Introduction to Information Security Management : ISO 27000 family of standards and its requirements

- K S S Murali Krishna

Takeaways for…Legal practitioners

- Legal profession
- Law enforcement
- Legal consultancy
- Workforce
- Students of Law

Data breaches are on the rise, often crippling organisations and compromising privacy of customers and citizens. How to protect gullible, defend or render assistance to affected parties? (Possibilities and challenges)

Over this week you are revisiting…

- Laws (Cyber crime vs law, Data Protection Laws of diff countries, GDPR, IT Act 2008, CERT-In & NIC guidelines)
- Cyber warfare, threats & vulnerabilities
- Cyber Crimes
- Social media crimes
- Internet Governance (ICANN. Domain names..)
- Cyber Security (intro)
- Mobile Security
- Banking Tech, Fintech
- Cyber Crisis Management (techniques)
- Incident Handling
- Forensic Investigations
- Electronic Contracts
- Cryptography
- Intro to ISO 27000 family

Using ISO 27001

- A kind of gold standard for ISMS (protect information assets)
- Provides know-how to protect most valuable information assets
- All responsible functionaries should have minimal foundational understanding
- Many claim ISO 27001 certifications – but what does it really mean
- Prove to partners, customers, etc – that they are taking "due care" of their critical and sensitive data & environments

