Legal, ethical and Intellectual property rights in Healthcare technology and Cybersecurity in hospitals

To make cybersecurity measures explicit, the written norms are required. These norms are known as cybersecurity standards: the generic sets of prescriptions for an ideal execution of certain measures. The standards may involve methods, guidelines, reference frameworks, etc. It ensures efficiency of security, facilitates integration and interoperability, enables meaningful comparison of measures, reduces complexity, and provide the structure for new developments.

A security standard is "a published specification that establishes a common language, and contains a technical specification or other precise criteria and is designed to be used consistently, as a rule, a guideline, or a definition." The goal of security standards is to improve the security of information technology (IT) systems, networks, and critical infrastructures. The Well-Written cybersecurity standards enable consistency among product developers and serve as a reliable standard for purchasing security products.

Standards can be contrasted with another category of documents, generally referred to as guidelines. Both standards and guidelines provide guidance aimed at enhancing cyber security, but guidelines usually lack the level of consensus and formality associated with standards. Some standards, such as American National Standards Institute (ANSI) Standards and Federal Information Processing Standard (FIPS) Publications, are easily recognized because they include the term standard in their titles. Others are harder to recognize. For example, standards issued by the International Telecommunications Union (ITU), an international standards developer, are designated as Recommendations.

A standard issued by the IETF starts out as an RFC and retains that designation even after being adopted as a standard. In other cases, documents that are not standards in the strict sense of the word may be treated as such by an organization if it suits the organization’s needs. For example, many US and international organizations and businesses have adopted National Institute of Standards and Technology (NIST) Special Publications as standards, even though those documents are published as guidelines for use by US Federal agencies. Some organizations develop both standards and guidelines. For example, in addition to international standards, ISO/IEC issues several types of guidelines, including technical specifications, publicly available specifications (PAS), and technical reports, according to the ISO/IEC Directives, Part 1, Section 3.

A technical specification may be published when the immediate release of an international standard is not feasible, such as when the subject in question is still under development. A PAS may be an intermediate specification published prior to the development of a full international standard, or in International Electro technical Commission (IEC) it may be a “dual logo” publication published in collaboration with an external organization. A PAS does not fulfill the requirements for a standard. A technical report is an informative document generally intended to educate the reader, not to specify an international standard.

Security standards are generally provided for all organizations regardless of their size or the industry and sector in which they operate. This section includes information about each standard that is usually recognized as an essential component of any cybersecurity strategy.

International Organization for Standardization (ISO):

ISO stands for International Organization for Standardization. These standards provide a world-class specification for products, services and computers, to ensure quality, safety and efficiency. They are instrumental in facilitating international trade.

ISO standard is officially established on 23 February 1947. It is an independent, non-governmental international organization. Today, it has a membership of 162 national standards bodies and 784 technical committees and subcommittees to take care of standards development. ISO has published over 22336 International Standards and its related documents which covers almost every industry, from information technology, to food safety, to agriculture and healthcare.

The International Organization for Standardization (ISO) defines a standard as "a document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines, or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context" [1]. Numerous standards have been developed for cyber security to help organizations better manage security risk, implement security controls that meet legal and regulatory requirements, and achieve performance and cost benefits. This article provides an overview of cyber security standards in general and highlights some of the major ongoing international, regional, national, industry, and government standards efforts. It also discusses the advantages of having standards and explains how organizations can participate in standards research and development.

ISO 27000 Series:

It is the family of information security standards which is developed by the International Organization for Standardization and the International Electro technical Commission to provide a globally recognized framework for best information security management. It helps the organization to keep their information assets secure such as employee details, financial information, and intellectual property.

The need of ISO 27000 series arises because of the risk of cyber-attacks which the organization face. The cyber-attacks are growing day by day making hackers a constant threat to any industry that uses technology.

The ISO 27000 series can be categorized into many types. They are-

- ISO 27001
- ISO 27000
- ISO 27002
- ISO 27005
- ISO 27032

IT Act

The Information Technology Act also known as ITA-2000, or the IT Act main aims is to provide the legal infrastructure in India which deal with cybercrime and e-commerce. The IT Act is based on the United Nations Model Law on E-Commerce 1996 recommended by the General Assembly of United Nations. This act is also used to check misuse of cyber network and computer in India. It was officially passed in 2000 and amended in 2008. It has been designed to give the boost to Electronic commerce, e-transactions and related activities associated with commerce and trade. It also facilitate electronic governance by means of reliable electronic records.

IT Act 2000 has 13 chapters, 94 sections and 4 schedules. The first 14 sections concerning digital signatures and other sections deal with the certifying authorities who are licenced to issue digital signature certificates, sections 43 to 47 provides penalties and compensation, section 48 to 64 deal with appeal to high court, sections 65 to 79 deal with offences, and the remaining section 80 to 94 deal with miscellaneous of the act.

Copyright Act

The Copyright Act 1957 amended by the Copyright Amendment Act 2012 governs the subject of copyright law in India. This Act is applicable from 21 January 1958. Copyright is a legal term which describes the ownership of control of the rights to the authors of "original works of authorship" that are fixed in a tangible form of expression. An original work of authorship is a distribution of certain works of creative expression including books, video, movies, music, and computer programs. The copyright law has been enacted to balance the use and reuse of creative works against the desire of the creators of art, literature, music and monetize their work by controlling who can make and sell copies of the work.

The copyright act covers the following-

- Rights of copyright owners
- Works eligible for protection
- Duration of copyright
- Who can claim copyright

The copyright act does not covers the following-

- Ideas, procedures, methods, processes, concepts, systems, principles, or discoveries
- Works that are not fixed in a tangible form (such as a choreographic work that has not been notated or recorded or an improvisational speech that has not been written down)
- Familiar symbols or designs
- Titles, names, short phrases, and slogans
- Mere variations of typographic ornamentation, lettering, or coloring

Patent Law

Patent law is a law that deals with new inventions. Traditional patent law protect tangible scientific inventions, such as circuit boards, heating coils, car engines, or zippers. As time increases patent law have been used to protect a broader variety of inventions such as business practices, coding algorithms, or genetically modified organisms. It is the right to exclude others from making, using, selling, importing, inducing others to infringe, and offering a product specially adapted for practice of the patent.

In general, a patent is a right that can be granted if an invention is:

- Not a natural object or process
- New
- Useful
- Not obvious.

Intellectual property rights (IPR)

Intellectual property rights is a right that allow creators, or owners of patents, trademarks or copyrighted works to benefit from their own plans, ideas, or other intangible assets or investment in a creation. These IPR rights are outlined in the Article 27 of the Universal Declaration of Human Rights. It provides for the right to benefit from the protection of moral and material interests resulting from authorship of scientific, literary or artistic productions. These property rights allow the holder to exercise a monopoly on the use of the item for a specified period.

DISHA: The first step towards securing patient health data in India

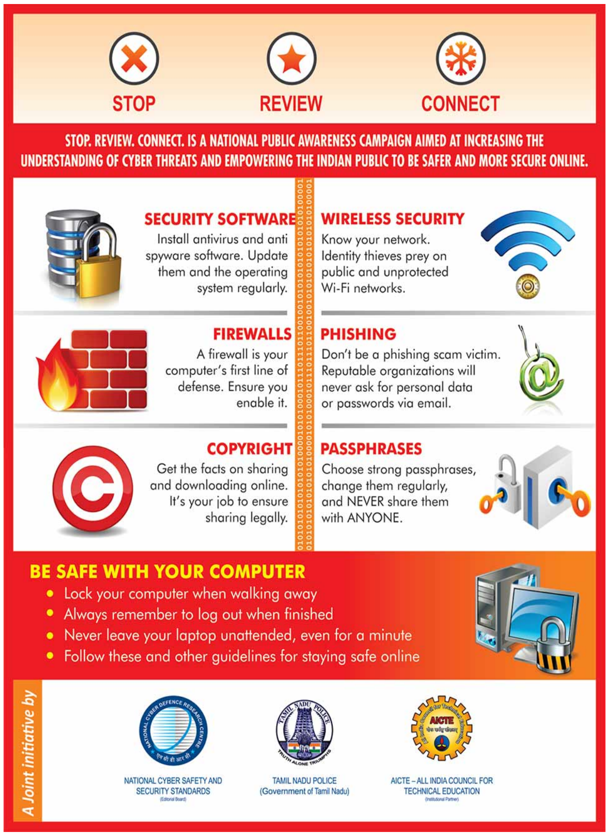
The Digital Information Security in Healthcare Act ('DISHA') is that firm first step taken by the Indian Government in the long journey to securing the healthcare data of patients in India. In a country with more than one billion people, data is bound to be scattered, even more so when it comes to healthcare data. It is common practice for a doctor to have to write up a repeat diagnostic test because they have no way of accessing the patient's medical records. This is despite the fact that the law requires doctors to maintain the medical records of their in-patients for at least three years. In a move to drastically improve healthcare delivery in India and protect patient data, DISHA proposes to change all of that.

DISHA has three primary objectives - setting up a central and state level digital health authority, enforcing privacy and security measures for digital health data, and regulating the storage and exchange of electronic health data. The collection, receipt, storage, handling and transfer of sensitive personal data or information ('SPDI') in electronic form is subject to the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011 (the 'Data Protection Rules'), a set of rules prescribed under the Information Technology Act 2000 - India's principal legislation governing information technology. The Data Protection Rules consider a select set of information to be SPDI. From a healthcare perspective, this includes information relating to physical, physiological and mental health conditions, sexual orientation as well as medical records and history.

The Data Protection Rules apply to any corporate entity that in some way deals with the SPDI of a person. The compliance requirements under the Data Protection Rules were largely limited to obtaining consent prior to collection or transfer, publishing a privacy policy, and maintaining 'reasonable' security practices and procedures to protect SPDI. While there is a requirement for entities to meet ISO standards for data protection, it is also possible for them to have a user agree that their existing data protection practices, irrespective of whether they match ISO standards or not, are reasonable. This workaround would, in effect, satisfy the compliance requirements under the Data Protection Rules.

DISHA aims to be a piece of legislation focused on healthcare data privacy, confidentiality, security and standardization. DISHA will create regulatory authorities, both at the central and state level, to enforce the rights and duties envisaged under the legislation. At the central level, the setting up of a National Electronic Health Authority ('NeHA') is proposed, which would be the apex authority entrusted with formulating standards and operational guidelines and protocols for the generation, collection, storage, and transfer of digital health data. At the state level, the State Electronic Health Authority ('SeHA') will be responsible for ensuring that the requirements of DISHA are followed on the ground, at the institutional level.

Cyber Security Awareness Posters:



STOP REVIEW CONNECT

STOP. REVIEW. CONNECT. IS A NATIONAL PUBLIC AWARENESS CAMPAIGN AIMED AT INCREASING THE UNDERSTANDING OF CYBER THREATS AND EMPOWERING THE INDIAN PUBLIC TO BE SAFER AND MORE SECURE ONLINE.

SECURITY SOFTWARE
Install antivirus and anti spyware software. Update them and the operating system regularly.

WIRELESS SECURITY
Know your network. Identity thieves prey on public and unprotected Wi-Fi networks.

FIREWALLS
A firewall is your computer's first line of defense. Ensure you enable it.

PHISHING
Don't be a phishing scam victim. Reputable organizations will never ask for personal data or passwords via email.

COPYRIGHT
Get the facts on sharing and downloading online. It's your job to ensure sharing legally.

PASSPHRASES
Choose strong passphrases, change them regularly, and NEVER share them with ANYONE.

BE SAFE WITH YOUR COMPUTER

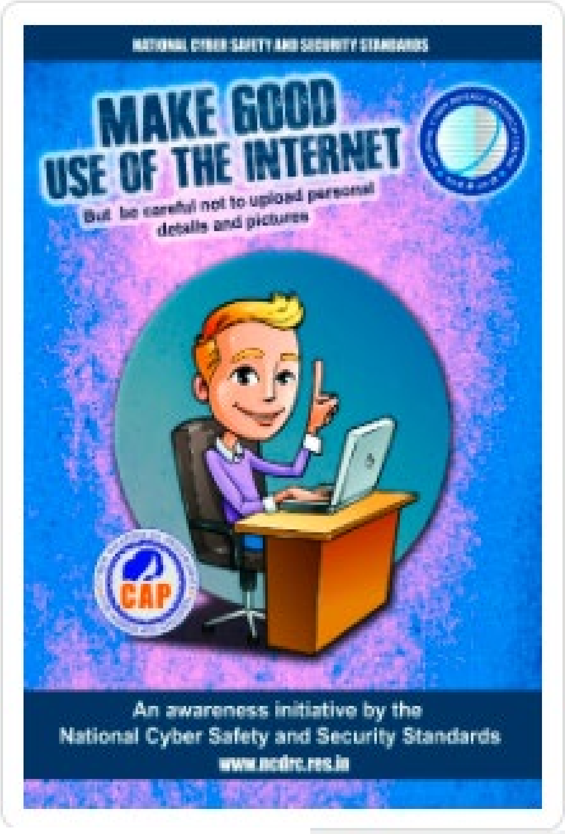
- Lock your computer when walking away
- Always remember to log out when finished
- Never leave your laptop unattended, even for a minute
- Follow these and other guidelines for staying safe online

