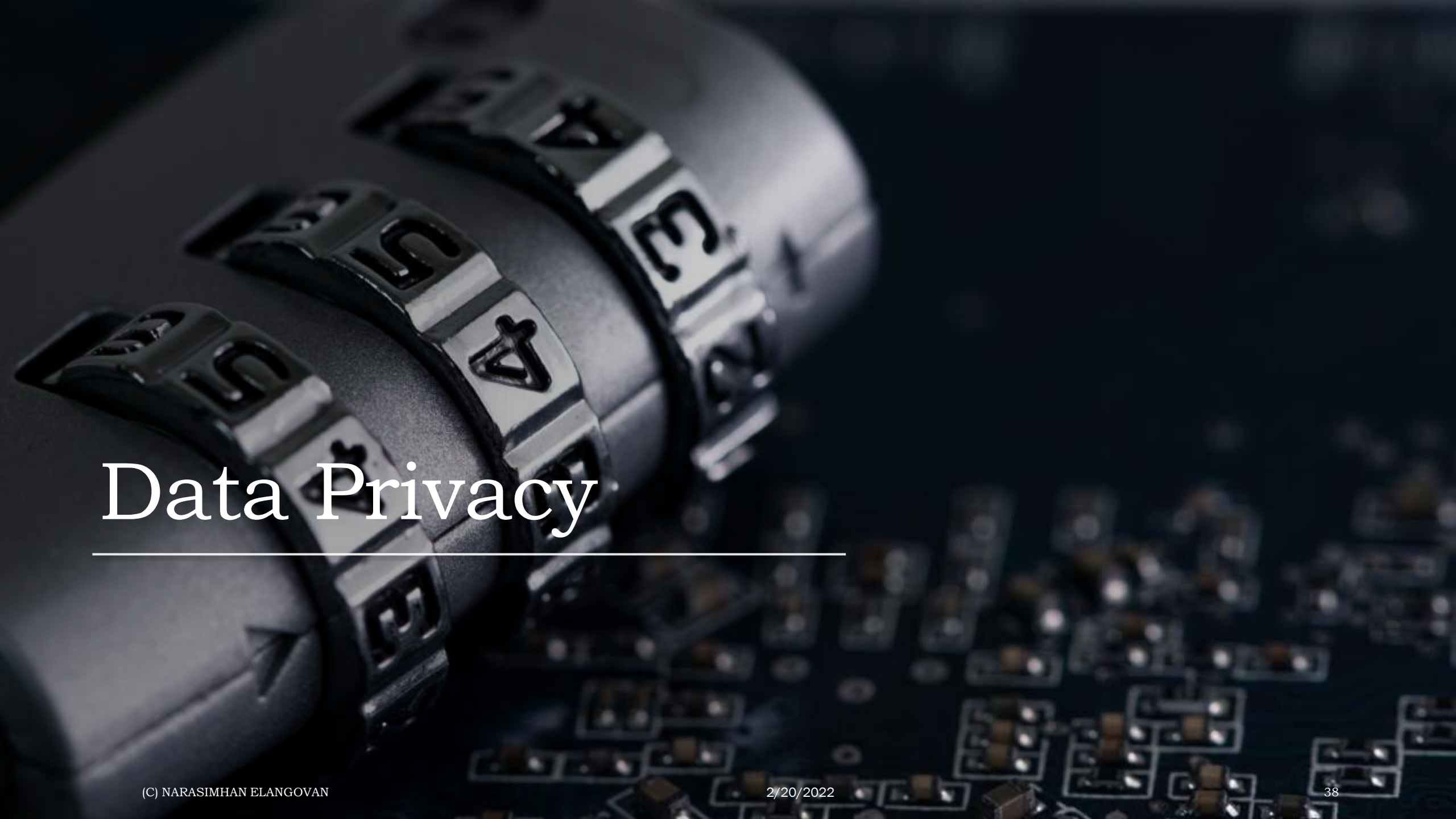


Third-party Digital Risk Assessment (TPDRA) Scope

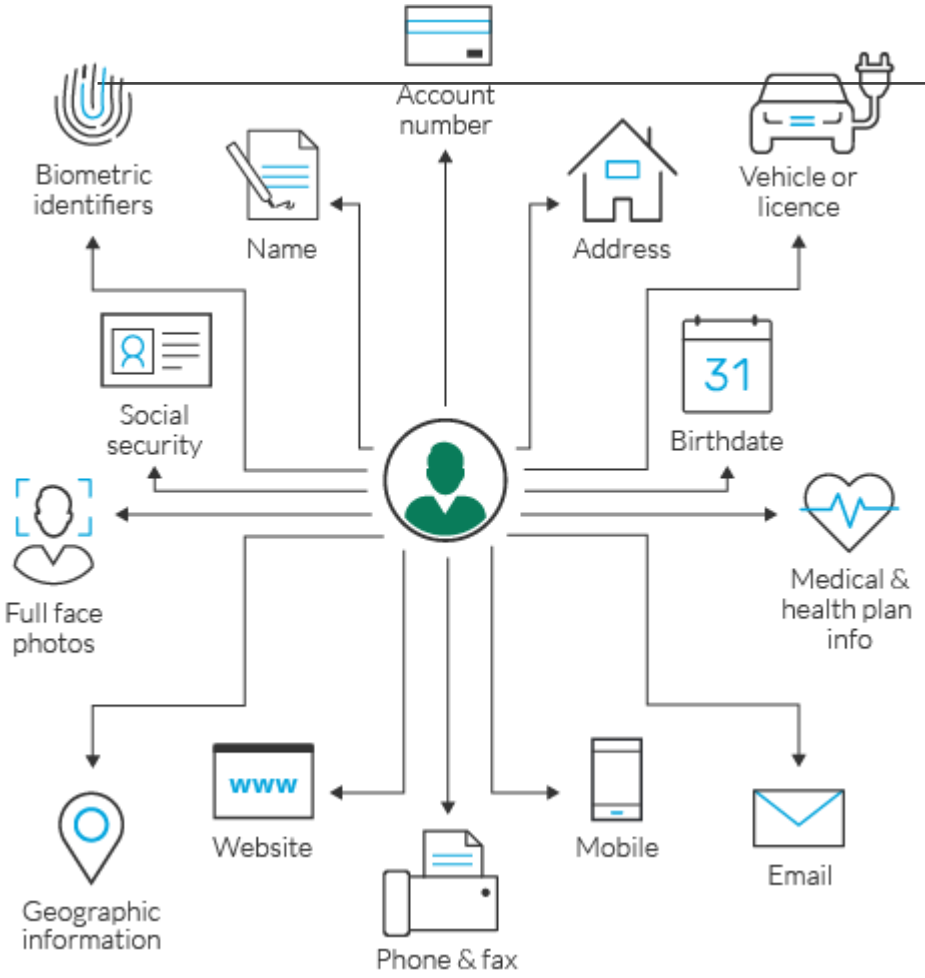
- Information Security Program & Organizational Security
- Human resources security
- Asset Management
- Access control management
- Cryptography
- Physical and Environmental security
- Operations security
- Threat and Vulnerability Management
- Logging and Monitoring
- Communications security
- System acquisition, development, and maintenance
- Subcontractor Management
- Information security Incident management
- Business continuity management
- Compliance
- Cyber security

