'Cyber Security'

Need for Proactive & Preventive actions

Savita Utreja, Director

Indian Computer Emergency Response Team (CERT-In)

Ministry of Communications and Information Technology

Government of India

Web: http://www.cert-in.org.in, E-mail: sutreja@mit.gov.in

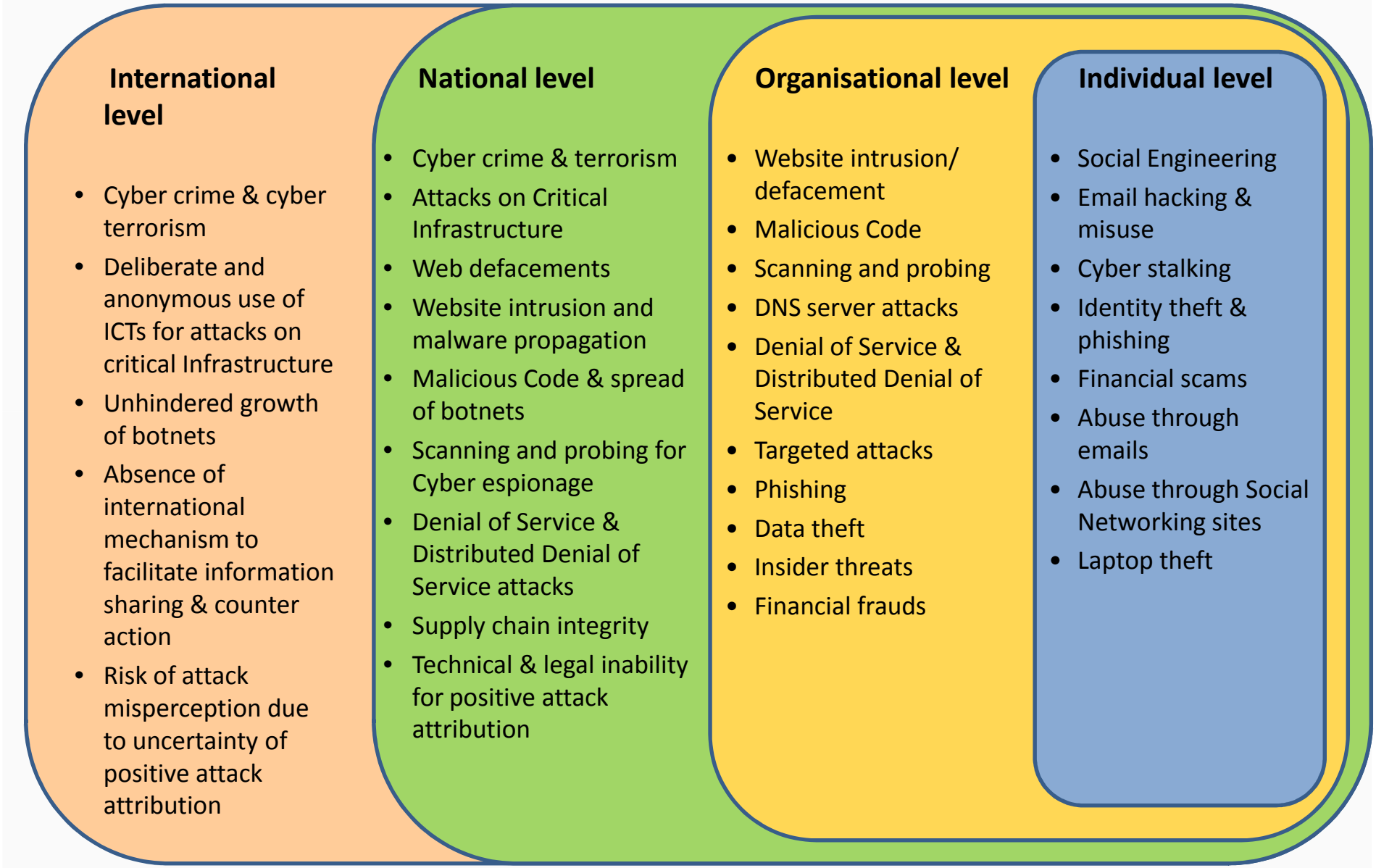
"In security matters, there is nothing like absolute security"