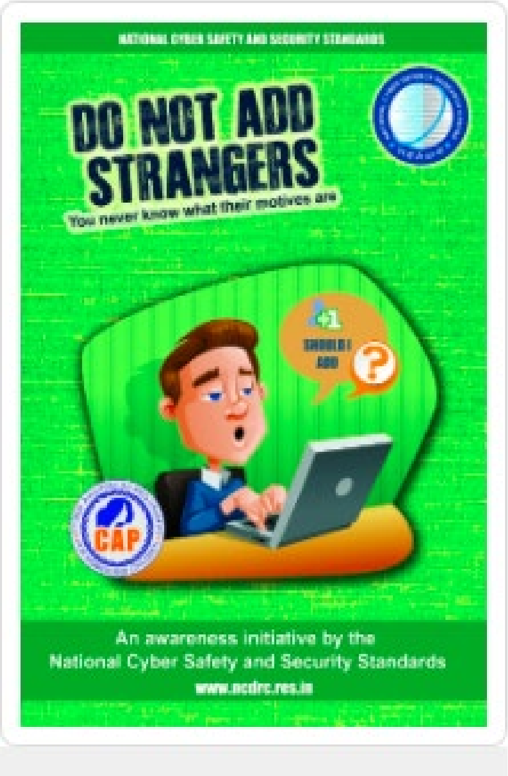
A Joint initiative by

NATIONAL CYBER SAFETY AND SECURITY STANDARDS (Editorial Board)

TAMIL NADU POLICE (Government of Tamil Nadu)

AICTE – ALL INDIA COUNCIL FOR TECHNICAL EDUCATION (Institutional Partner)


NATIONAL CYBER SAFETY AND SECURITY STANDARDS
MAKE GOOD USE OF THE INTERNET
But be careful not to upload personal details and pictures
CAP
An awareness initiative by the National Cyber Safety and Security Standards
www.ncdrc.res.in


NATIONAL CYBER SAFETY AND SECURITY STANDARDS
DO NOT ADD STRANGERS
You never know what their motives are
+1
SHOULD I ADD
?
CAP
An awareness initiative by the National Cyber Safety and Security Standards
www.ncdrc.res.in

References:

1. https://www.cgi.com/sites/default/files/2019-08/cgi-understanding-cybersecurity-standards-white-paper.pdf
2. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=152153
3. https://www.javatpoint.com/cyber-security-standards
4. https://ncdrc.res.in/cyber-security-awareness-posters.php
5. http://www.nishithdesai.com/fileadmin/user_upload/pdfs/NDA%20In%20The%20Media/News%20Articles/180725_A_DISHA-The-First-Step-towards-Securing-Patient-Health-Data-in-India.pdf

PUBLIC HEALTH FOUNDATION OF INDIA

भारतीय विज्ञान संस्थान
Indian Institute of Science

Indian Institute of Space Science and Technology

ASSOCIATION OF HEALTHCARE PROVIDERS INDIA

Certificate Course in **Healthcare Technology (CCHT)**

Legal , ethical and Intellectual property rights in Healthcare technology and Cybersecurity in hospitals

CERTIFICATE COURSE IN HEALTHCARE TECHNOLOGY

Who am I ?

Kumar is a Senior Technology and Security leader with 20+ years of proven expertise in Digital Strategy, Digital Innovation, Systems Design and Development, Planning, Budgeting, Enterprise Architecture, Information Security and Privacy. He brings in a perfect blend of technology and security vision, resulting in consistent development of innovative digital strategies. He has realised these strategies by implementing high performance, scalable and secure digital solutions resulting in improved efficiency, improved compliance, and reduction in cost.

He has completed his Executive Education in General Management from Indian Institute of Management, Bangalore, and Post-Graduation (M.Phil.) in Hospital and Health Systems Management from Birla Institute of Technology and Science, Pilani (BITS). In addition to this, he is a Certified Healthcare CIO, ISO 27001:2013 Lead Information Security auditor, DSCI Certified Data Privacy Lead Assessor and a TOGAF certified practitioner.

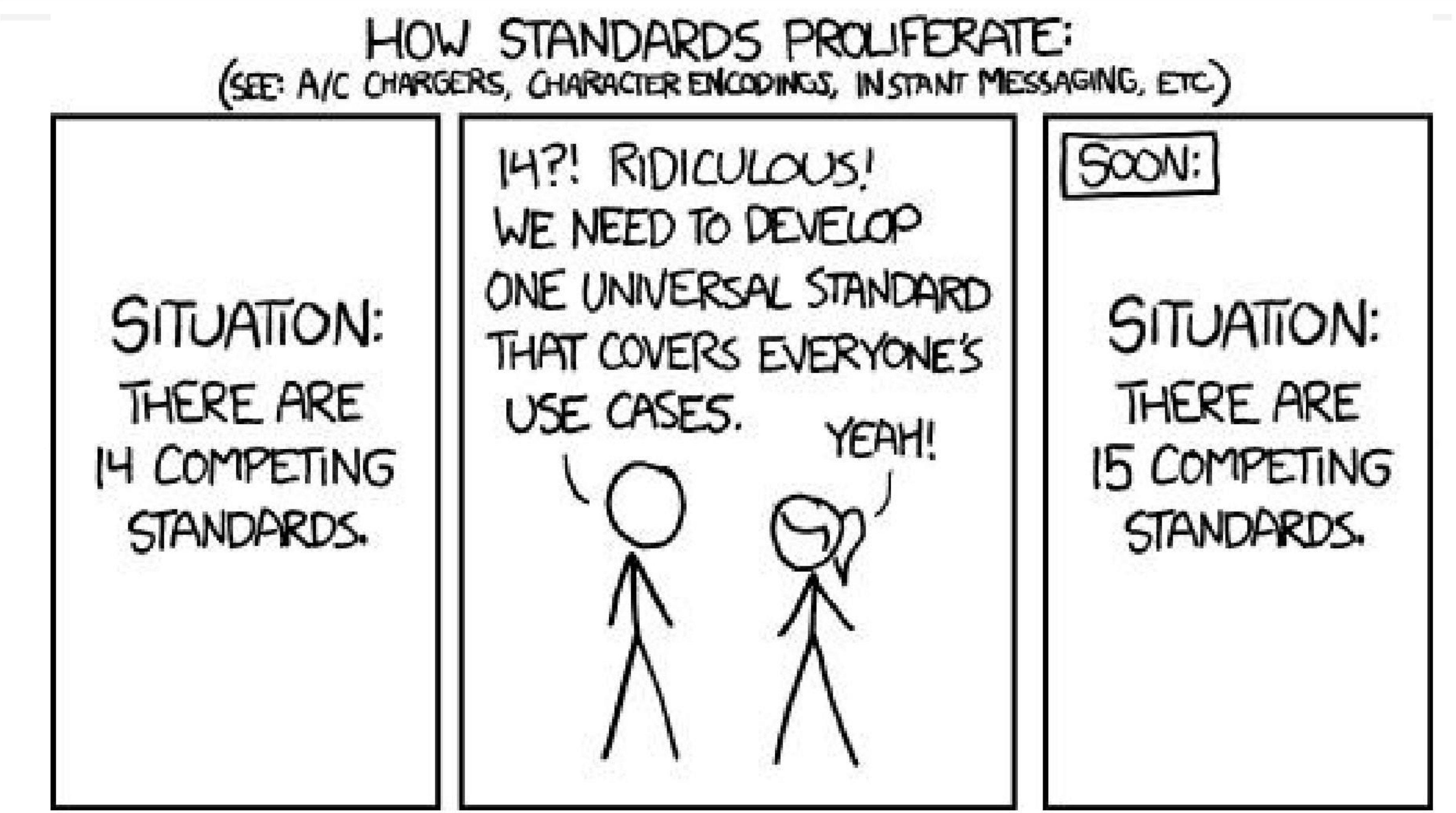
Learning Objectives

- Understand the need for standards
- ISO 27001 Information Security Standards and its Domains
- Data Privacy
- Importance of Data Security and Privacy

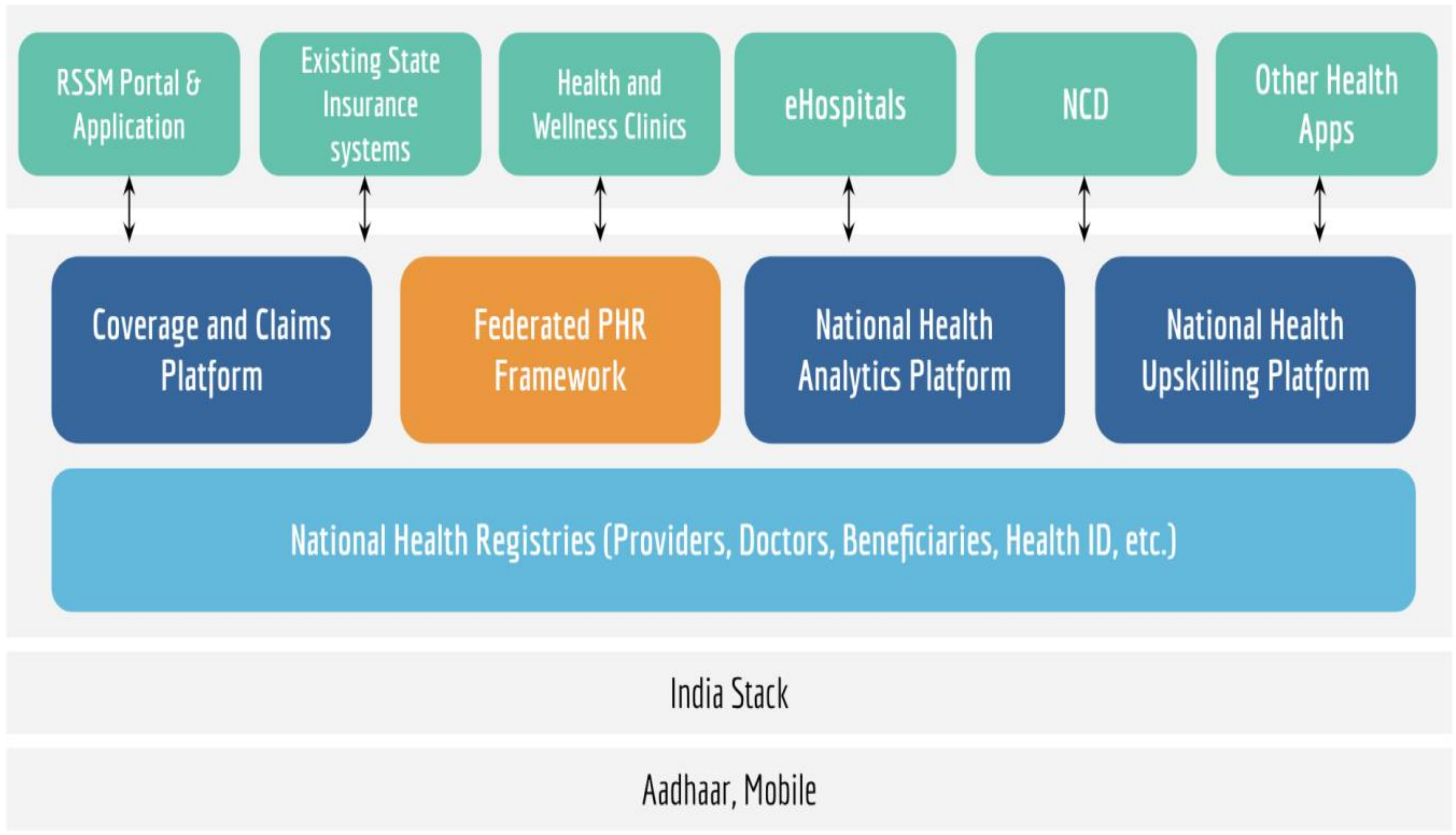
Overview of the Session

- ✓ Overview on Standards
- ✓ Nation Digital Health Blueprint
- ✓ ISO 27001 Detailed Overview
- ✓ Data Privacy Overview
- ✓ Cybersecurity and its Importance

Context


HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC.)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.

National Health Stack



RSSM Portal & Application

Existing State Insurance systems

Health and Wellness Clinics

eHospitals

NCD

Other Health Apps

Coverage and Claims Platform

Federated PHR Framework

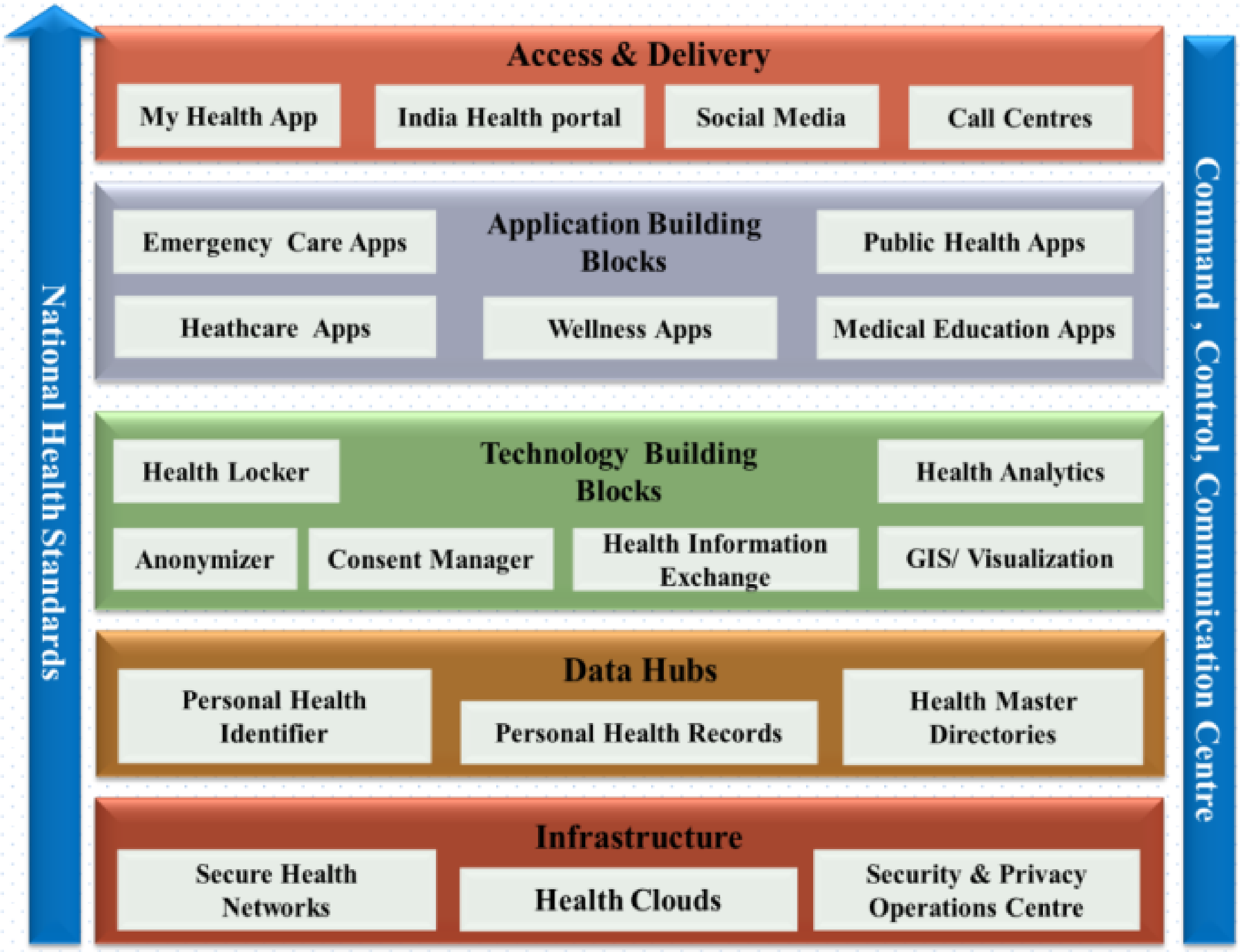
National Health Analytics Platform

National Health Upskilling Platform

National Health Registries (Providers, Doctors, Beneficiaries, Health ID, etc.)