Typical Questionnaire

	I. Information Systems Acquisition Development and Maintenance		0% of Section Completed
I.1	Does your company perform any type of application development?		
I.2	Do you perform any type of application testing?		
I.3	Does the company have an internal organization that provides project management oversight?		
I.4	Does the company have an independent quality assurance function responsible for the testing of software and infrastructure prior to implementation?		
I.5	Does your organization support or maintain a development, test, staging, QA or production environment?		
I.6	Do you have a documented change control process?		
I.7	Does your organization patch systems and applications?		
I.8	Are systems and networks periodically assessed for vulnerabilities?		
I.9	Do you support, host, maintain, etc. a web site with access to target data?		
I.10	Do you use or have installed on any system penetration, threat or vulnerability assessment tools?		
	J. Information Security Incident Management		**0% of Section Completed**
J.1	Does your company have an Incident Management policy?		
J.2	Does your company have a formal information security Incident Response Program / Plan?		
J.3	Does your company have a security incident response team with clearly defined and documented roles and responsibilities?		
J.4	Is an Incident Response contact list or calling tree maintained?		
J.5	Is documentation maintained on previous incidents, outcomes and issues and their remediation?		
	K. Business Continuity Management		**0% of Section Completed**
K.1	Does your company have a written policy for business continuity and disaster recovery.		
	L. Compliance		**0% of Section Completed**
L.1	Is your organization required to comply with any legal, regulatory or industry, requirements, etc. (GLBA, SOX, PCI)?		
L.2	Is your organization required to comply with any SEC regulations?		
L.3	Within the last year, has there been an independent review of the company's security policies, standards, procedures, and/or guidelines?		
L.4	Has a network penetration test been conducted within the last year?		



Data Privacy



COMMON TYPES OF PII

Examples of PII Data

- Name
- Email address
- Social Media Posts
- Physical, physiological, or genetic information
- Medical information
- Location
- Bank details
- IP address
- Cookies
- Cultural identity

Where can it be found?

- Emails
- Documents
- Databases
- Removable media
- Metadata
- Log files
- Backups