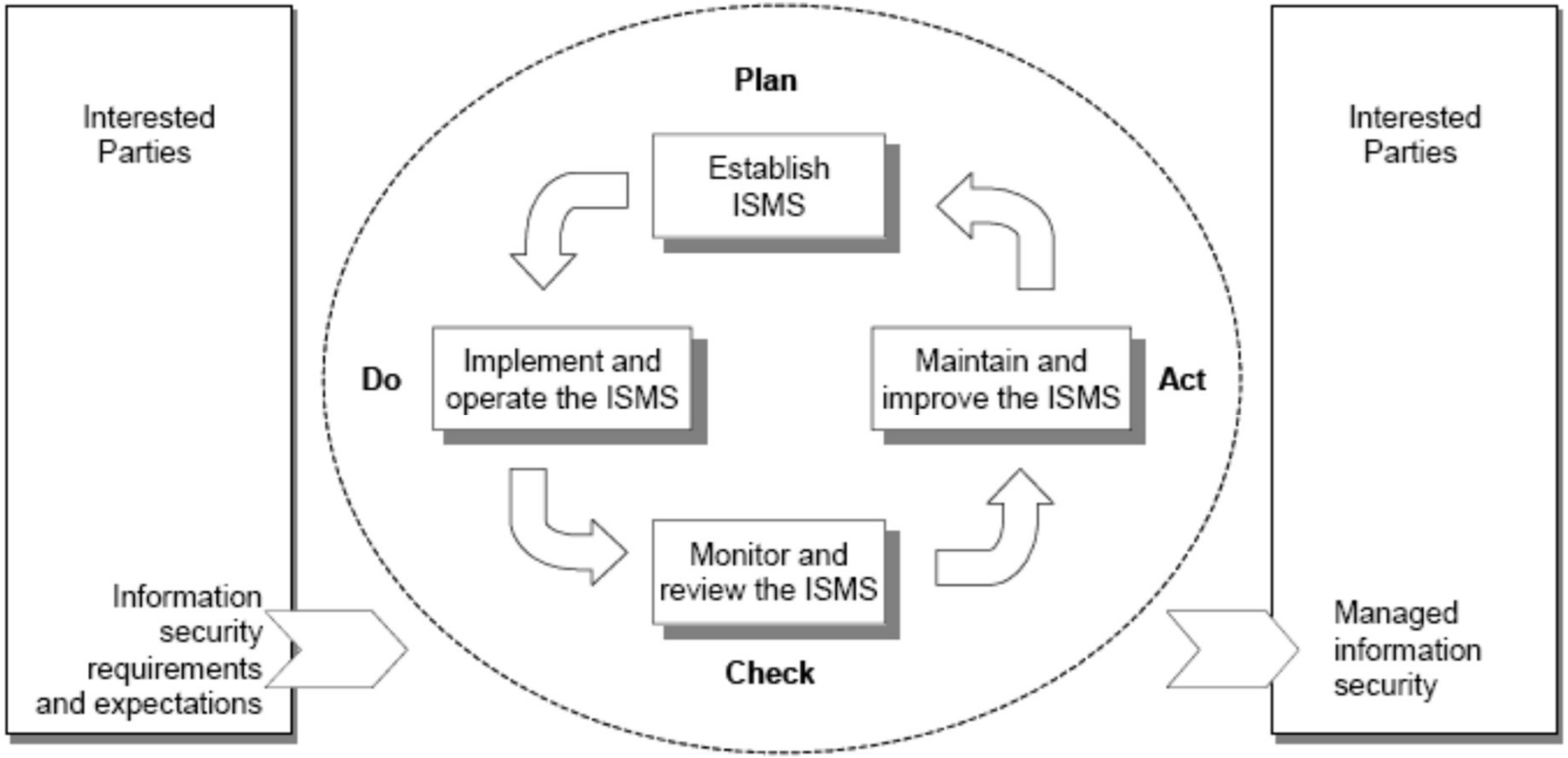
Major Benefits of ISO 27001

- Comply with legal, regulatory & contractual requirements
- Competitive advantage
- Lower losses and costs (cost-effective controls)
- Better growth and profits (customer confidence and reputation)

Information Security Management System

- ISMS preserves information's **confidentiality, integrity and availability (also authenticity, accountability and non-repudiation)**
- applies a **risk management process** and
- gives **confidence to interested parties** that risks are adequately managed

Information Security Management System



Source : ISO

Figure 1 — PDCA model applied to ISMS processes

ISO 27001

- **Standard provides requirements** to establish, implement, maintain and continually improve information security management system

- Adoption of ISMS is **Strategic decision and within organisational context**

- ISMS should **meet organisation's needs, objectives**, security requirements, processes, size and structure.

- Factors affecting ISMS **change over period in time** (re-evaluate)

ISO 27001 : Two parts

- 11 main clauses that are mandatory
  - 0-3 : Intro., Scope, Normative References, Terms & Definitions
  - 4-8 : mandatory requirements of standard
- Annex A with 93 control objectives and controls that are determined by entity using risk management process (4 sections)
  - Organisational controls (A.5)
  - People Controls (A.6)
  - Physical Controls (A.7)
  - Technological Controls (A.8)

Layers of security:

- Perimeter
- End point
- Network
- Operating System
- Application
- Data
- Physical

ISO 27000 family of standards

- These standards help entities stay safe if IT security, cybersecurity and privacy protection are vital
- **ISO/IEC 27001** is the world's best-known standard for information security management systems (ISMS) and their requirements.
- Additional best practice in data protection and cyber resilience are covered by **more than a dozen standards** in the ISO/IEC 27000 family.
  - Eg: 27002 (implementation of controls), 27017 (Privacy like GDPR), 27017 & 27018 (Cloud data security). These supplement ISO 27001 – extra info to implement Annex A controls)
- Together, they enable organizations of all sectors and sizes to manage the security of assets such as financial information, intellectual property, employee data and information entrusted by third parties.