India Stack

Aadhaar, Mobile



National Health Standards

Access & Delivery

- My Health App
- India Health portal
- Social Media
- Call Centres

Application Building Blocks

- Emergency Care Apps
- Public Health Apps
- Heathcare Apps
- Wellness Apps
- Medical Education Apps

Technology Building Blocks

- Health Locker
- Health Analytics
- Anonymizer
- Consent Manager
- Health Information Exchange
- GIS/ Visualization

Data Hubs

- Personal Health Identifier
- Personal Health Records
- Health Master Directories

Infrastructure

- Secure Health Networks
- Health Clouds
- Security & Privacy Operations Centre

Command , Control, Communication Centre

National Digital Health Blue Print

Without standards, there can be no improvement

Taiichi Ohno – Founder of Toyota Production Systems

Health Technology Standards

Vocabulary Standards

- CPT
- ICD 10/11
- LOINC
- National Drug Code (NDC)
- RadLex
- RxNorm
- SNOMED CT
- CDC
- Unified Code Units of Measure

Content

- Consolidated CDA
- HL7
- FHIR

Transport

- DICOM

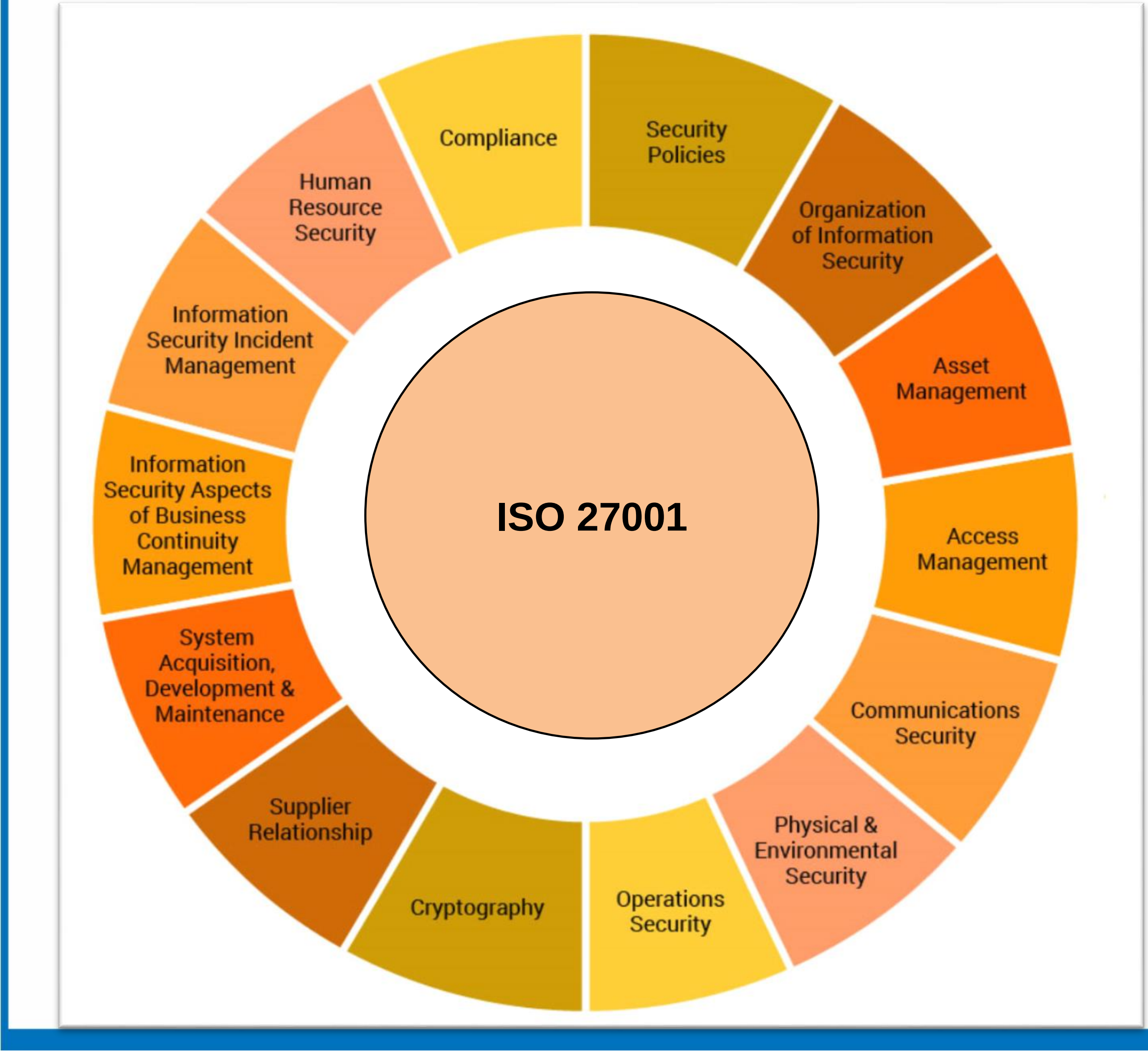
Security

- ISO 27001 Standards
- Personal Data Protection

ISO 27001

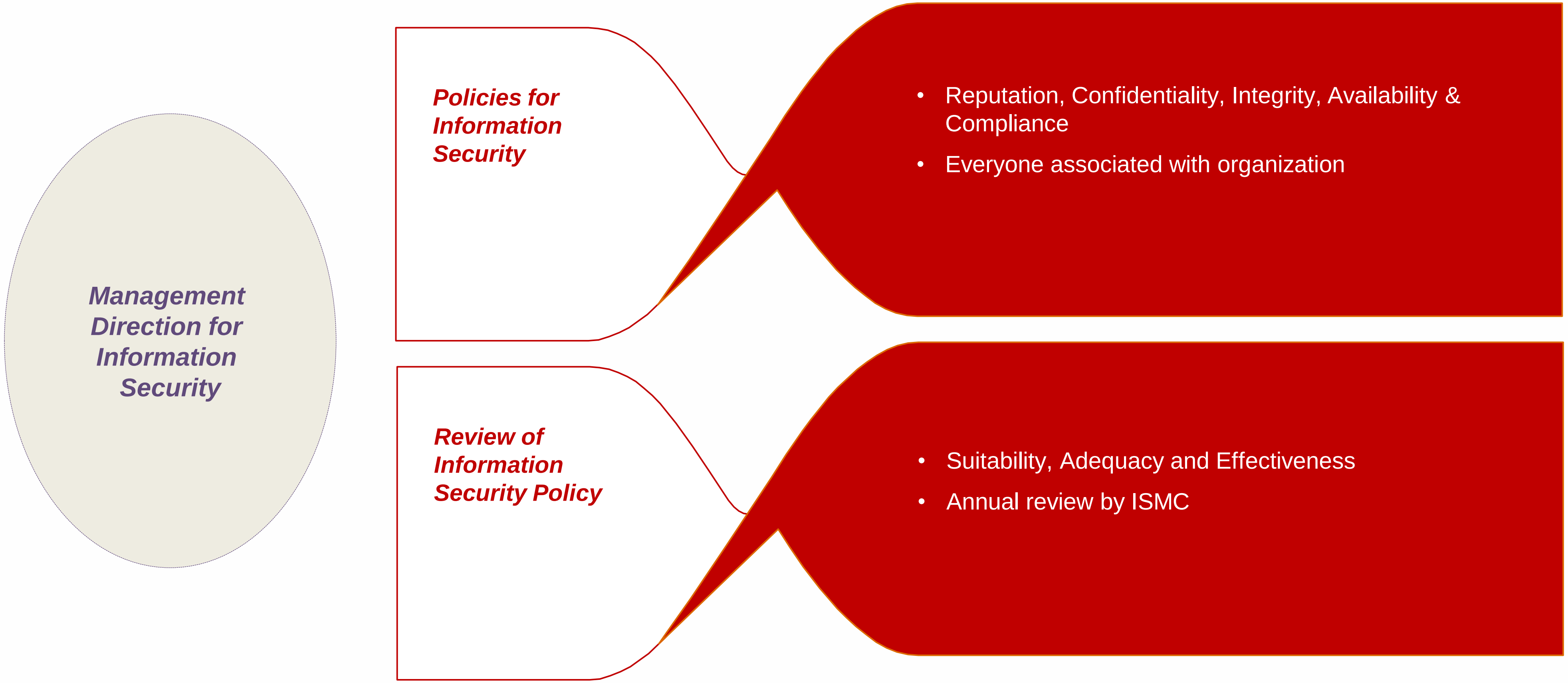
Overview

- Globally recognized framework
- Aligned to PDCA model of ITIL
- Top – Down approach
- Continual improvement
- Reputation, People, Process, Technology & Compliance
- 14 Domains, 35 Control Objectives, 114 Controls


ISO 27001
Security Policies
Organization of Information Security
Asset Management
Access Management
Communications Security
Physical & Environmental Security
Operations Security
Cryptography
Supplier Relationship
System Acquisition, Development & Maintenance
Information Security Aspects of Business Continuity Management
Information Security Incident Management
Human Resource Security
Compliance

ISO 270001 Domains

Domain 1: Information Security Policies



Management Direction for Information Security

Policies for Information Security

- Reputation, Confidentiality, Integrity, Availability & Compliance
- Everyone associated with organization

Review of Information Security Policy

- Suitability, Adequacy and Effectiveness
- Annual review by ISMC

Domain 2 Organization of Information Security

Information Security Roles and Responsibilities

- Define ISMC Organization Structure
- Agreed Roles & Responsibilities
- Establish Security Forums

Segregation of Duties

- Formation of SoD
- Compensating controls where SoD is not possible

Contact with Authorities

- Maintain relevant contacts such as Fire, Emergency, Law enforcement agencies, etc.,

Contact with Special Interest Groups

- Maintain relevant contacts with special interest groups such as BSI, HIPAA, ISF, etc.,
- Display relevant contacts on premise

Information Security in Project Management

- Maintain and monitor Information Security adherence on all project and/or initiatives

Internal Organization

Mobile Device Policy

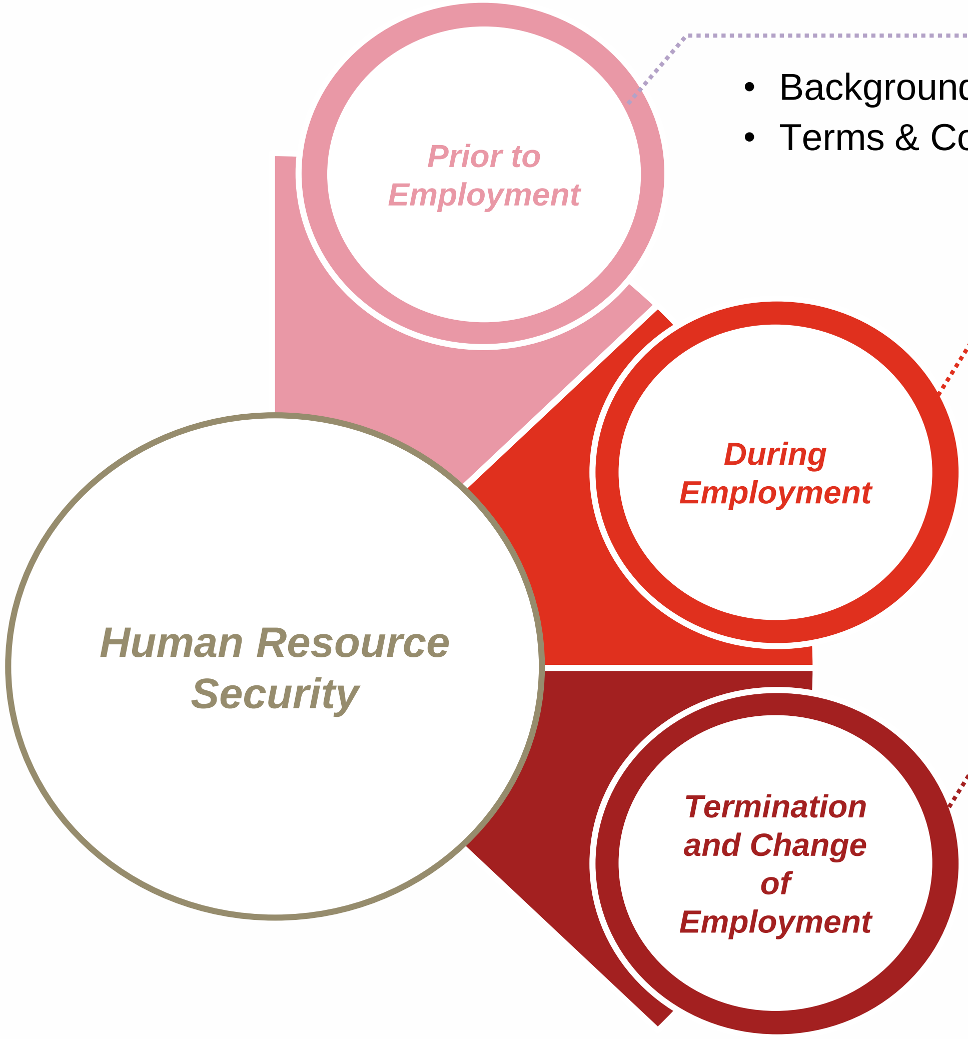
- Governed by appropriate controls
- BYOD Governance and minimum controls
- Adherence to Acceptable Usage Policy (AUP)