"We are only trying to build comfort levels, because security costs money and lack of it costs much more"

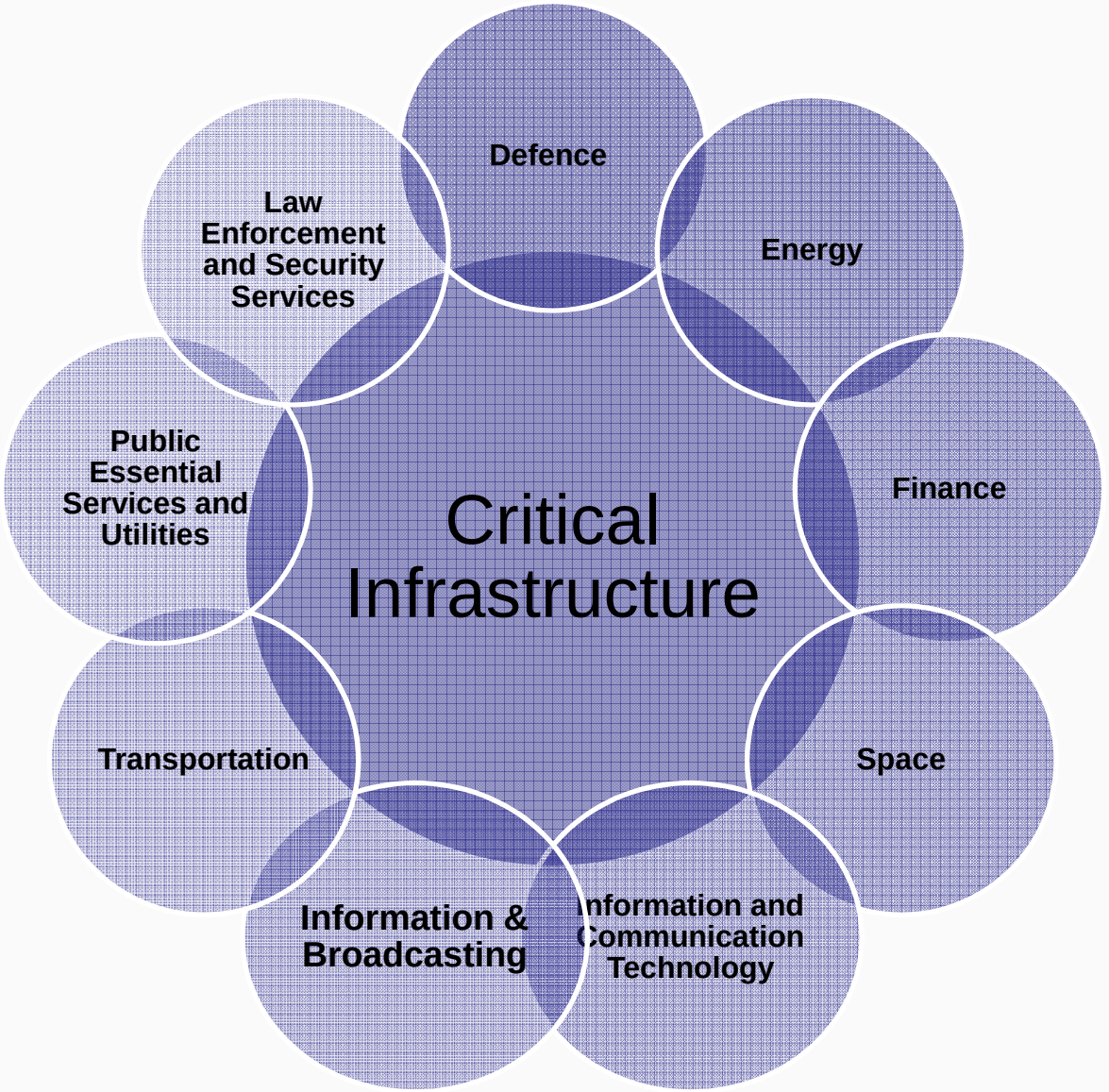
"Comfort level is a manifestation of efforts as well as a realization of their effectiveness & limitations"