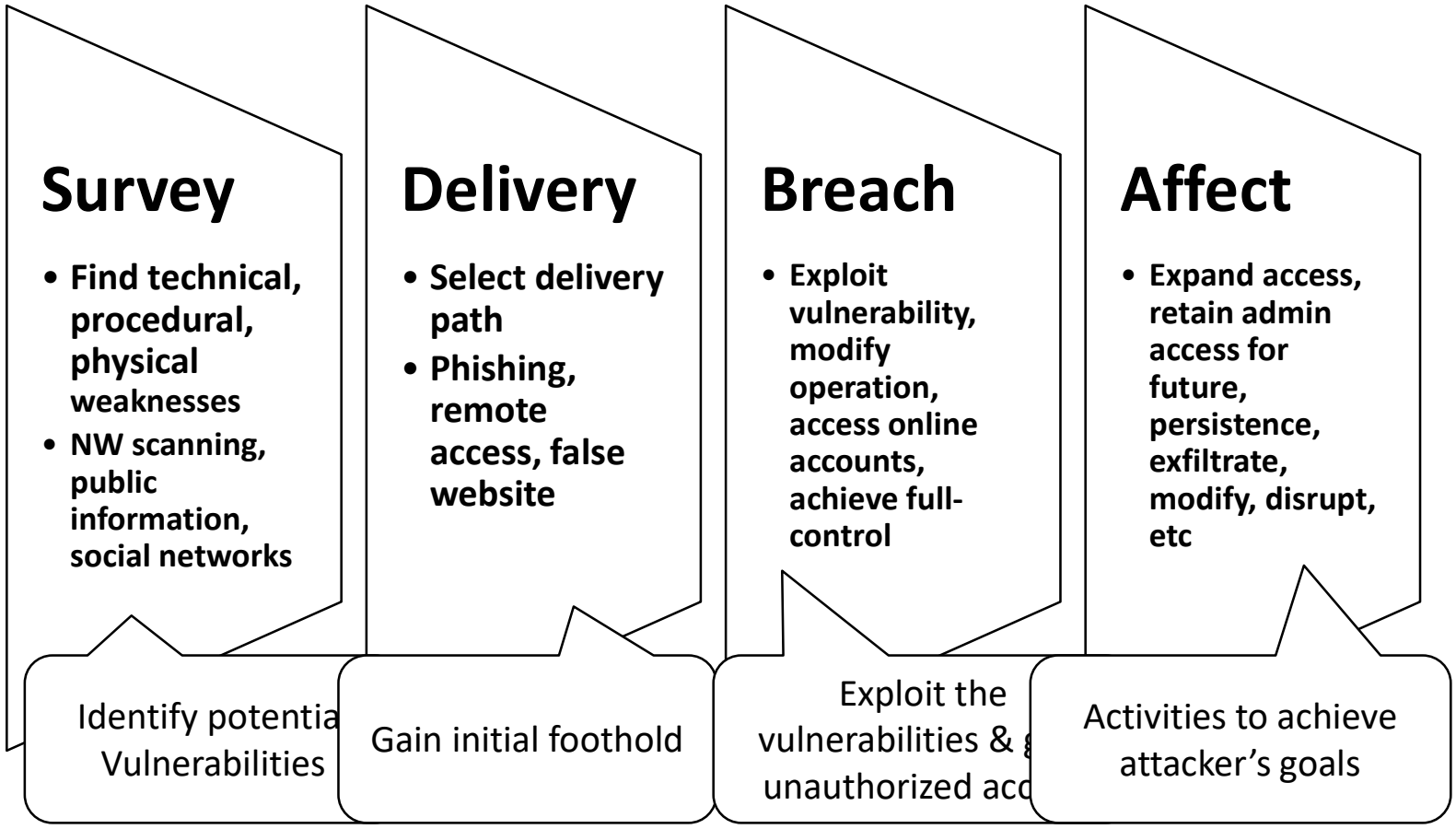
How does ISMS work

- It protects against Confidentiality, Integrity and Availability (also accountability, non-repudiation and authenticity)
  - identify potential incidents
  - find ways to prevent incidents from happening
- It is managing information security risks
  - Risk assessment and treatment
  - Continuous protection using safeguards (implement, maintain, improve)