Teleworking

- Identification of Teleworking Sites
- Physical Access Governance
- Secure Communication Channel

Mobile Devices & Teleworking

Domain 3 Human Resource Security

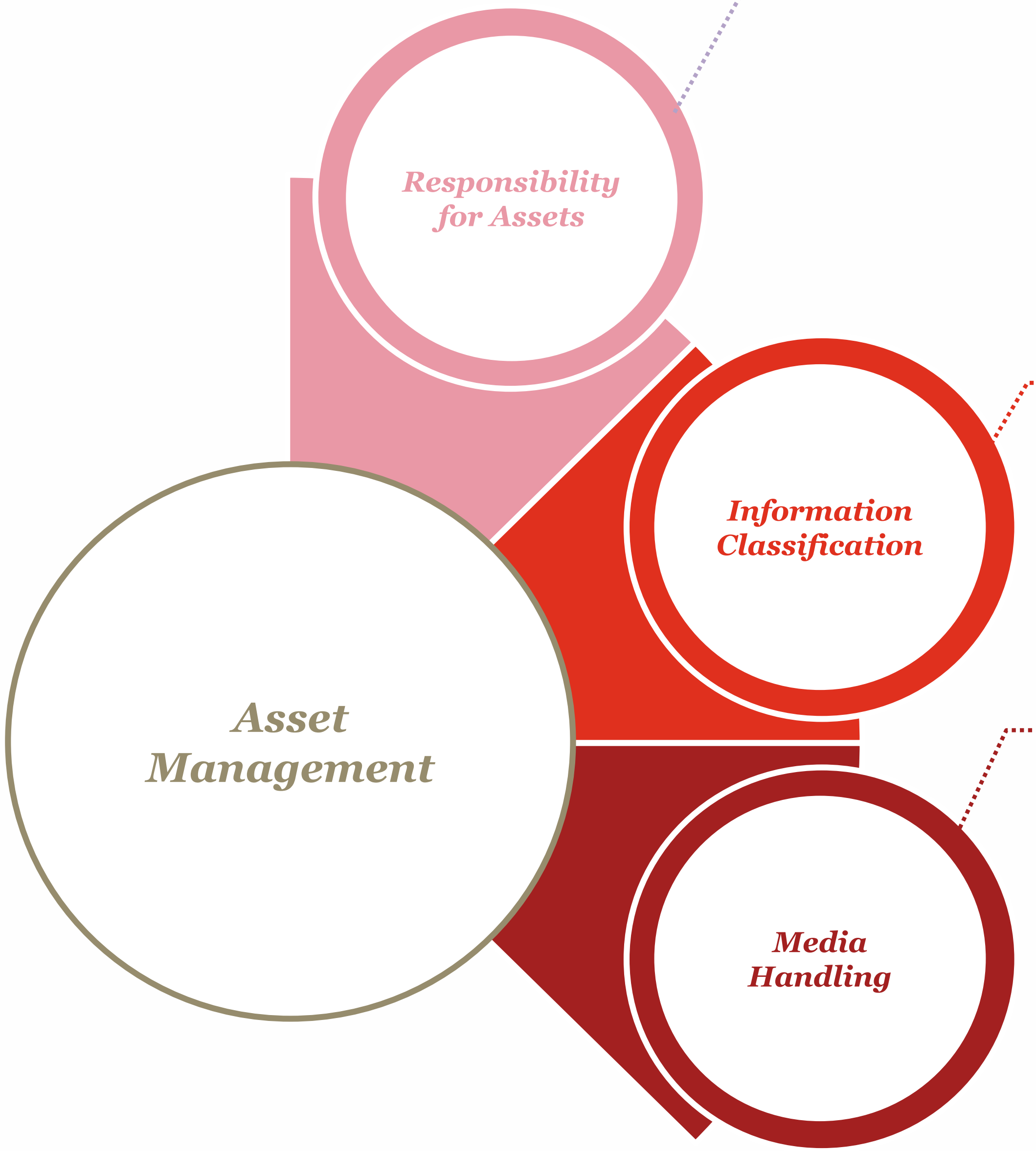


- Background Checks
- Terms & Conditions of Employment

- Management Responsibilities
- Sufficient Training & Awareness
- Disciplinary Processes

- Documented responsibilities towards termination and change in employment
- Governance for Access Modification, Revocation and Addition

Domain 4 Asset Management



Inventory of Assets

- Document and Maintain inventory of all Assets
- Assets managed based on classification

Inventory of Assets

- Identify and assign Asset Owners

Acceptable Use of Assets

- Identify, Document and Implement Acceptable Use of Assets

Return of Assets

- Assets shall be returned in accordance with Policy

Classification of Information

- Public, Internal, Confidential, Secret, Restricted

Labelling of Information

- Asset owners to apply labelling based on classification

Handling of Assets

- Document and Implement Asset Handling in accordance with Policy

Management of Removable Media

- Document Controls and Guidelines for Media Removal
- Control and Maintain Media Removal Register

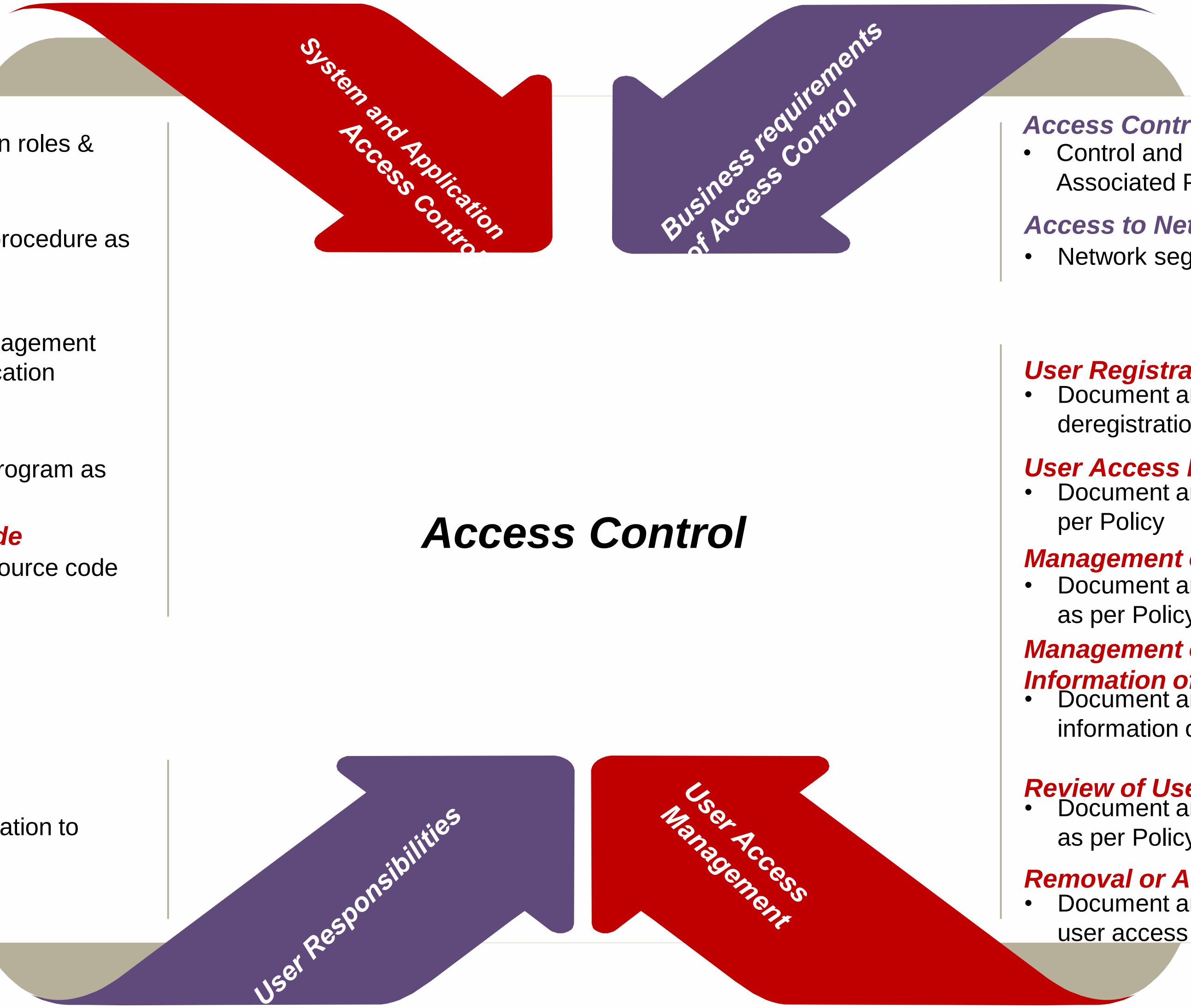
Disposal of Media

- Document Controls and Guidelines for Media Disposal
- Control and Maintain Media Disposal Register

Physical Media Transfer

- Document Controls and Guidelines Physical Media Transfer

Domain 5 Access Control


System and Application Access Control
Business requirements of Access Control
Access Control
User Responsibilities
User Access Management

Information Access Restriction

- Access restrictions to be applied based on roles & responsibilities

Secure Logon Procedures

- Document and implement secure logon procedure as per Policy

Password Management System

- Document and implement password management system including securing and communication procedure as per Policy

Use of Privileged Utility Program

- Control and implement privileged utility program as per Policy

Access Control to Program Source Code

- Control and monitor access to program source code as per Policy

Use of Secret Authentication Information

- Adequacy of secret authentication information to protect assets

Access Control Policy

- Control and Monitor User Access Rights and Associated Privileges

Access to Network and Network Services

- Network segregation and monitor network services

User Registration and Deregistration

- Document and Control user registration and deregistration

User Access Provisioning

- Document and Maintain user access provisioning as per Policy

Management of Privileged Access Rights

- Document and Maintain privileged user provisioning as per Policy

Management of Secret Authentication Information of User

- Document and Maintain secret authentication information of user as per Policy

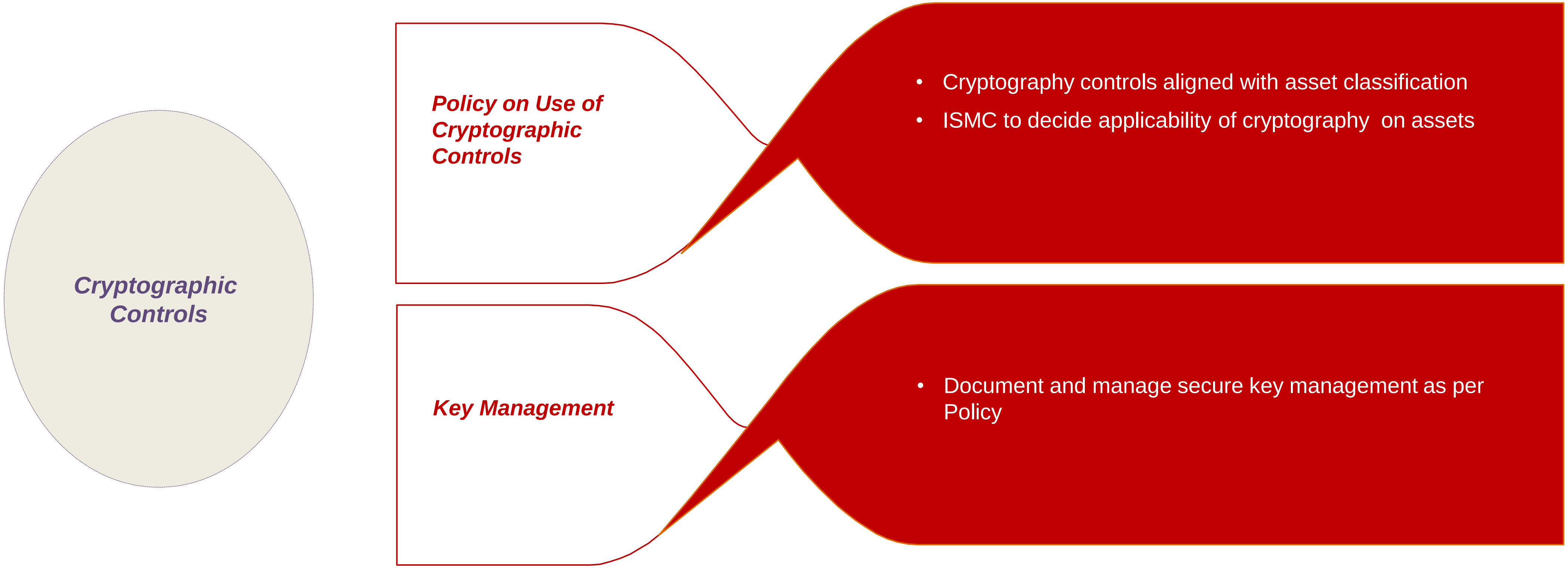
Review of User Access Rights

- Document and Maintain review of user access rights as per Policy

Removal or Adjustment of Access Rights

- Document and Maintain removal or adjustment of user access rights as per Policy