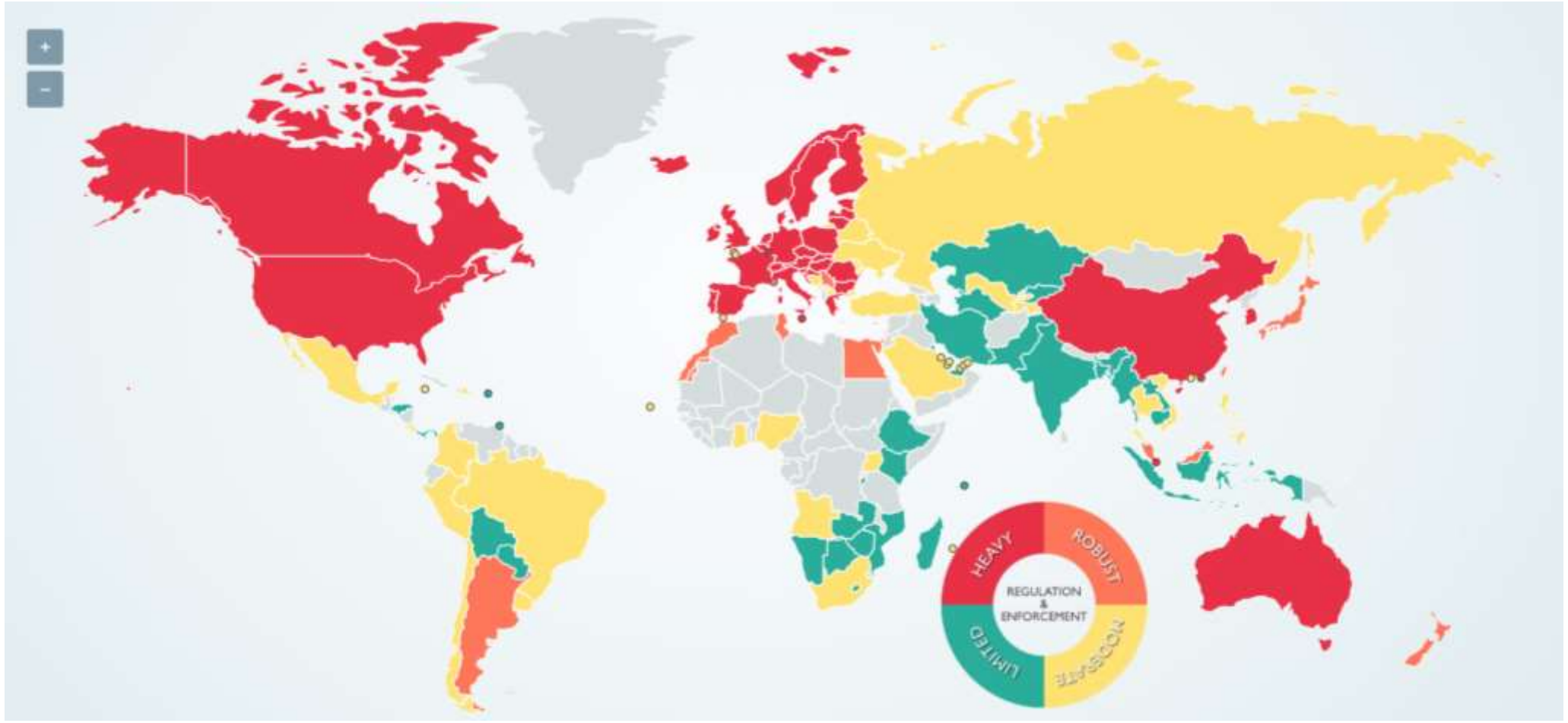
Direct Data Monetization

- Bartering/trading with information
- Enhancing products or services with information
- Selling raw data through brokers (DaaS)
- Offering insights, analyses and reports (e.g., subscriptions)

Indirect Data Monetization

- Improving process performance or effectiveness
- Developing new products or markets
- Building and solidifying partner relationships
- Publishing branded indexes

Data Regulations across the Globe



Source: DLA Piper

Map not to Scale

Data Privacy - Generally Accepted Privacy Principles

Management

- Organization handling private information should have appropriate policies, procedures, and governance structures in place to protect the privacy of the information

Notice

- The organization provides notice to the Data subjects about its privacy policies and procedures and also indicates the purposes for which information is being collected and used.

Choice and Consent

- The entity should inform data subjects of their option regarding the data they own and get consent (implicit or explicit) from those individuals for the collection, storage, use, and sharing of that information.

Collection

- The collection of personal information purposes should disclose in their privacy notices by the organization.

Usage, Retention, and Disposal

- The organization should retain personal information as long as it is required after that data should be disposed of securely

Data Privacy - Generally Accepted Privacy Principles

Access

- Organizations should provide individual access to their information with the ability to review and update whenever need.

Disclosure to Third Parties

- The information is only shared with third parties by the organization if that sharing is consistent with purposes disclosed in privacy notices and they have the implicit or explicit consent of the individual to share that information.

Security

- It's the organization's responsibility to secure private information against unauthorized access, either physically or logically.

Quality

- The organization should take appropriate steps to guarantee that the private information they maintain is accurate, complete, and relevant.

Monitoring and Enforcement

- The organization should have a program in place to monitor compliance with its privacy policies and provide procedures to address dispute pertaining the same.

VAPT

VAPT

- Vulnerability Assessment (VA)?
  - A Vulnerability Assessment is a rapid automated review of network devices, servers and systems to identify key vulnerabilities and configuration issues that an attacker may be able to take advantage off. Its generally conducted within the network on internal devices and due to its low footprint can be carried out as often as every day.

- What is Penetration Testing (PT or PenTest)?
  - A Penetration Test is an in-depth expert-driven activity focused on identifying various possible routes an attacker could use to break into the network. In-addition with the vulnerabilities it also identifies the potential damage and further internal compromise an attacker could carry out once they are past the perimeter.

VAPT – Typical Scope

- Network Scanning
- Port Scanning
- System Identification & Trusted System Scanning
- Vulnerability Scanning
- Malware Scanning
- Spoofing
- Scenario Analysis
- Application Security Testing & Code Review
- OS Fingerprinting
- Service Fingerprinting
- Access Control Mapping
- Denial Of Service (DOS) Attacks
- DDOS Attacks
- Authorization Testing
- Lockout Testing
- Password Cracking
- Cookie Security
- Functional validations
- Containment Measure Testing
- War Dialing
- DMZ Network Architecture Review
- Firewall Rule Base Review
- Server Assessment (OS Security Configuration)
- Security Device Assessment
- Network Device Assessment
- Database Assessment
- Website Assessment (Process)
- Vulnerability Research & Verification
- IDS/IPS review & Fine tuning of Signatures
- Man in the Middle attack
- Man in the browser attack
- Any other attacks

ISO 27001

ISO 27001

- ISO/IEC 27001 is an international standard on how to manage information security.
- It details requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS)
- The aim is to help organizations make the information assets they hold more secure.
- With the proportion of organizations that have embraced the Information Technology revolution becoming a clear majority, it is clear that auditors can expect great opportunities in this regard

Types of audits

- The standard requires that an organisation is required to plan and conduct a schedule of “internal audits” to be able to claim compliance with the standard.
- Furthermore, if an organisation desires to achieve certification, it will require “external audits” to be carried out by a “Certification Body” – an organisation with competent auditing resources against ISO 27001.