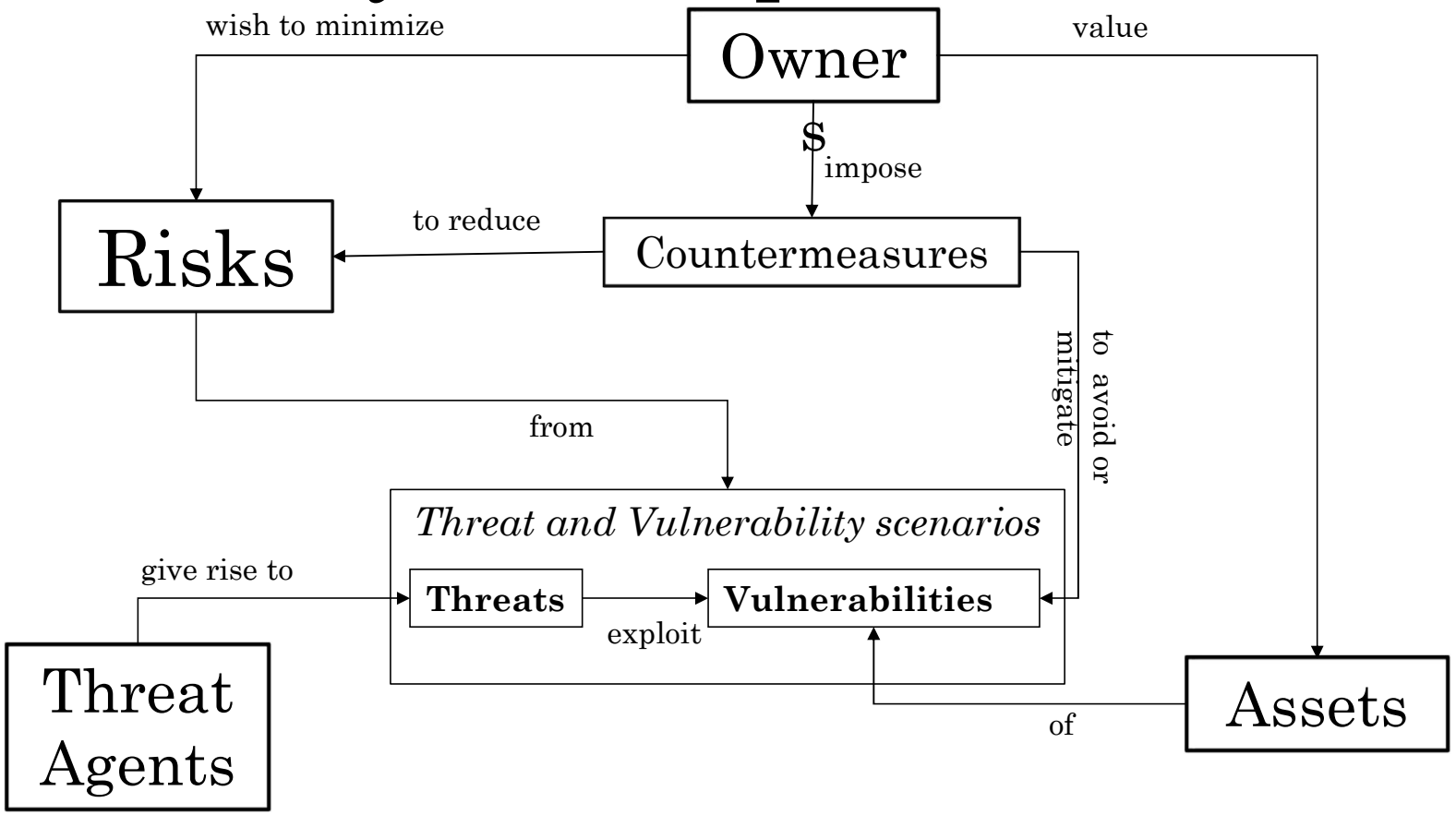
Risk Management Approach (in short)

ISMS Process	Information Security Risk Management Process
Plan	Establishing the context Risk assessment Developing risk treatment plan Risk acceptance
Do	Implementation of risk treatment plan
Check	Continual monitoring and reviewing of risks
Act	Maintain and improve the Information Security Risk Management Process