Domain 6 Cryptography



Cryptographic Controls

Policy on Use of Cryptographic Controls

- Cryptography controls aligned with asset classification
- ISMC to decide applicability of cryptography on assets

Key Management

- Document and manage secure key management as per Policy

Domain 7 Physical and Environmental Security

Physical Security Perimeter

- Physical security perimeter to be defined and physical appropriate controls be implemented

Physical Entry Controls

- Maintain and monitor physical access to organization facilities

Securing Office, Rooms and Facilities

- Maintain and monitor physical access to organization facilities

Protecting against External and Environmental Threats

- Document and implement protection against external and environmental threats

Working in Secure Areas

- Identity and implement security controls in restricted areas

Delivery and Loading Areas

- Identity and isolate delivery & loading areas

Secure Areas

Equipment Siting & Protection

- Located and protected in line with its criticality and classification

Supporting Utilities

- All equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities

Cabling Security

- Define and implement appropriate cabling standards for data networking, electric power and telecommunications cables

Equipment Maintenance

- Equipment maintenance standards and procedures shall be followed considering asset classification

Removal of Assets

- Document and maintain records related to removal of assets

Security of Equipment and Asset off-premises

- All equipment are in compliance with security Policy

Secure Disposal or Re-Use Equipments

- All equipment are in compliance with asset disposal Policy

Unattended User Equipments

- Appropriate security measures shall be adopted to protect the unattended equipment

Clear Desk and Clear Screen

- Assets are suitably protected using clear desk and clear screen policy

Equipment Security

Domain 8 Operations Security

Information Systems Audit Controls

- Documented procedures for Information System Audit Controls

Management of Vulnerabilities

- Documented procedures for Vulnerability Management

Installation of Software on Operational Environments

- Documented procedures for software installations on operational environments

Event Logging

- Documented Event Logging Procedures

Protection of Log Information

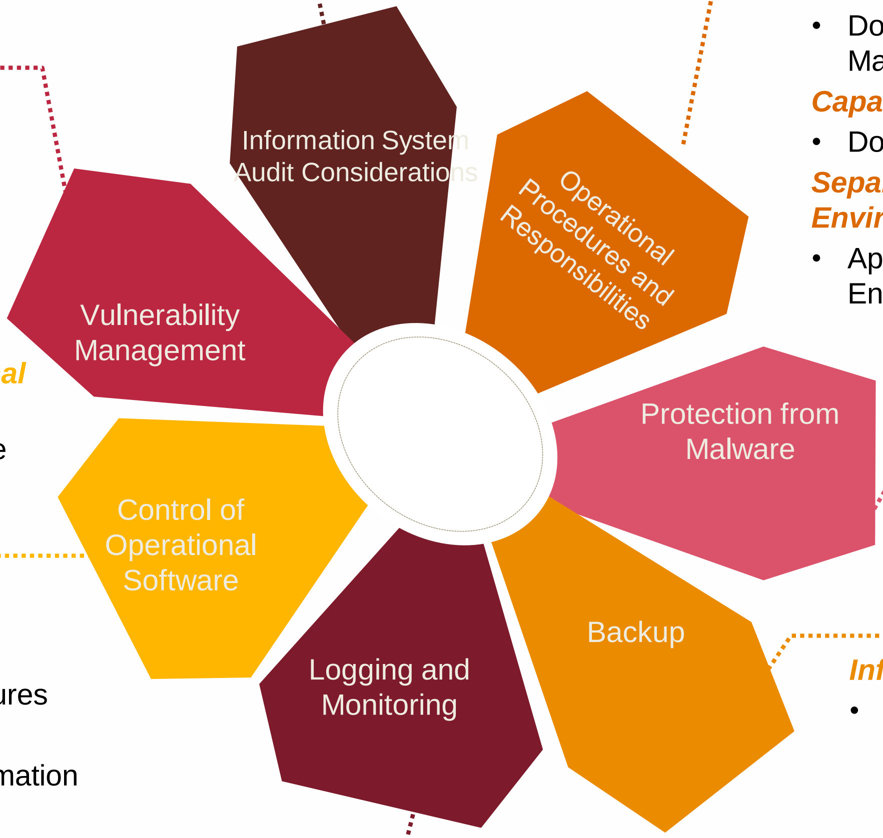
- Documented Protection of Log Information

Administrator and Operator Logs

- Documented procedures for Administrator and Operator Logs

Clock Synchronization

- Documented procedure for Clock Synchronization


Information System Audit Considerations
Operational Procedures and Responsibilities
Protection from Malware
Backup
Logging and Monitoring
Control of Operational Software
Vulnerability Management

Documented Operating Procedures

- Operating procedures are documented and communicated

Change and Release Management

- Documented operating procedures for Change and Release Management

Capacity Management

- Documented Capacity Management procedures

Separation of Development, Testing and Operational Environments

- Appropriate separation of Development, Testing and Production Environments

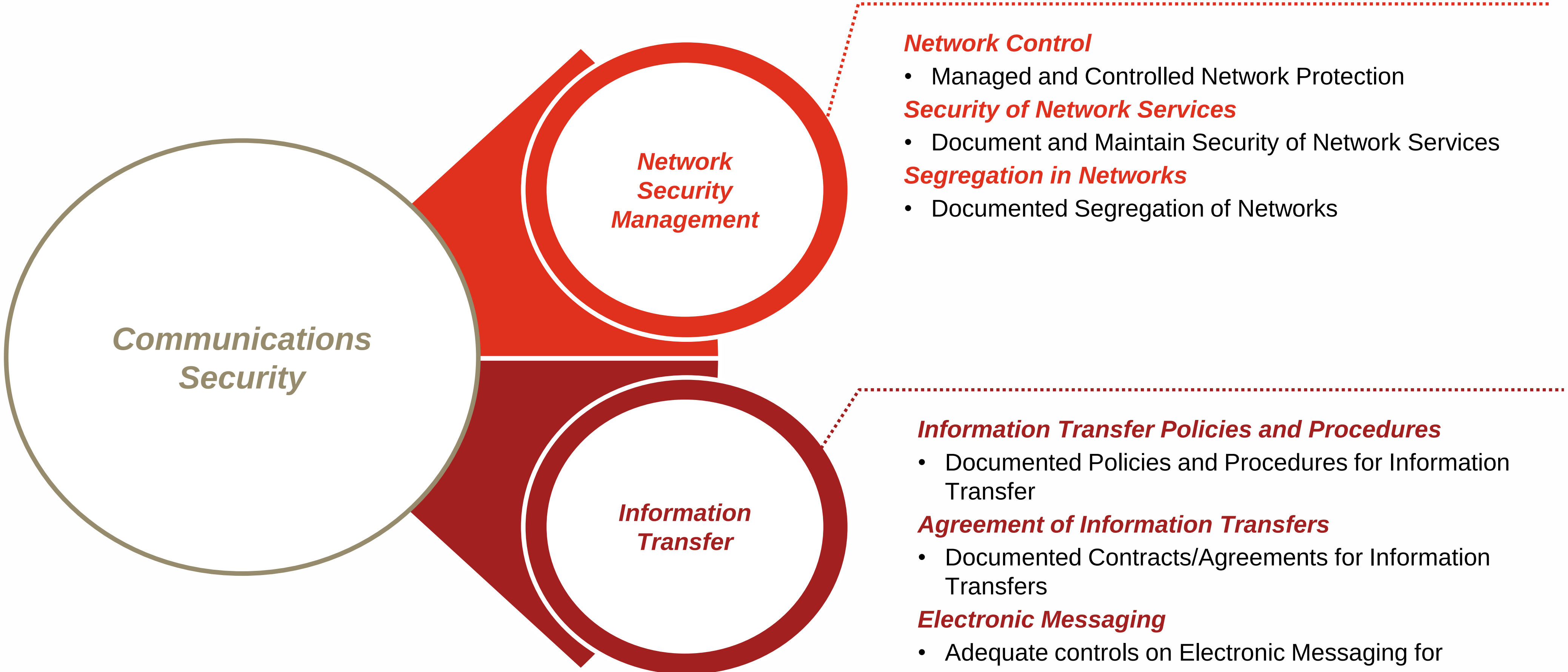
Controls against Malware

- Documented controls against Malware

Information Backup

- Documented procedures for
  - Backup and Restoration
  - Backup Verification and Testing
  - Backup Storage and Retention

Domain 9 Communications Security



Network Control

- Managed and Controlled Network Protection

Security of Network Services

- Document and Maintain Security of Network Services

Segregation in Networks

- Documented Segregation of Networks

Information Transfer Policies and Procedures

- Documented Policies and Procedures for Information Transfer

Agreement of Information Transfers

- Documented Contracts/Agreements for Information Transfers

Electronic Messaging

- Adequate controls on Electronic Messaging for Information Transfer

Confidentiality and Non-Disclosure Agreements

- Documented Confidentiality and NDA clauses for Information Transfer

Domain 10 System Acquisition, Development and Maintenance

Information Security Requirements Analysis and Specification

- New product to be Information Security compliant

Securing application services on public networks

- Maintain and monitor security controls as per law on all public networks

Protecting application services transactions

- Maintain and monitor application services for Information Security Compliance

Security Requirements of Information Security

Secure Development Policy

- Document and monitor adherence to information security controls during application development and/or enhancement

System Change Control Procedure

- Document and monitor Change Control procedure

Technical Review of Applications after Operational Platform Changes

- Document and monitor procedures for all changes in organization Assets

Restrictions on Changes to Software Packages

- Document and implement only essential changes to software packages

Secure Systems Engineering Principles

- Document and implement secure system engineering principles

Secure Development Environment

- Document and implement secure development environment

System Security Testing

- Document and implement secure testing environment

Secure Acceptance Testing

- Document and implement secure acceptance testing

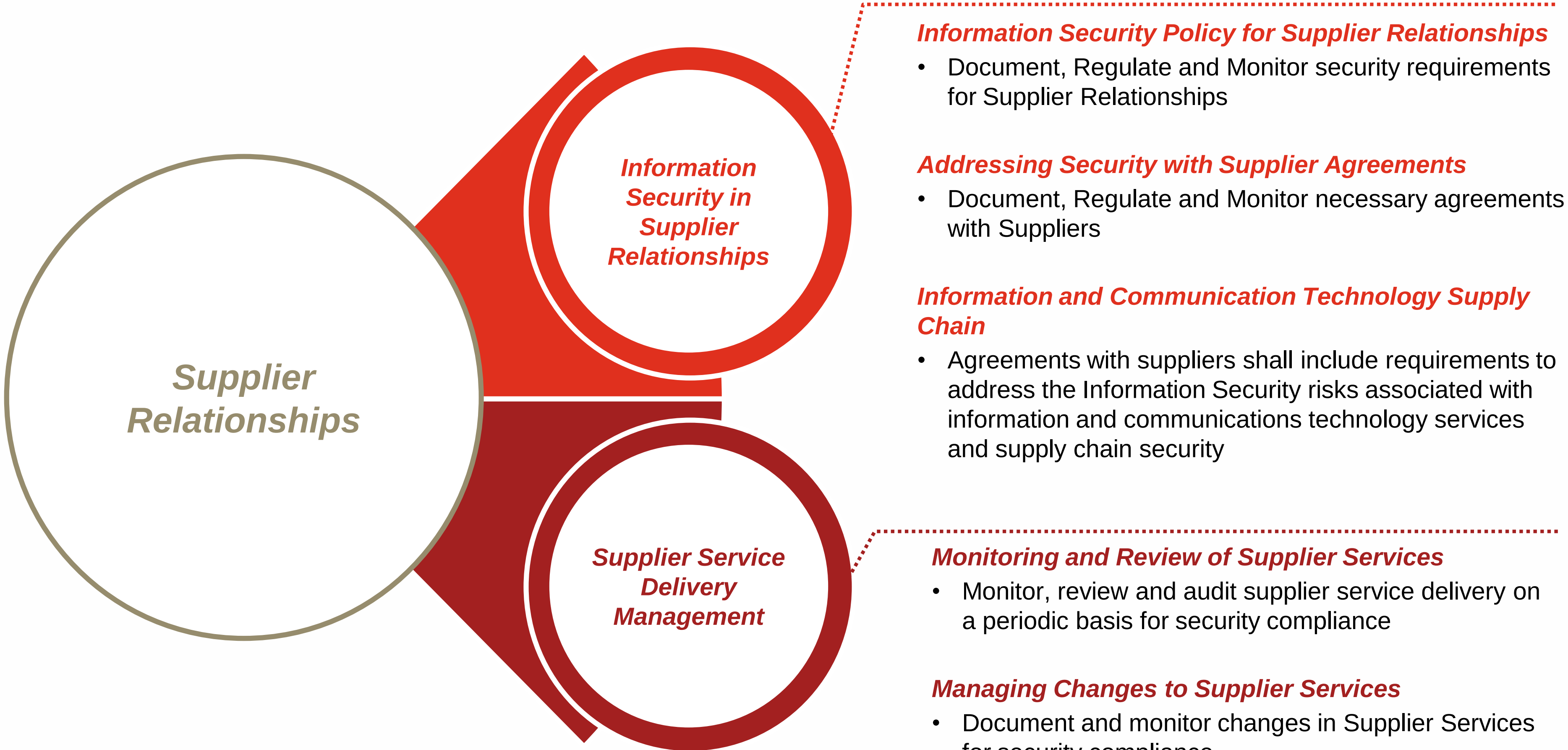
Security in Development and Support Process