ISO 27001 internal audit

- **Documentation review** – This is a review of the organisation's policies, procedures, standards, and guidance documentation to ensure that it is fit for purpose and is reviewed and maintained.
- **Evidential audit (or field review)** – This is an audit activity that actively samples evidence to show that policies are being complied with, that procedures and standards are being followed, and that guidance is being considered.
- **Analysis** – Following on from documentation review and/or evidential sampling, the auditor will assess and analyse the findings to confirm if the standard requirements are being met.
- **Audit report** – An audit report will need to be prepared as required by the standard in Clause 9.2 f) and provided to management to ensure visibility.
- **Management review** – is a required activity under Clause 9.3 Management review, which must consider the findings of the audits carried out to ensure that corrective actions and improvements are implemented as necessary.

External ISO 27001 audit

- The processes for external audit are essentially the same as for the internal audit programme but usually carried out to achieve and maintain certification.
- The programme of external [certification] audits will be determined by the external auditors [certification body] but will follow a systematic requirement (see below).
- The relevant auditor will provide a plan of the audit, and once the organisation confirms this, resources will be allocated and dates, times and locations agreed.

Virtual CISO

Virtual CISO

- an outsourced security advisor whose responsibilities varies depending upon your business needs.
- Scope of work
  - Provide leadership on risk, governance, Incident Response, Disaster Recovery & Business Continuity
  - Provide Expert assessment on security threats, risks compliance
  - Provide consultation to build effective cybersecurity & resiliency program
  - Facilitate the integration of security into your business strategy, process & culture
  - Manage the development, roll-out, and ongoing maintenance of cybersecurity programs
  - Assist with integration and interpretation of information security program controls
  - Serve as an Industry expert (HIPAA, PCI-DSS, NIST, ISO 27001, various standards, and compliances)
  - Serve as security liaison to auditors, assessors, and examiners

Forensic Audits and Analysts

Forensic Audits and Analysts

- Financial Forensics
  - Accounting investigation
  - Fund Flow investigation
  - Economic crimes
  - Tax violations
  - Fraud Analytics
  - Insurance Claims
- Digital Forensics
  - Cyber crime investigation
  - Forensic Analysts
  - Analyse digital footprints and compromised Systems