Stop the attack and minimize impact

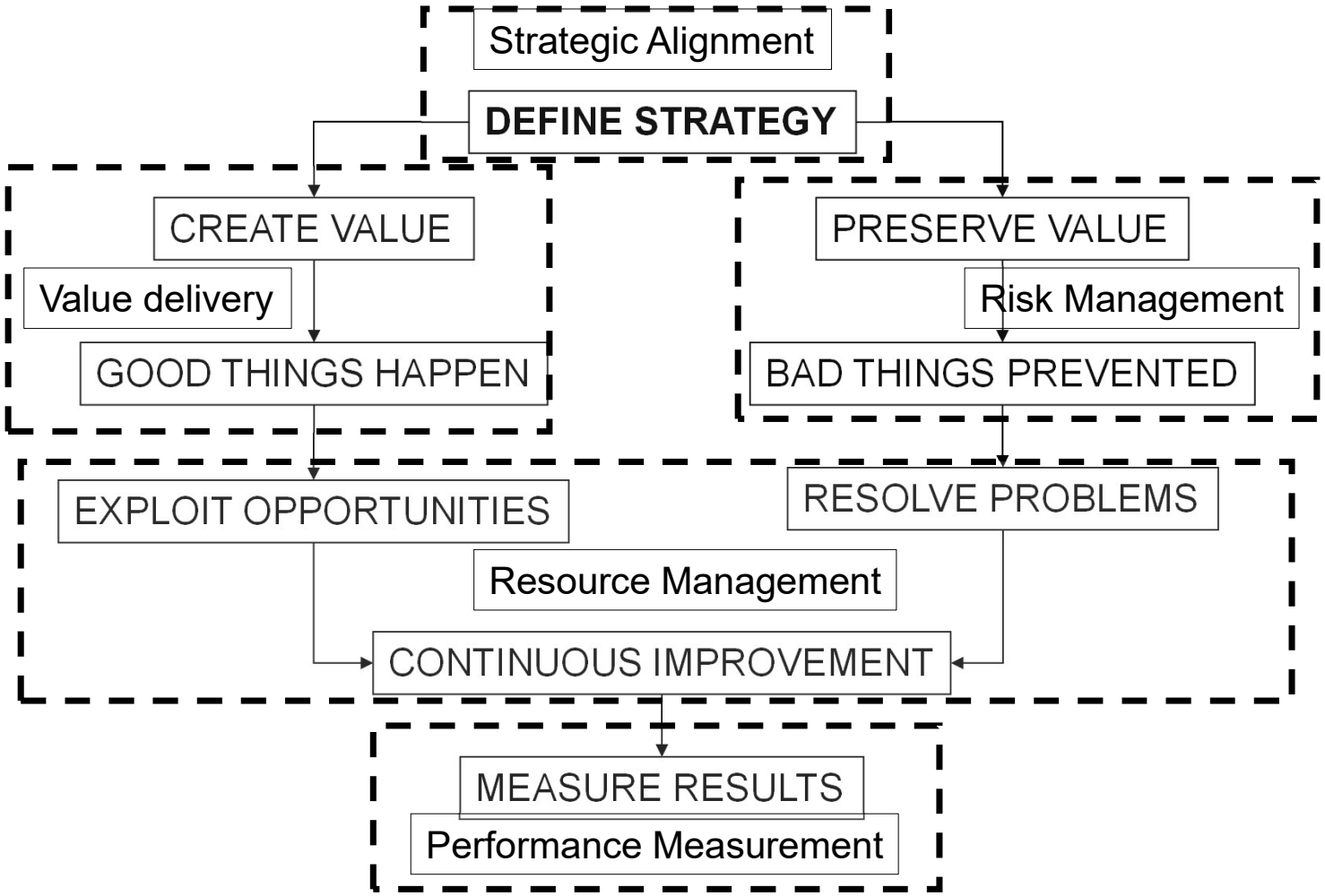


Risk Analysis Components



Source : ISO

Controls help Governance



Structure & content of ISO 27001

- **Context of the organization** (drivers, needs & expectations, scope and ISMS requirements)
- **Leadership** (leadership, commitment, policy, roles, responsibilities and authorities)
- **Planning** (address risks and opportunities, setting & achieving info.-security objectives)
- **Support** (resources, competence, awareness, communication, documentation)
- **Operation** (operational planning and control, info-security risk assessment and treatment
- **Performance evaluation** (monitoring, measurement, analysis, evaluation, internal audit and management review)
- **Improvement** (nonconformity and corrective action, continual improvement)
- Annex A (normative) Reference **control objectives** and controls

Management System - components

Understanding the Entity
- Entity's Context
- Needs & expectation of stakeholders
- Scope of ISMS
- Adoption of ISMS framework

Planning
- Actions to address risks and opportunities
- I-Sec objectives
- Planning to achieve objectives

Support
- Resources
- Competence
- Awareness
- Communication
- Documentation (structure & control)

Leadership
- Leadership & Commitment
- Policy
- Roles, responsibilities & authorities

Operation
- Operational planning & control
- I-Sec risk assessment
- I-Sec risk treatment

Performance Evaluation
- Monitoring, measurement, analysis & evaluation
- Internal Audit
- Management Review

Improvement
- Non-Conformity & corrective action
- Continual improvement

A few Control categories

- I-Sec Policies (Management's Direction)
  - define, approve, publish & communicate
- I-Sec organisation (structure)
  - Internal, external authorities, SoD

- Mobile devices & teleworking
- Human Resource Security
  - before, during and after employment
  - Screening, awareness, disciplinary