With the increase in use of information technology, cyber security has assumed a lot of significance, since IT resources can be target, source as well as means of trouble

Cyber threats and concerns



Targets of cyber attacks



Today's Enterprise – Struggle for balance

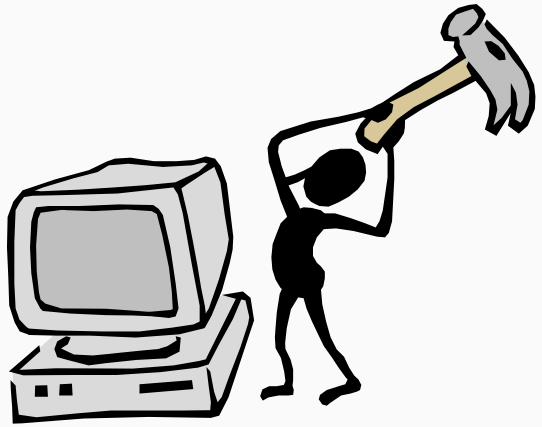
Today, enterprises using IT need to balance four requirements simultaneously

- Sensible investments and reasonable ROI
- Compliance with legal requirements
- Facilitate business with secure access to information and IT resources
- Keep intruders at bay

Cyber Security Assurance - Emphasis

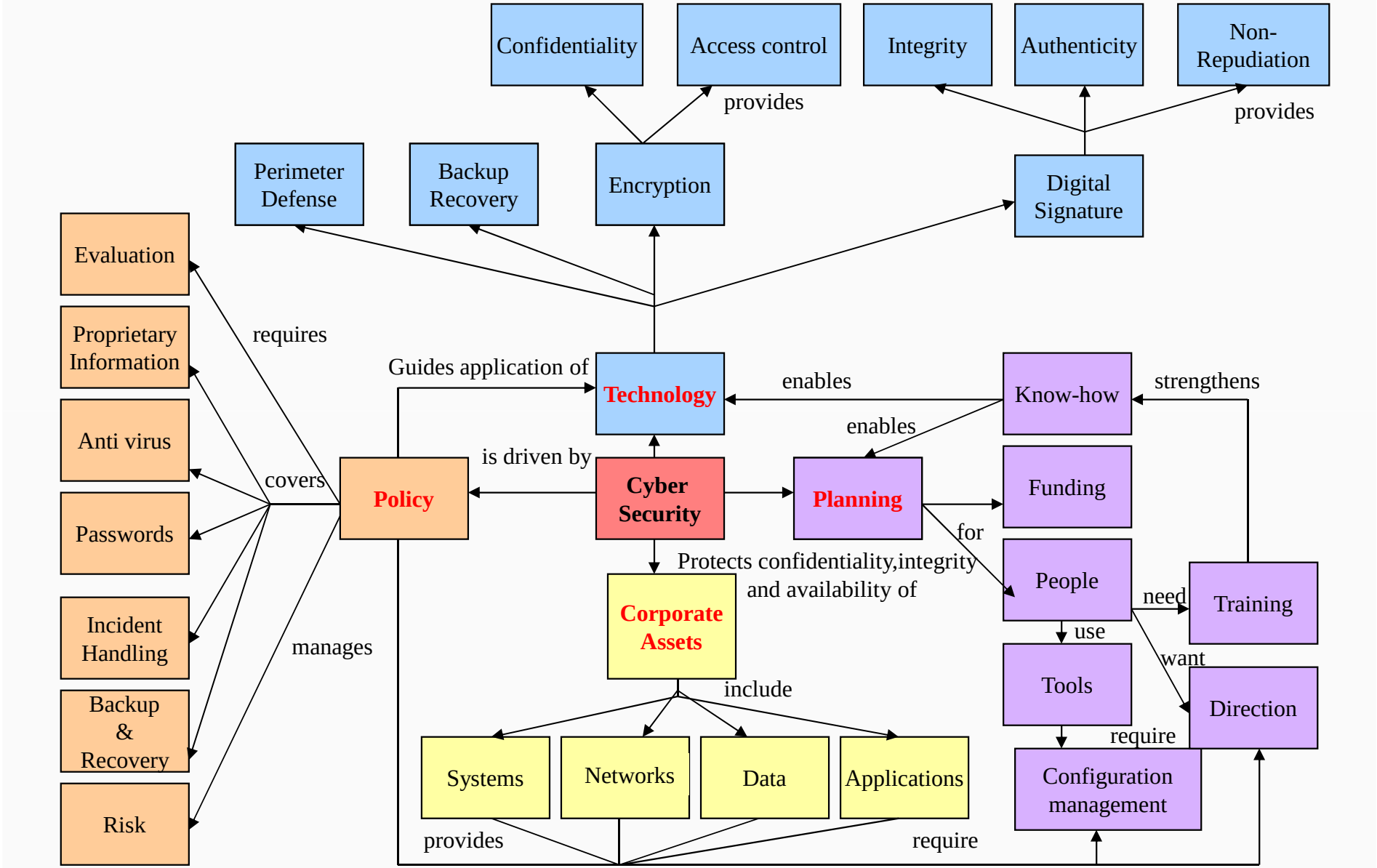
With security assurance, we are not intending to make the system 'hacker proof', but devise a mechanism which can, to a large extent