Certifications

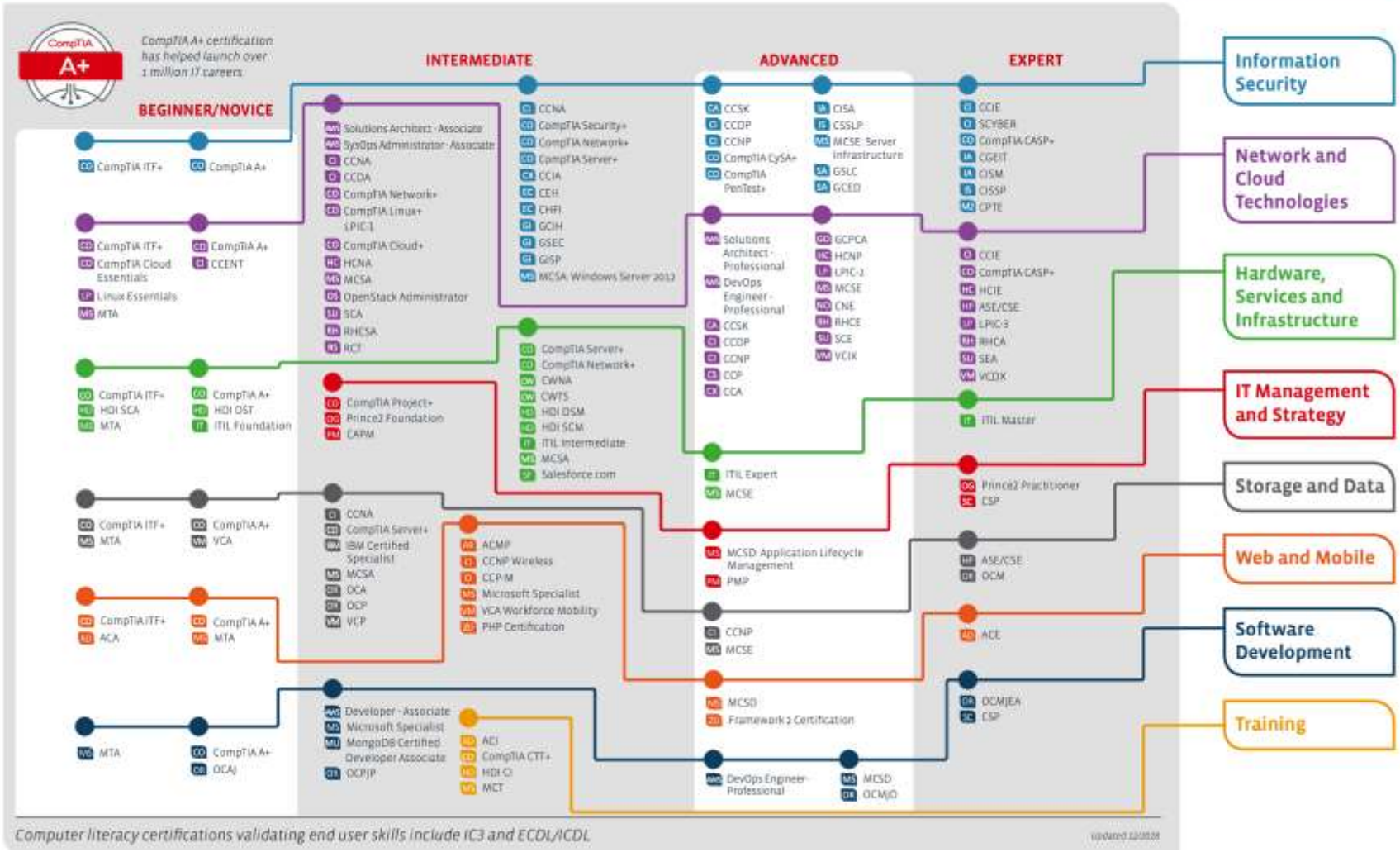

Cybersecurity Domains
Security Engineering
Federated Identity
Cloud Security
Data Protection
Network Design
Secure Application Development
System Integration
Access Control
Cryptography
Identity Management
Security Architecture
Privileged Access Management
Identity & Access Management
Physical Security
Framework and Standard
NIST
ISO/IEC
SANS/CSC
Career Development
Certification
Training
Conferences
Peer Groups
Self Study
Risk Assessment
Vulnerability scan
4th Party Risk
3rd Party Risk
Penetration test
Blueteam
Redteam
Social Engineering
Application
Infrastructure
Source Code Scan
Data-Centric Risk Assessment
Data-Flow Map
Blackbox
Whitebox
Security Operation
DR
Recovery
BCP
Detection
Protection
Prevention
SIEM
SOC
Vulnerability Management
Active Defense
Data Leakage
Incident Response
Breach Notification
Containment
Investigation
Eradication
Forensics
Threat Intelligence
External
Internal
Contextual
IOCs
Intel. Sharing
User Education
Training (new skills)
Awareness (reinforcement)
Governance
Industry Specific
Federal
Laws and Regulations
State
Audit
Executive Management Involvement
Company's Written Supervisory Procedures (WSPs)
Compliance & Enforcement
Policy
Procedure
Guideline
Standard

IT Certification Roadmap

Explore the possibilities with the CompTIA Interactive IT Roadmap at: CompTIA.org/CertsRoadmap