Protection of Test Data

- Document and implement prohibition of using production data for testing

Test Data

Domain 11 Supplier Relationships


Supplier Relationships
Information Security in Supplier Relationships
Supplier Service Delivery Management

Information Security Policy for Supplier Relationships

- Document, Regulate and Monitor security requirements for Supplier Relationships

Addressing Security with Supplier Agreements

- Document, Regulate and Monitor necessary agreements with Suppliers

Information and Communication Technology Supply Chain

- Agreements with suppliers shall include requirements to address the Information Security risks associated with information and communications technology services and supply chain security

Monitoring and Review of Supplier Services

- Monitor, review and audit supplier service delivery on a periodic basis for security compliance

Managing Changes to Supplier Services

- Document and monitor changes in Supplier Services for security compliance

Domain 12 Information Security Incident Management Policy

Management of Information Security Incidents and Improvements

Responsibilities and Procedures

- Document and Manage Information Security Incidents

Reporting Information Security Events

- Document and Maintain reporting of Information Security Events

Reporting Information Security Weaknesses

- Document and Manage Information Security Weaknesses

Assessment of and Decision on Information Security Events

- Document and Maintain classification, prioritization and decisions related to Information Security Events

Response to Information Security Incidents

- Document and Maintain Information Security Incident Response

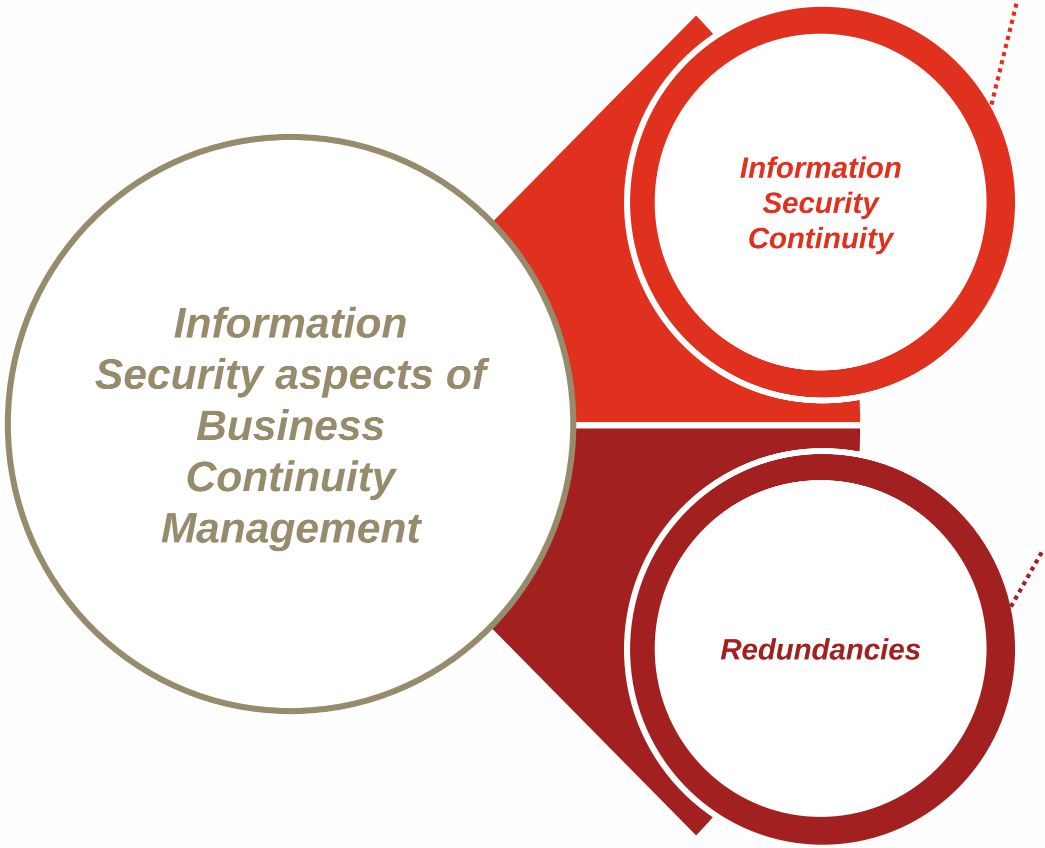
Learning from Information Security Incidents

- Document and Maintain knowledgebase of Information Security Incidents and corresponding remediation

Collection of Evidences

- Document and Implement procedures related to collection of evidences on Information Security Incidents

Domain 13 Information Security Aspects of Business Continuity Management


Information Security aspects of Business Continuity Management
Information Security Continuity
Redundancies

Planning Information Security Continuity

- Define, Document and Implement Disaster Recovery Plan
- Define, Document and Implement Information Recovery Guidelines

Implementing Information Security Continuity

- Define, Document and Implement Business Continuity Management Framework

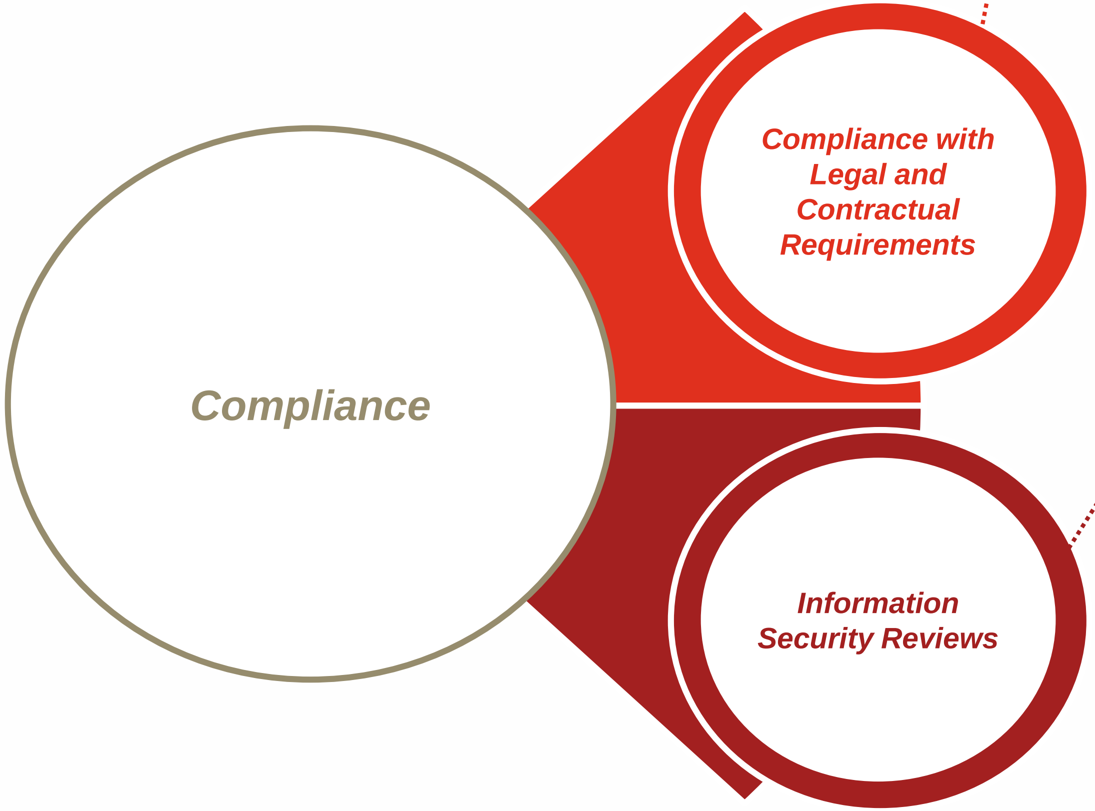
Verify, Review and Evaluate Information Security Continuity

- Document and Manage Business Continuity and Disaster Recovery Plan

Availability of Information Processing Facilities

- Document and Monitor business critical information systems
- Document and Monitor redundant components prior using in case of eventuality

Domain 14 Compliance


Compliance
Compliance with Legal and Contractual Requirements
Information Security Reviews

Identification of Applicable Legislation and Contractual Requirements

- Document and Manage relevant Regulatory and Legal compliance for Information Security

Intellectual Property Rights (IPR)

- Define, Document and Monitor Licenses, Patent, Copyright, IPRs, etc.,

Protection of Records

- Define, Document and Monitor records in accordance with relevant Regulatory, Legal and Statutory compliance

Privacy and Protection of Personally Identifiable Information

- Define, Document and Monitor Personally Identifiable and Privacy related information

Regulation of cryptographic controls

- Document and Manage Compliance Assurance

Independent Review of Information Security

- Define and Implement periodic independent Information Security review to assess current state

Compliance with Security Policies and Standards

- Define and Implement periodic self-assessment of Information Security posture and remediate as necessary

Technical Compliance Review

- Document and Implement Information Security compliance checklist for all the assets

Data Privacy

State of Privacy

WE JUST WANT TO TRACK YOUR CUSTOMER JOURNEY SO THAT WE CAN ENGAGE WITH YOU BETTER.
YA 32 43246
TOM FISH BURNE

© marketoonist.com

SELLING MY OWN DAMN DATA
I WENT TO POPEYE'S 5 TIMES THIS WEEK
I HAVE SIX COUSINS ON MY MOM'S SIDE
SAID "AVOCADO" TWICE TODAY
STILL NOT SURE WHAT A 401k IS
IT TOOK ME TWO HOURS TO DECIDE WHAT TO WATCH ON NETFLIX YESTERDAY
MADE A SPOTIFY PLAYLIST FOR MY DOG.
HUNG DRY MY CLOTHES ON A USB CABLE
MISSED MY FLIGHT TO SEATTLE SO I DID NOT GO.
CRIED WHILE CUTTING BOK CHOY
GAVE $7 TO A MASSAGE CHAIR ON KICKSTARTER
j.nguyen

CUTTING OUT THE MIDDLEMAN

Information about you, what you buy, where you go, even where you *look* is the oil that fuels the digital economy

What is Data Privacy and Data Security

Data Privacy

Data Privacy governs how data is collected, shared and used.

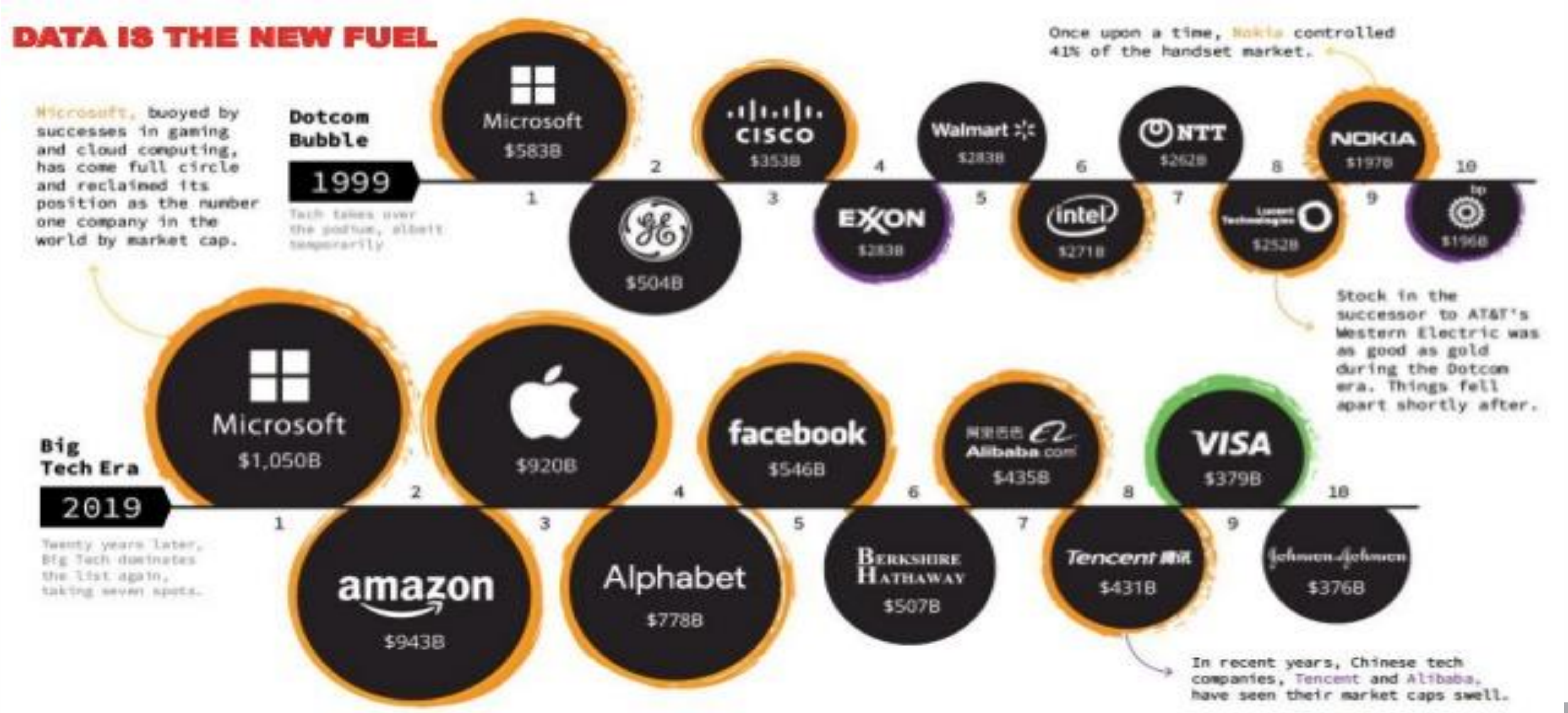
Data Security

Data Security protects data from compromise by external attackers and malicious insiders.