- Anticipate potential problems
- Pre-empt through proactive measures
- Protect against considerable damages
- Ensure recovery and restoration



'It is all about the ability to expect the expected before we are ready to expect the unexpected'

Cyber Security Assurance - Focus



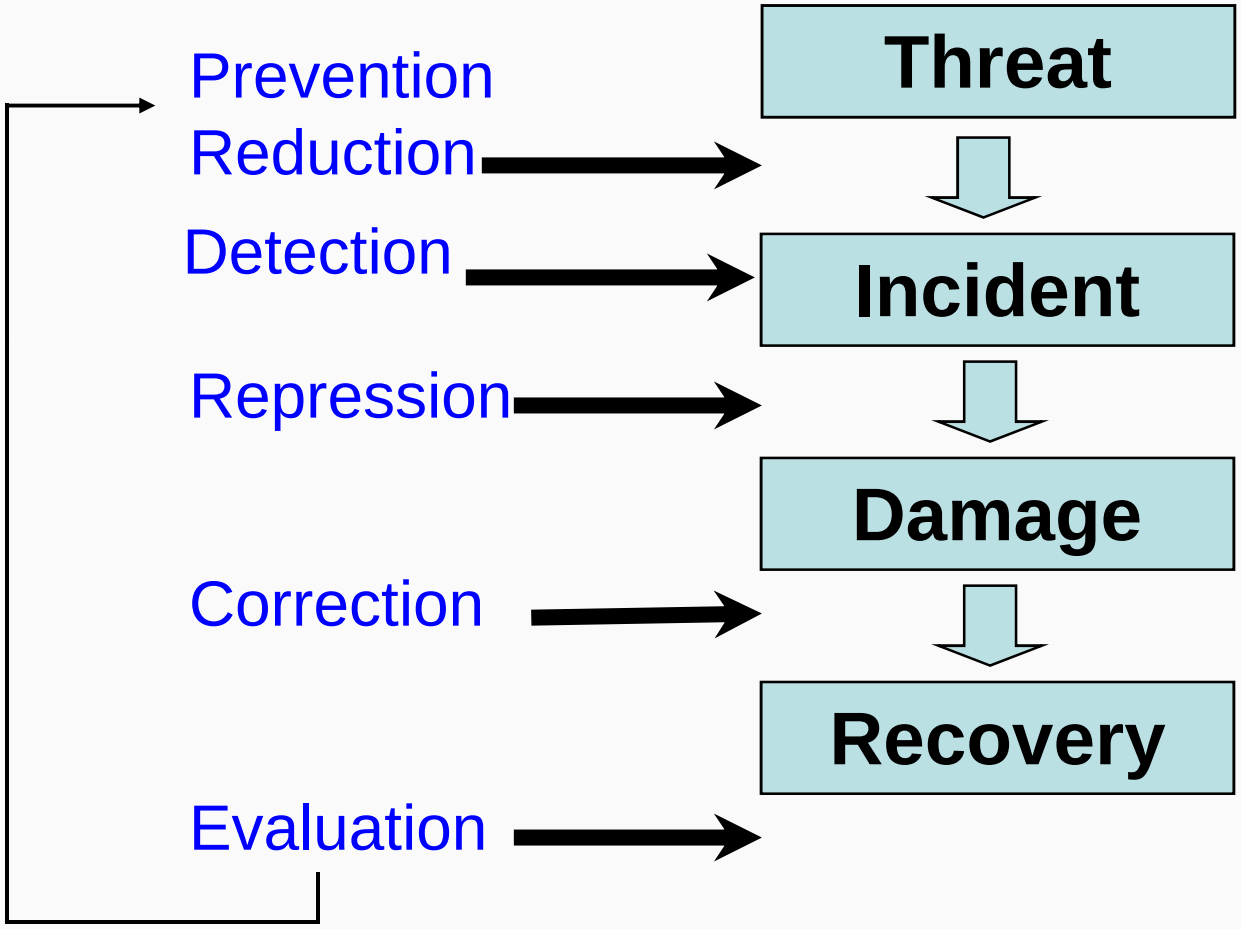
Security Assurance Ladder

Security assurance emphasis depends on the kind of environment

- Low risk : ***'Awareness'*** *– know your security concerns and follow best practices*
- Medium risk*:* ***'Awareness & Action'*** *– Proactive strategies leave you better prepared to handle security threats and incidents*
- High risk*:* ***'Awareness, Action and Assurance'*** *– Since security failures could be disastrous and may lead to unaffordable consequences, assurance (basis of trust & confidence) that the security controls work when needed most is essential.*

Security Assurance - Outcome

Effective Security Management – Control, Continuity & Repetitiveness



What is the need of today

- To constantly protect the critical information systems from vulnerabilities, external and internal threats.

- To follow Information Security Management practices which involves balancing security best practices with proper management and oversight.