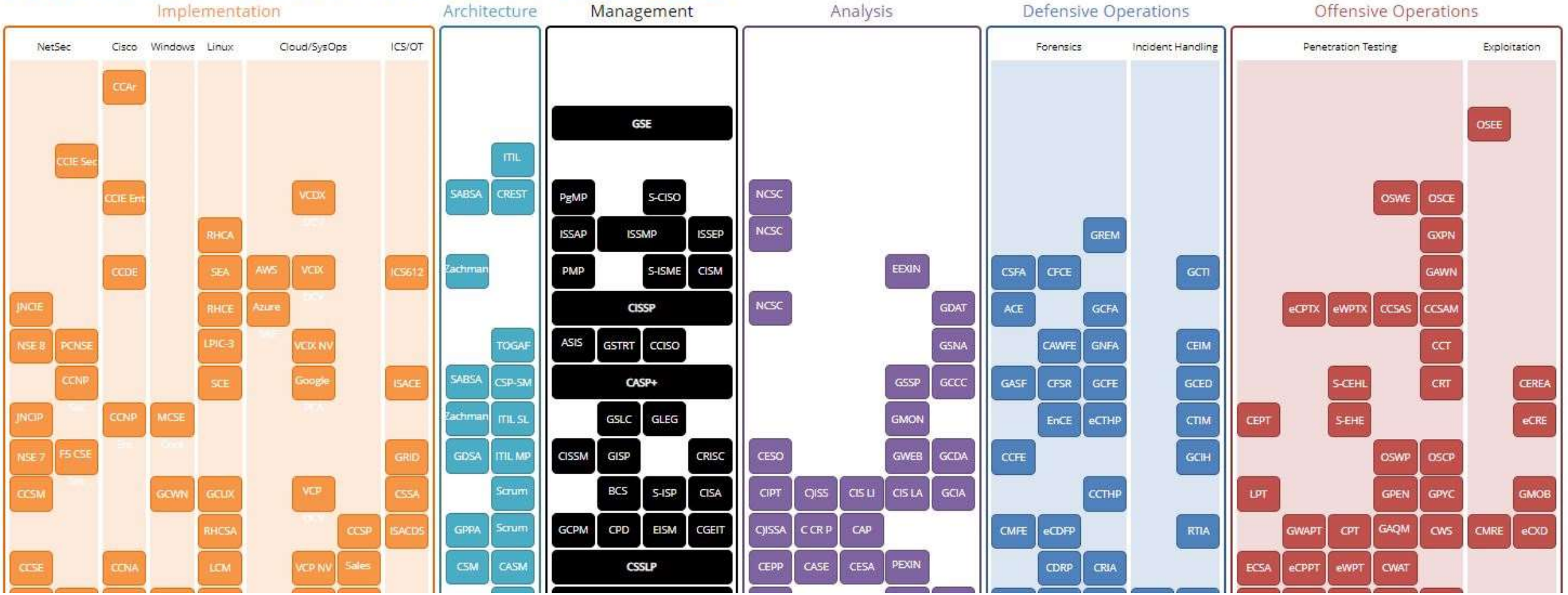
CompTIA

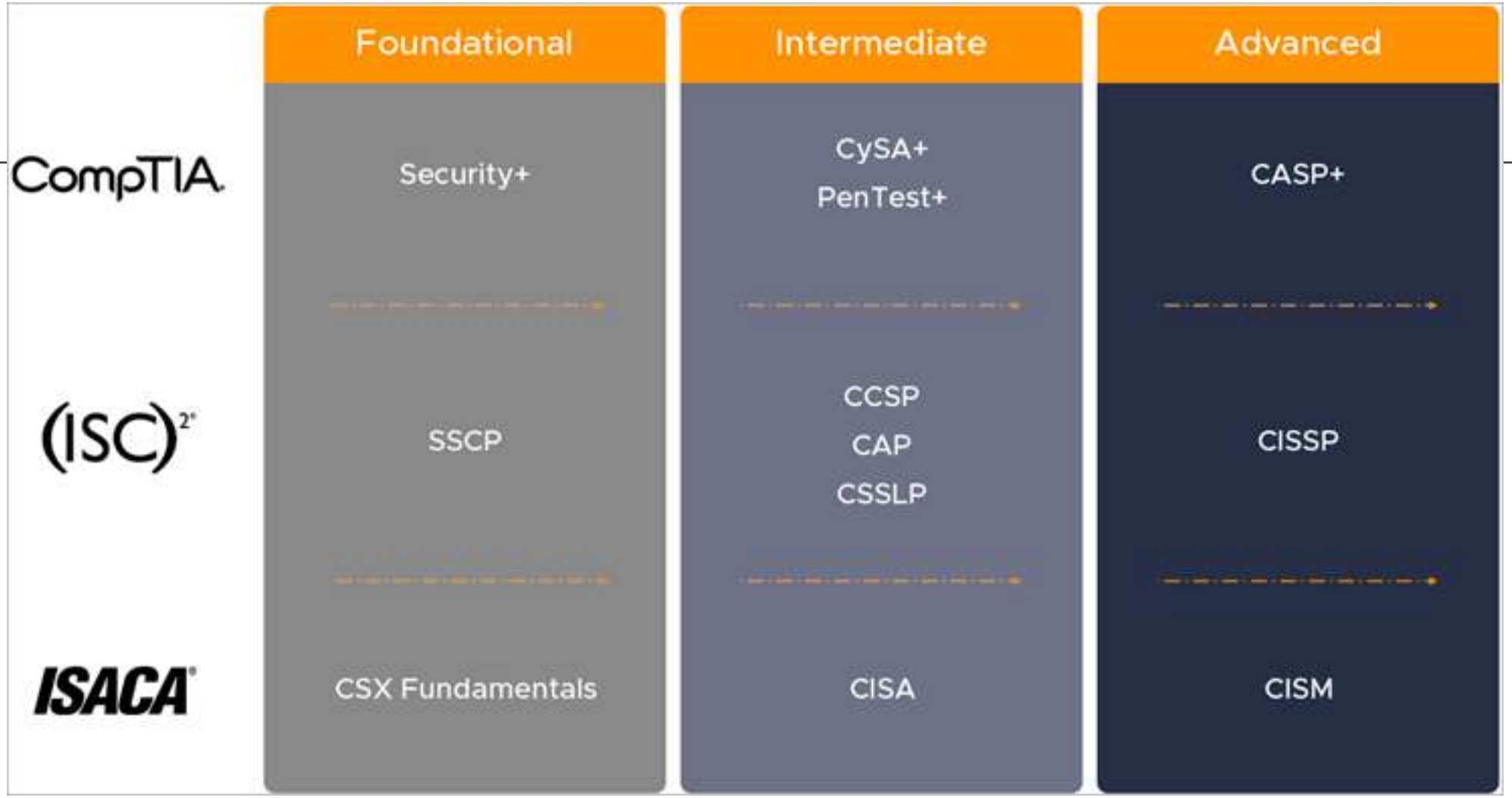
Certifications validate expertise in your chosen career.



Computer literacy certifications validating end user skills include IC3 and ECDL/ICDL

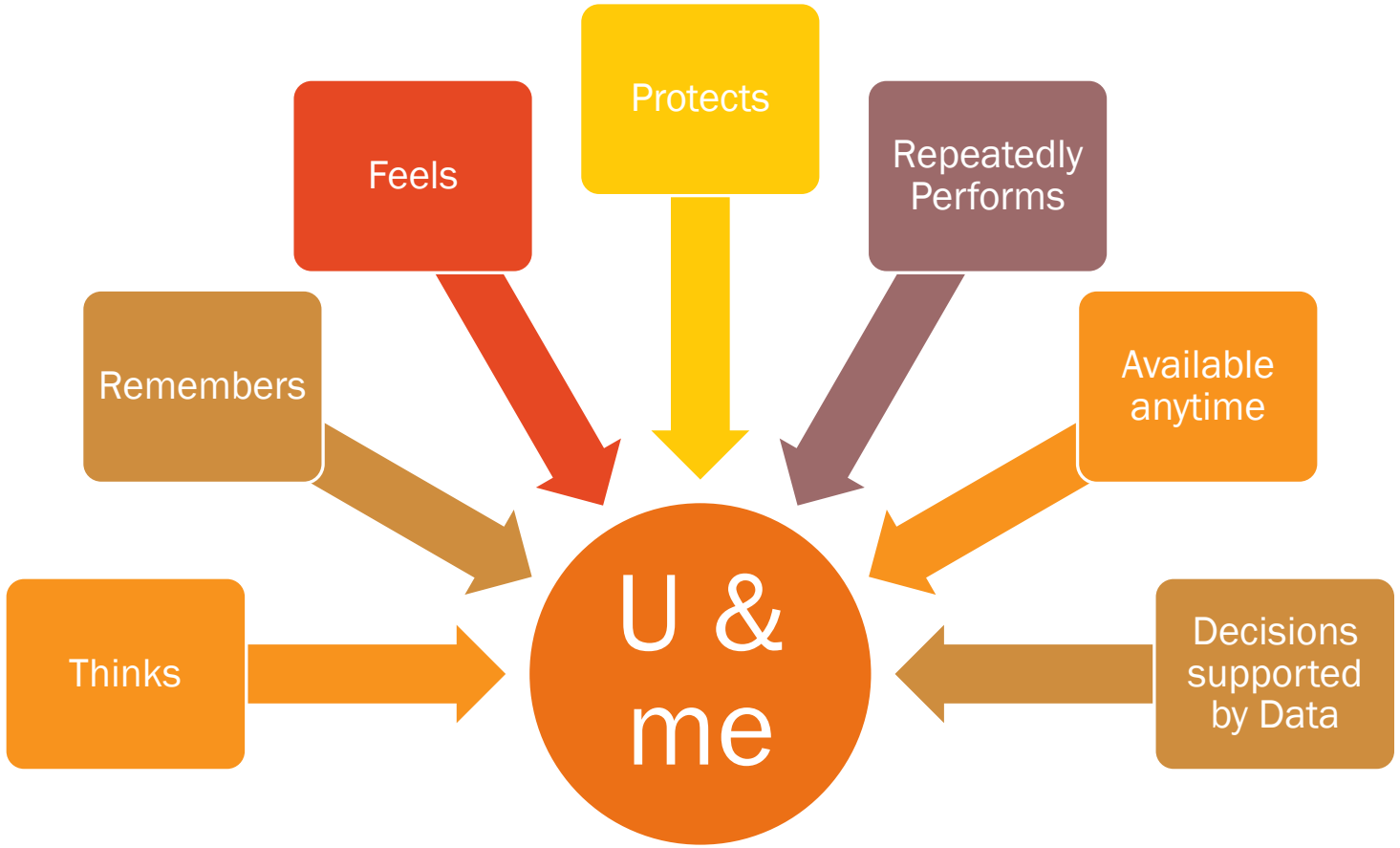
Security Certification Progression Chart 2020