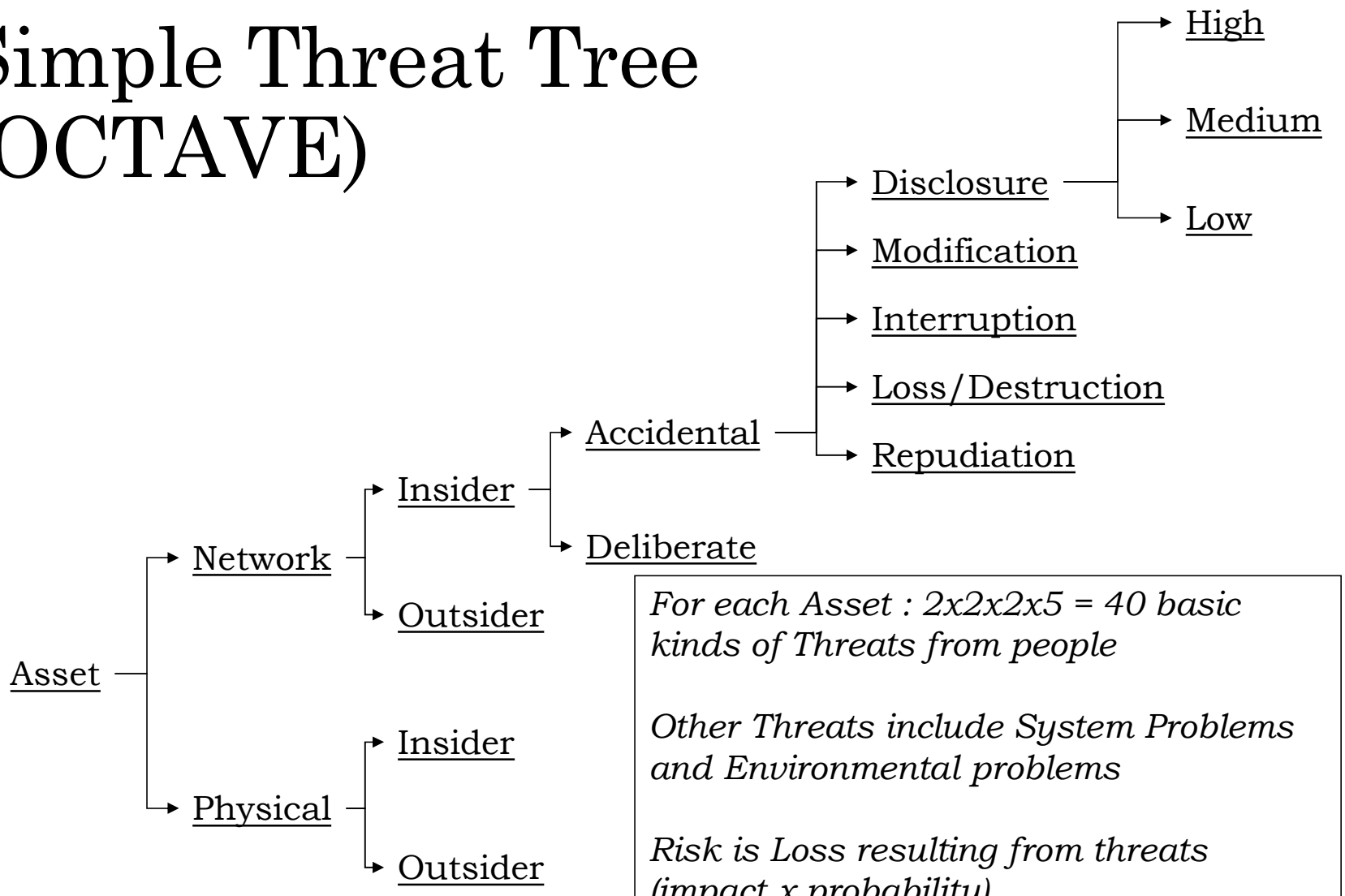
- Asset Management
  - Inventory, ownership of Assets
  - Acceptable use of assets
  - Return of Assets
- Information Classification (severity, sensitivity)
  - Classify, label, handling acc'g classification)

- Access Control
  - Business need to know/do
  - User access management
    - (registration / deregistration
    - Access Provisioning
    - Privileged access rights
    - Review & revision of rights
    - Secure passwords / authentication info.
  - System & application access control

Govt. of India guidelines

- CERT-In guidelines on Cyber Security
- IT Act 2000
- Guidelines on Domain Names
- Guidelines on Web-site Security
- Directions on ISO 27001 compliance
- Advisories and Incident Reporting
- Cert-In guidelines - compliance

Simple Threat Tree (OCTAVE)



For each Asset : 2x2x2x5 = 40 basic kinds of Threats from people

Other Threats include System Problems and Environmental problems

Risk is Loss resulting from threats (impact x probability)

Threat Properties

Threats from People	Outcome	Impact
Threats from System problems	Disclosure Modification loss/destruction Interruption non-repudiation	high, medium, low
Threats from Other problems (beyond org'ns control)		

Information Security Management System - Framework

Why ISMS :

- We have obligations – legal, regulatory and contractual
- Information is of value and is an asset that needs protection.

What is ISMS :

- Managed Services – matching requirements with outcomes – People, process, technology
- Not all Information is equally important – Secrets, Internal, Public
- Properties of Information being protected– Confidentiality, Integrity, Availability, Non-repudiation, Accountability, Assurance
- Risk-based approach to provide cost-effective protection