Types of Privacy

- **Informational Privacy** refers to all data about a person, in general everything other people know about a person, and especially includes individual-related data
- **Physical Privacy** refers to the intrusions into one's physical space or solitude
- **Decisional Privacy** refers to the protection of individual from government interference with personal and family decisions
- **Proprietary Privacy** refers to the right an individual has to his/her genetic information.

Data is the New “Fuel”



DATA IS THE NEW FUEL

Dotcom Bubble

1999

Tech takes over the podium, albeit temporarily

1 Microsoft $583B
2 GE $504B
3 CISCO $353B
4 EXXON $283B
5 Walmart $283B
6 intel $271B
7 NTT $262B
8 Lucent Technologies $252B
9 NOKIA $197B
10 bp $196B

Microsoft, buoyed by successes in gaming and cloud computing, has come full circle and reclaimed its position as the number one company in the world by market cap.

Once upon a time, Nokia controlled 41% of the handset market.

Stock in the successor to AT&T's Western Electric was as good as gold during the Dotcom era. Things fell apart shortly after.

Big Tech Era

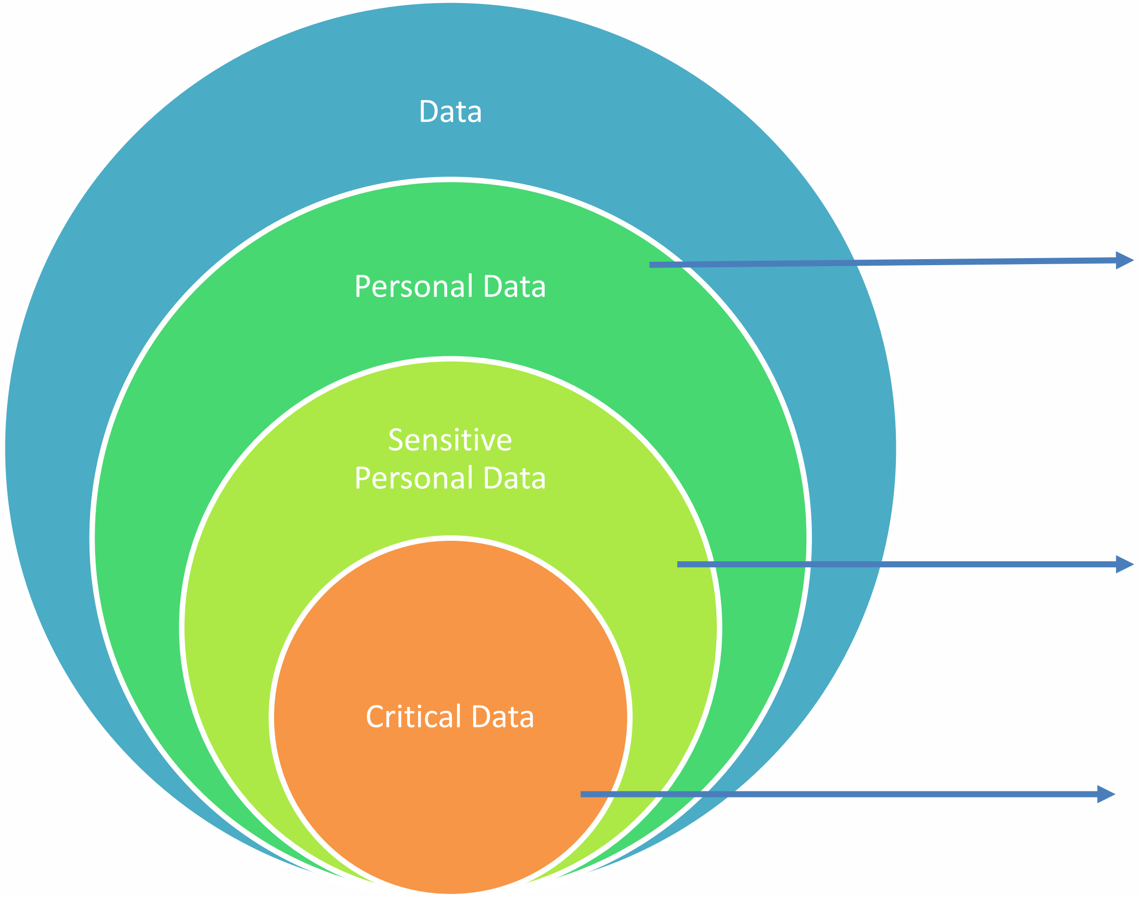
2019

Twenty years later, Big Tech dominates the list again, taking seven spots.

1 Microsoft $1,050B
2 amazon $943B
3 $920B
4 Alphabet $778B
5 facebook $546B
6 Berkshire Hathaway $507B
7 Alibaba.com $435B
8 Tencent 腾讯 $431B
9 VISA $379B
10 Johnson&Johnson $376B

In recent years, Chinese tech companies, Tencent and Alibaba, have seen their market caps swell.

Data Classification



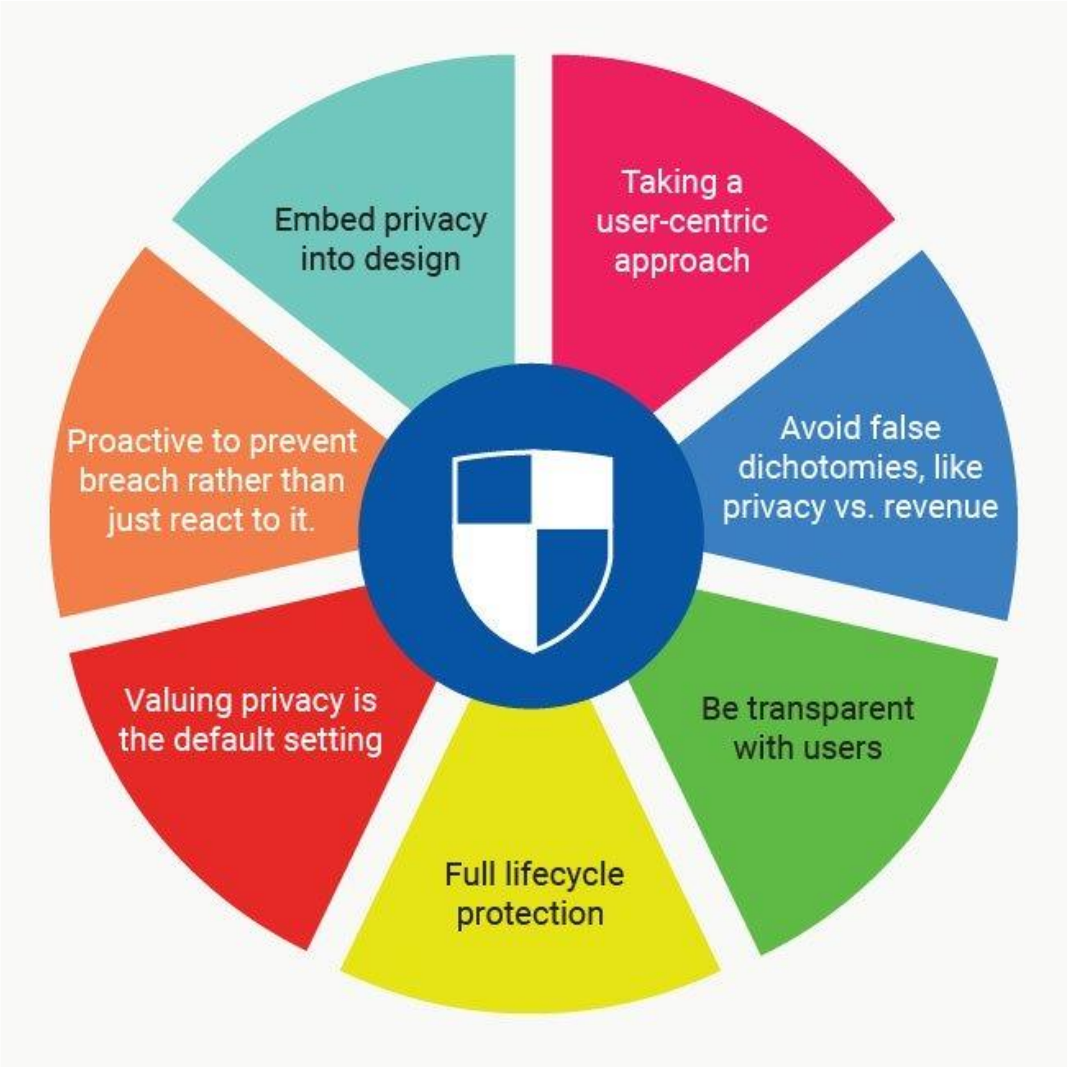
- Data Qualifies as personal data as soon as an individual can be singled out Ex: PAN Card, Passport

- Personal Data Sensitive in Nature
- In relation to subject’s fundamental rights & Freedoms. Impacts the individuals existence in the society ex: Politically Exposed Person/Celebrity Patient with a chronic disease, Financial Data, Sexual Orientation of a person, Caste etc..
- Could create significant risk to subject
- Classification of SPI is country, society and culture specific
- Government would notify what constitutes critical data

Privacy Principles

- **Notice:** Public statement of how a provider applies data protection to processing personal information, Describes how a provider collects, uses, retains and discloses personal and health information of a patient
- **Choice and Consent:** Patient should be given the choice for trading off his/her personal information to avail services. Consent should be proactively obtained, stored and preserved for any future use Should have a clear view of how the provider will use this information
- **Collection Limitation** Provider should collect only required data. Data collected should be fair and lawful means with the knowledge of the end user
- **Use Limitation:** Specifies health data should not be made available or otherwise used for any purpose other than what was agreed with the patient at the time of data collection
- **Access and Correction:** Enable the patient by providing access to the data for checking and correcting his/her record.
- **Security:** Stipulates the technical and organisation measures taken by the provider for securing the personal and health data of the patient
- **Disclosure to third party:** When sharing information with third parties, the principle of data protection should be held in these relationships
- **Openness:** Provider should have a general policy of openness about developments, practices and policies with respect to the personal data
- **Accountability:** The provider is accountable for complying the measures that give effect to the principles state

Privacy by Design


Embed privacy into design
Taking a user-centric approach
Avoid false dichotomies, like privacy vs. revenue
Be transparent with users
Full lifecycle protection
Valuing privacy is the default setting
Proactive to prevent breach rather than just react to it.

“Privacy must become integral to organizational priorities, project objectives, design processes, and planning operations. Privacy must be embedded into every standard, protocol and process that touches our lives.”

Current Framework for Data Protection In India

- The Information Technology Act 2000 and the Information Technology Amendment Act 2008 expanded the scope from a data protection standpoint
- **Sec 43 A** – For protecting Sensitive Personal Information. Will be repealed once the PDP Act gets passed
- **Sec 72 A** – For protecting Personal Information
- Entity should employ Reasonable Security Practices and Procedures. ISO 27001 or code of practices by industry associations approved by Govt. of India
- Body Corporate refers to an individual, employee , Government. Current rule excludes government of any privacy law
- In the current act the adjudicating officer has the power to direct compensation up to 5 Crores
- Appointment of grievance officer

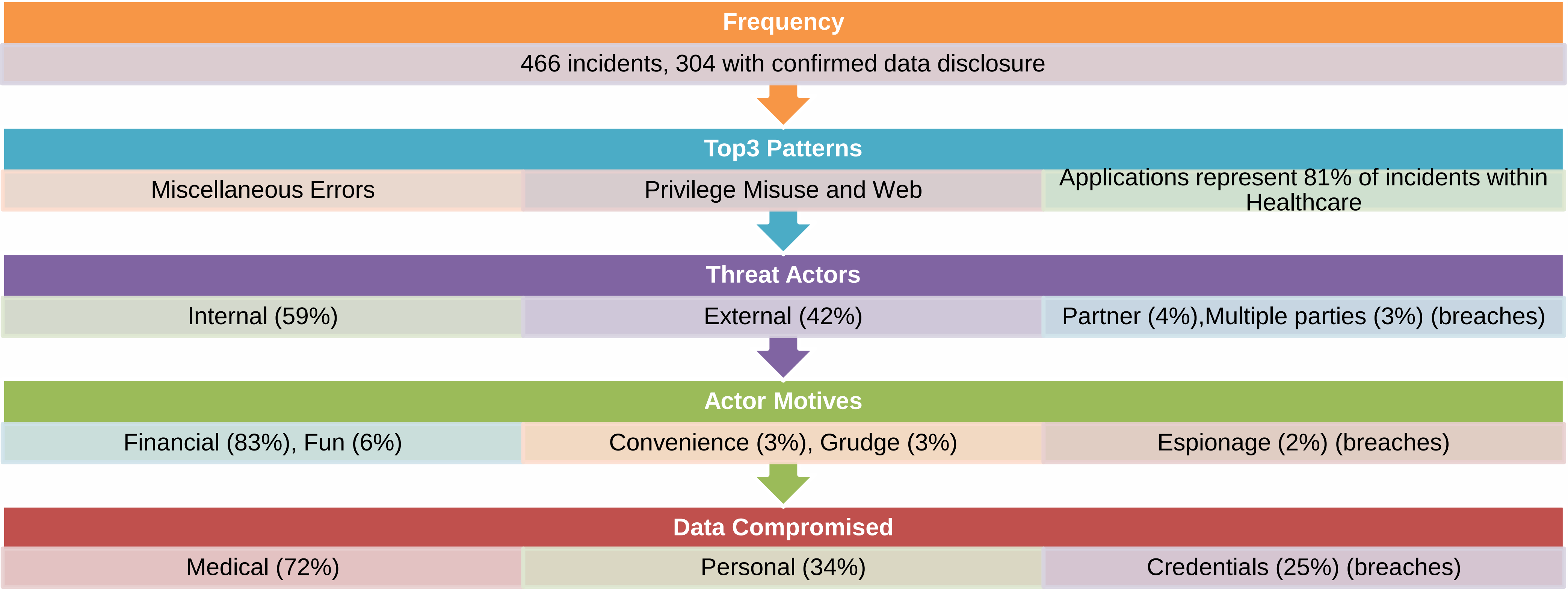
Key Highlights of Personal Data Protection Bill (Draft)

- Sensitive Personal Data
- Grounds for Processing Personal Data
- Consent
- Presentation Portability
- Right to be Forgotten
- Privacy by Design
- Transparency and Accountability
- Data Storage
- Data processing by Other Entities
- Cross Border Data Transfer
- Penalties
- Children’s Data Processing

Importance of Security & Privacy

Cybersecurity Attacks on the Rise

Healthcare stands out due to the majority of breaches being associated with internal actors. Denial of Service attacks are infrequent, but availability issues arise in the form of ransomware.