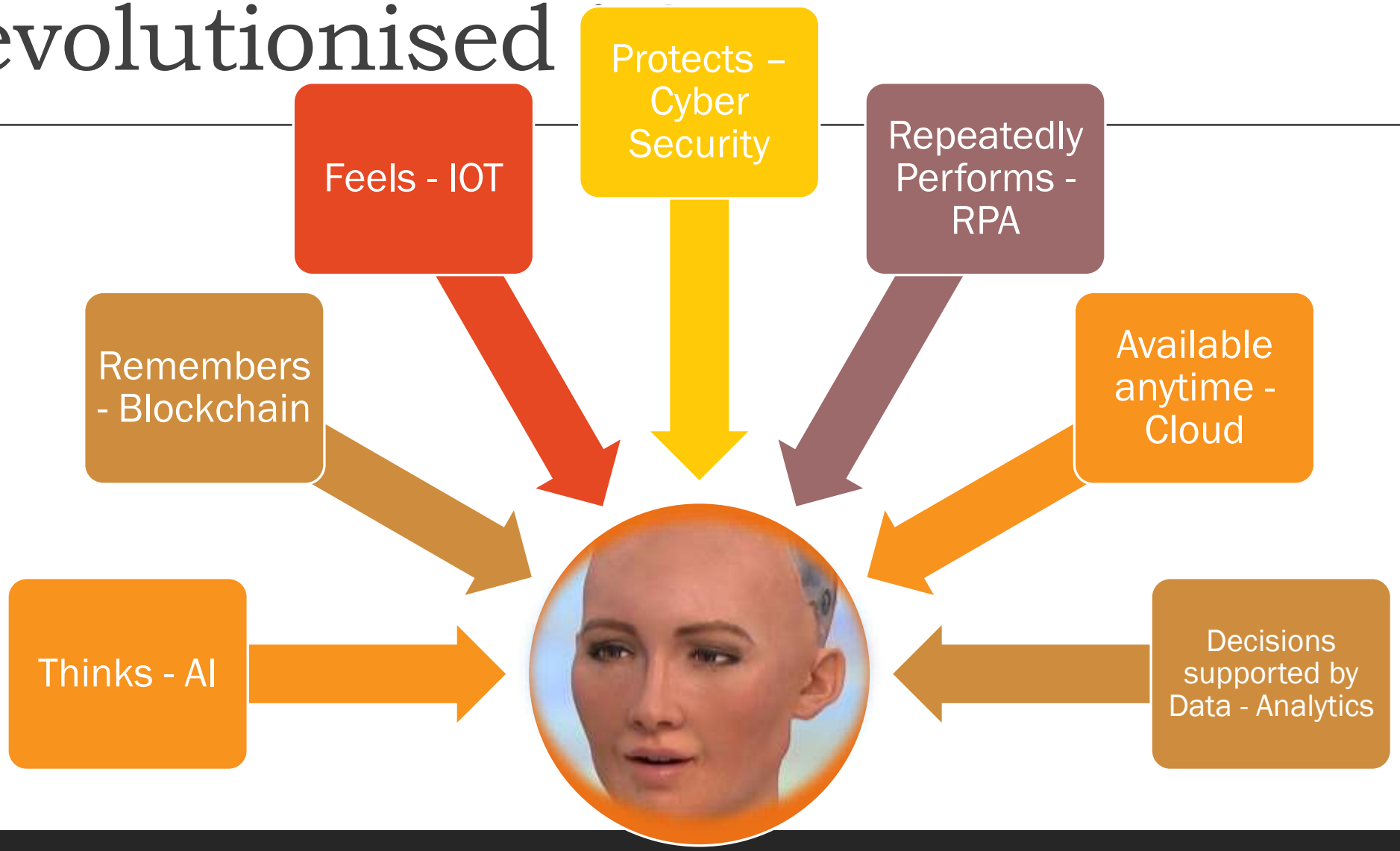

Foundational
Intermediate
Advanced
CompTIA
Security+
CySA+
PenTest+
CASP+
(ISC)²
SSCP
CCSP
CAP
CSSLP
CISSP
ISACA
CSX Fundamentals
CISA
CISM

Emerging Technologies

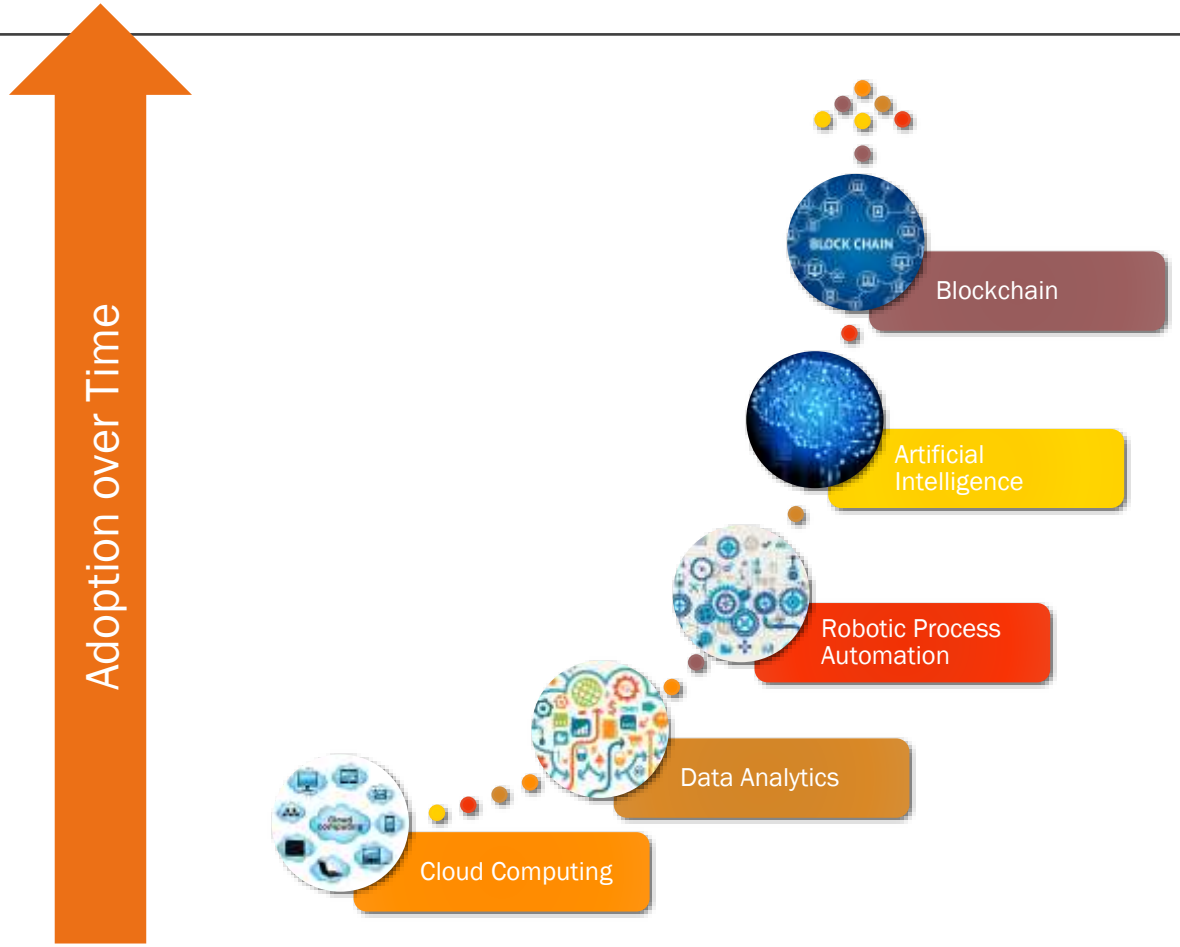
What can a human do?



How has Industry 4.0 revolutionised



Penetration Of Tech In Our Profession




" The World's Biggest
Problems are the World's
Biggest Opportunities."

About Us

KEN & Co.
Chartered Accountants

A Boutique Governance Risk, and Technology Consulting Firm

Digitization | Analytics | Risk | GRC | SOX | ISO | SOC | Forensic Audit | Privacy Law

LinkedIn | YouTube | Telegram

https://www.ken-co.in/

KEN & Co. is a Bangalore based professional firm with a right combination of zeal and experience in emerging areas such as Information technology advisory, process audit, systems implementation, gap assessment in existing systems & processes, in addition to tradition areas of tax, assurance, consulting and business advisory.

Considering the growing business challenges in day to day world and new complexities cropping every now and then, we adopt a multi-dimensional approach and help you better your business processes and services. As business grows beyond frontiers, we believe in adding value to every activity we perform!

Our area of operations ranges from traditional areas like tax and assurance to the new transpiring areas like Process Audit, Information Technology Audit, catering to the needs of e-commerce and start-ups.

Disclaimer

This publication contains information in summary form and is therefore intended for general guidance only. All information is provided in good faith. KEN & Co., makes no representation or warranty of any kind, express or implied, regarding the accuracy, adequacy, validity, reliability, availability or completeness of any information provided. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Detailed notification and regulations by the respective Departments is awaited.

Tech-enabled Solutions

IT Governances & Compliance

IT Assurance Services

Data Analytics & Business Intelligence

GDPR & Privacy Audits

Emerging Technology (AI, Blockchain, IoT)

Enterprise Risk Management

Forensic Audit

IT Automation & Implementation

Cyber Security

IT Consulting

ISO, PCI DSS, CMMI Compliance

SOC Assessments

IT Training

https://www.capsfoundation.in/

Thank You!

Questions?

Narasimhan Elangovan

Partner at KEN & Co. Chartered Accountants

Narasimhan Elangovan

narasimhan@ken-co.in

www.ken-co.in