Frequency

466 incidents, 304 with confirmed data disclosure

Top3 Patterns

Miscellaneous Errors	Privilege Misuse and Web	Applications represent 81% of incidents within Healthcare

Threat Actors

Internal (59%)	External (42%)	Partner (4%),Multiple parties (3%) (breaches)

Actor Motives

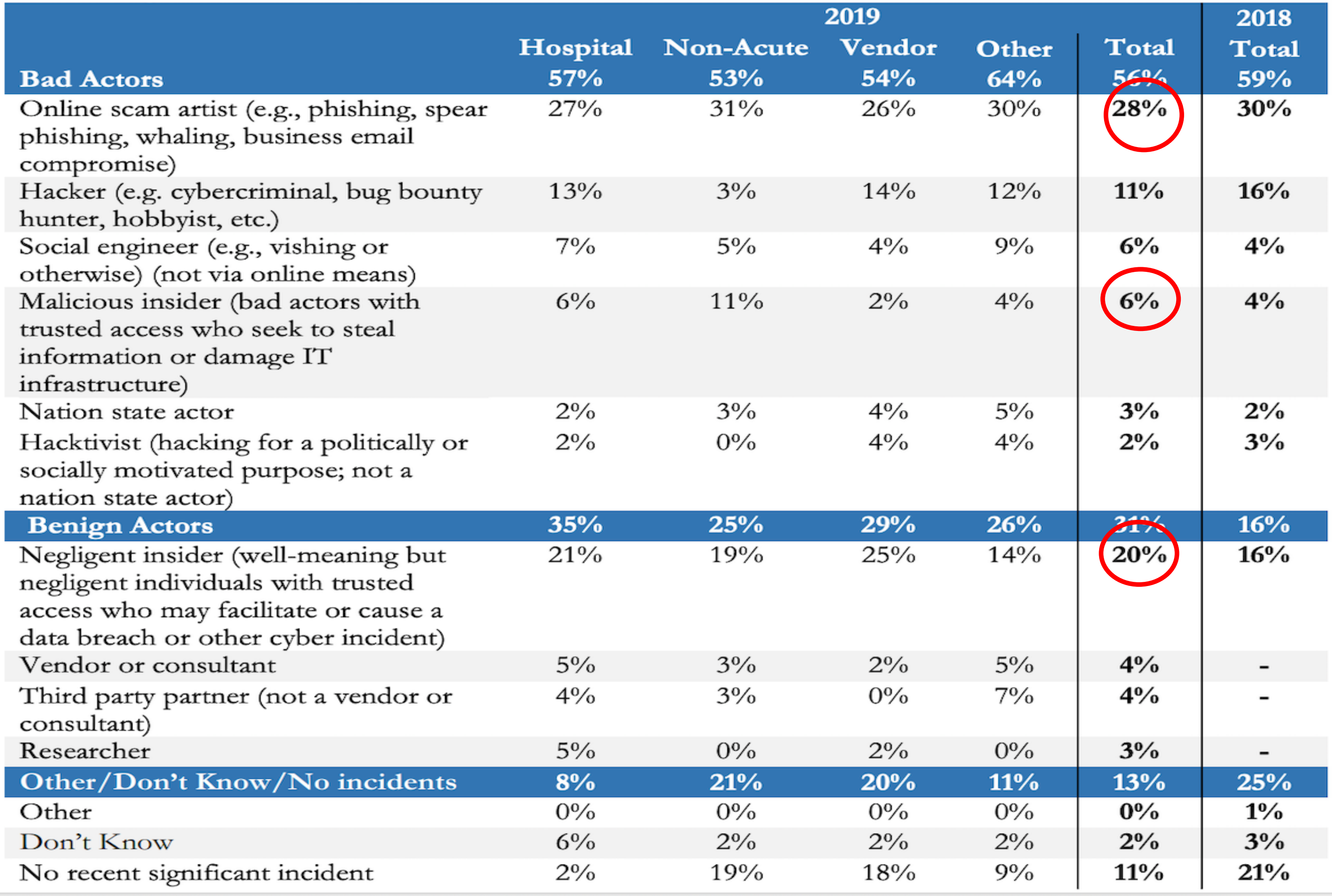
Financial (83%), Fun (6%)	Convenience (3%), Grudge (3%)	Espionage (2%) (breaches)

Data Compromised

Medical (72%)	Personal (34%)	Credentials (25%) (breaches)

Source: Verizon Data breach investigations report 2019

Significant Security Incident in the Past 12 Months – Threat Actors



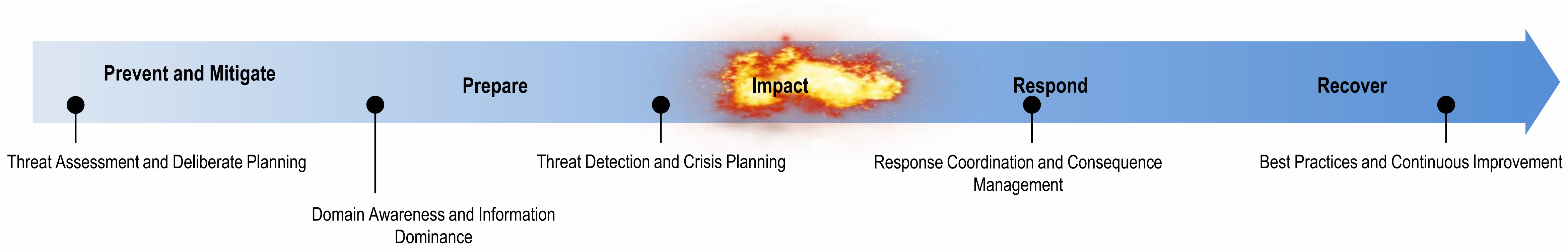
	2019					2018
	Hospital	**Non-Acute**	**Vendor**	**Other**	**Total**	**Total**
Bad Actors	**57%**	**53%**	**54%**	**64%**	**56%**	**59%**
Online scam artist (e.g., phishing, spear phishing, whaling, business email compromise)	27%	31%	26%	30%	**28%**	**30%**
Hacker (e.g. cybercriminal, bug bounty hunter, hobbyist, etc.)	13%	3%	14%	12%	**11%**	**16%**
Social engineer (e.g., vishing or otherwise) (not via online means)	7%	5%	4%	9%	**6%**	**4%**
Malicious insider (bad actors with trusted access who seek to steal information or damage IT infrastructure)	6%	11%	2%	4%	**6%**	**4%**
Nation state actor	2%	3%	4%	5%	**3%**	**2%**
Hacktivist (hacking for a politically or socially motivated purpose; not a nation state actor)	2%	0%	4%	4%	**2%**	**3%**
Benign Actors	**35%**	**25%**	**29%**	**26%**	**31%**	**16%**
Negligent insider (well-meaning but negligent individuals with trusted access who may facilitate or cause a data breach or other cyber incident)	21%	19%	25%	14%	**20%**	**16%**
Vendor or consultant	5%	3%	2%	5%	**4%**	**-**
Third party partner (not a vendor or consultant)	4%	3%	0%	7%	**4%**	**-**
Researcher	5%	0%	2%	0%	**3%**	**-**
Other/Don't Know/No incidents	**8%**	**21%**	**20%**	**11%**	**13%**	**25%**
Other	0%	0%	0%	0%	**0%**	**1%**
Don't Know	6%	2%	2%	2%	**2%**	**3%**
No recent significant incident	2%	19%	18%	9%	**11%**	**21%**

Source: HIMSS Cyber Security Survey 2019

Cycle of Emergency Management

An effective methodology for threat management is **systematic and consistent** between operational environments and threat scenarios

- Information is critical to understanding threats, assessing and managing risk in a cyclical process
- Threat-specific expertise and decision tools must be employed to make effective use of information

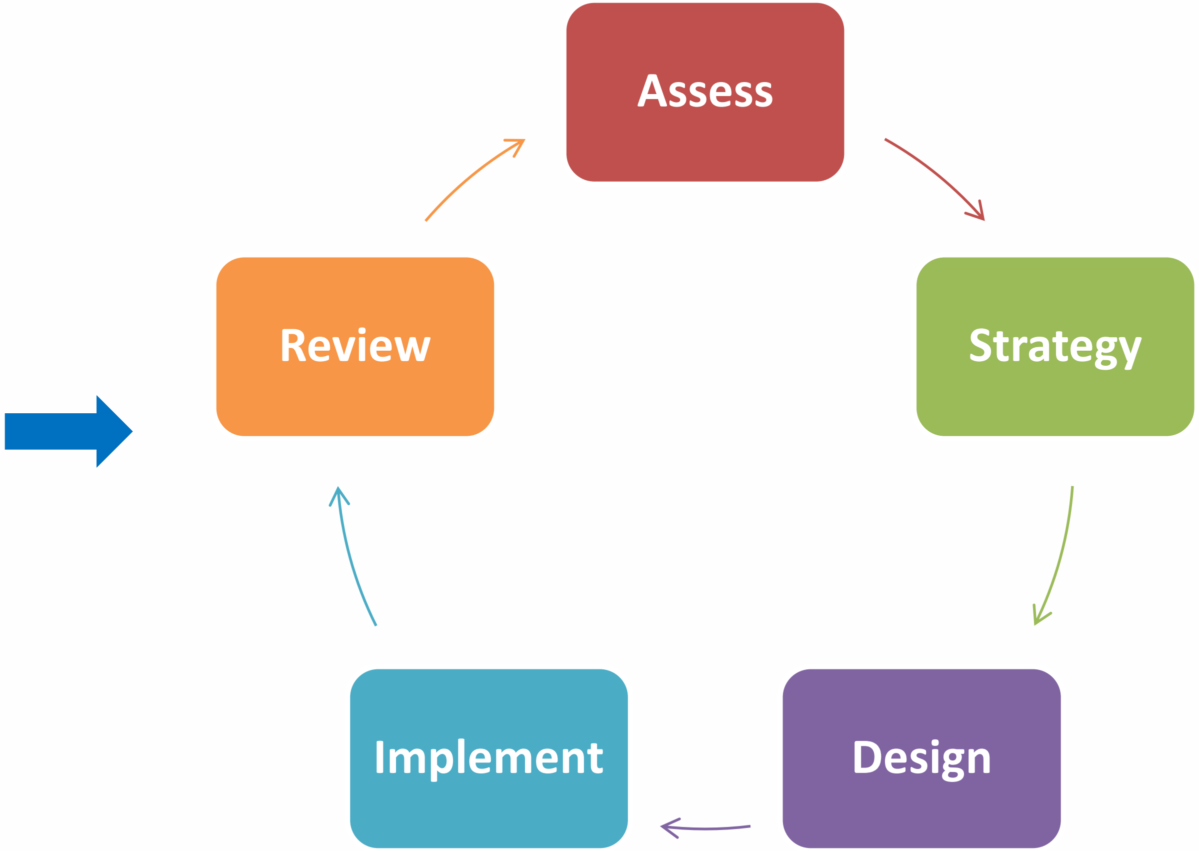


Prevent and Mitigate
Prepare
Impact
Respond
Recover
Threat Assessment and Deliberate Planning
Domain Awareness and Information Dominance
Threat Detection and Crisis Planning
Response Coordination and Consequence Management
Best Practices and Continuous Improvement

Source: HIMSS Healthcare Cyber Security Community, 2016

What should be our approach?

- Embed privacy and security across all aspect of technology
- Conduct an assessment to understand the current state, perform a gap analysis and identify the needs
- Secure Executive sponsorship
- Perform a Enterprise Security and risk assessment
- One size fits all approach will not work
- Don’t copy, paste policies, and procedures
- Security and privacy is everyone’s responsibility
- Security and Privacy does not have a destination…it is a journey !!! So start now …



References

- https://www.dsci.in/content/dsci-privacy-framework-dpf%C2%A9
- https://prsindia.org/billtrack/personal-data-protection-bill-2019
- https://www.dlapiperdataprotection.com/index.html
- https://privacyrights.org/
- http://cbprs.org/
- ISO 270001
- Verizon Data Breach Report
- HIMSS Cyber Security Report

Recap

We discussed

- ✓ Need for Standards
- ✓ Nation Digital Health Blueprint
- ✓ ISO 270001 domains
- ✓ Key overview of data security and privacy and its impact on Healthcare
- ✓ Emergency Management
- ✓ Approach to Data Security and Privacy Implementation

Activity

Based on what you learnt from this module,

- Do a high-level research on healthcare related security and privacy standards followed in European Union, Canada and Australia. Based on this prepare a 5-minute video to demonstrate your understanding.
- Understand the various types of threat vectors like Malware, Ransomware, Trojan, Worm etc. and also attacks like Phishing, Smishing, Vishing, Credential Stuffing, Brute Force Attack. Post this speak to your IT Head, Chief Information officer/Chief Information Security officer/Information Security manager and understand the steps taken by them to protect against the various threat vectors and attack types

Thank you