Standards, Compliance & Assurance

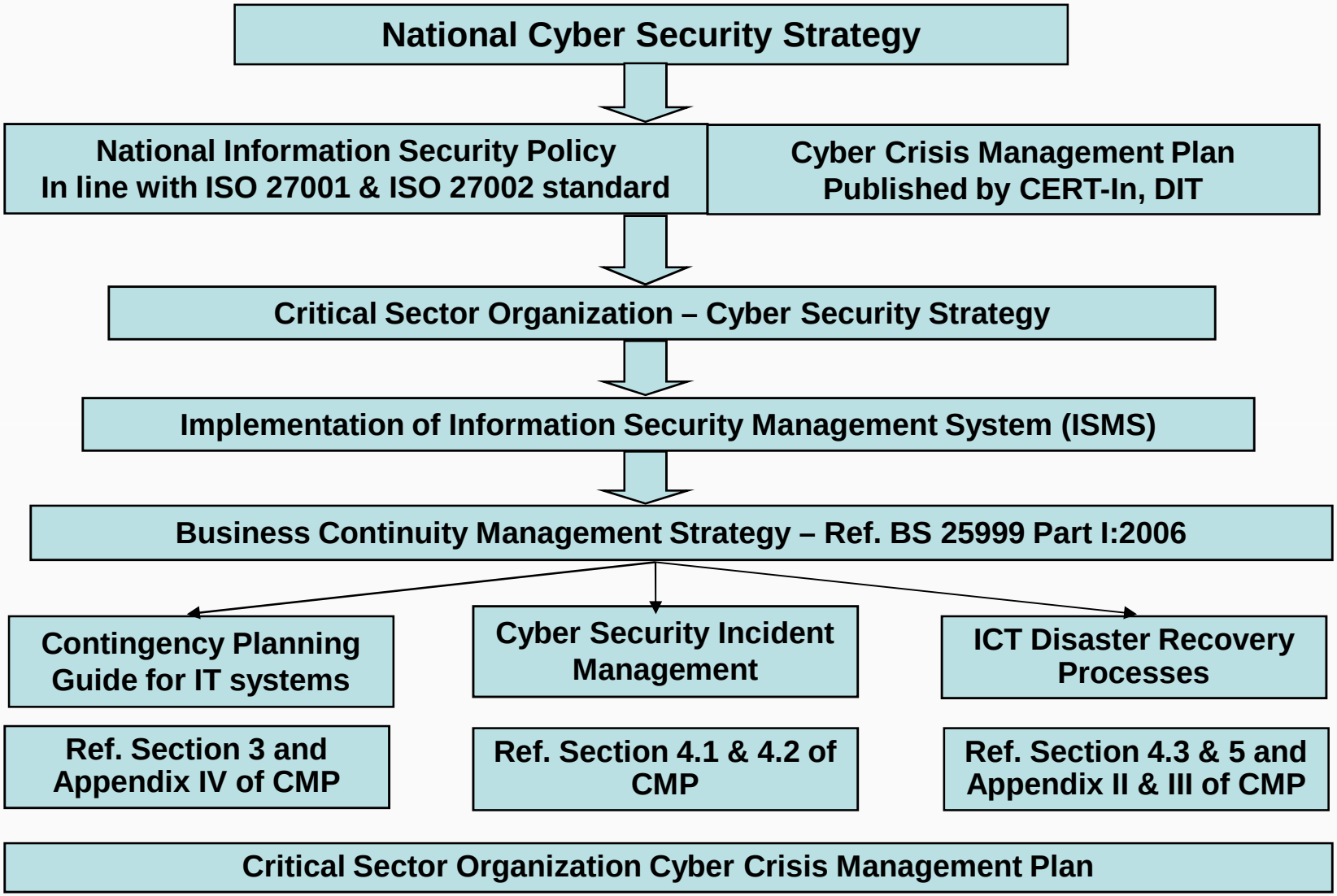
for effective

Crisis Management

Cyber Security Assurance Framework

- Security assurance plan - Information security management best practices as per international standard have been mandated for compliance within Govt. and critical sectors. Following enabling actions have been taken to assist compliance efforts, covering process, product, system and people:
  - ISMS certification scheme as per ISO 27001 standard
  - Tool for assisting ISMS implementation and self-assessments
  - Security test/evaluation facility for test and evaluation IT products as per ISO 15408 Common criteria standard
  - Empanelment of IT security auditing organisations for IT infrastructure audits for Govt and critical sectors
  - IT security skill specific training courses for people
  - Guidelines for infrastructure security, user-end equipment security and information security

Crisis Management Plan-Compliance Framework



Cyber security enabling assistance

Specific assistance in Cyber Security Crisis Management and Emergency Response by CERT-In

- Development and implementation of sectoral crisis management plan (CMP) in line with National crisis management plan (CMP) of CERT-In.
- Remote profiling of IT systems and Networks to determine the security posture.
- Cyber Security drills to enable the organizations to assess their preparedness to resist cyber attacks and enable timely detection, response, mitigation and recovery actions in the event of cyber attacks.

Sectoral CMP – Points for action

- Identify a member of senior management as a 'Point of Contact' to coordinate security policy compliance efforts across the sector and interact regularly with CERT-In.
- Establish a Sectoral Crisis Management Committee, on the lines of National Crisis Management Committee, with Secretary *(in case of Central Ministries/Depts)* or Chief Secretary *(in case of Sates/UTs)* as its Chairman and a 24x7 control room to monitor crisis situations .
- Prepare a list of organisational units that fall under the purview of sectoral CMP and provide them with a list of action points for compliance.
- Direct the organisational units to identify and designate a member of senior management as 'Chief Information Security Officer (CISO)'.
- Prepare a list of CISOs complete with up-to-date contact details .
- Prepare a sectoral CMP on the lines of CMP of CERT-In, outlining roles, responsibilities of sectoral stakeholders, CMP coordination process.
- Direct the organisational units to develop and implement their own CMP on the lines of CMP of CERT-In, including security best practices as per ISO 27001 and report compliance on a periodic basis.

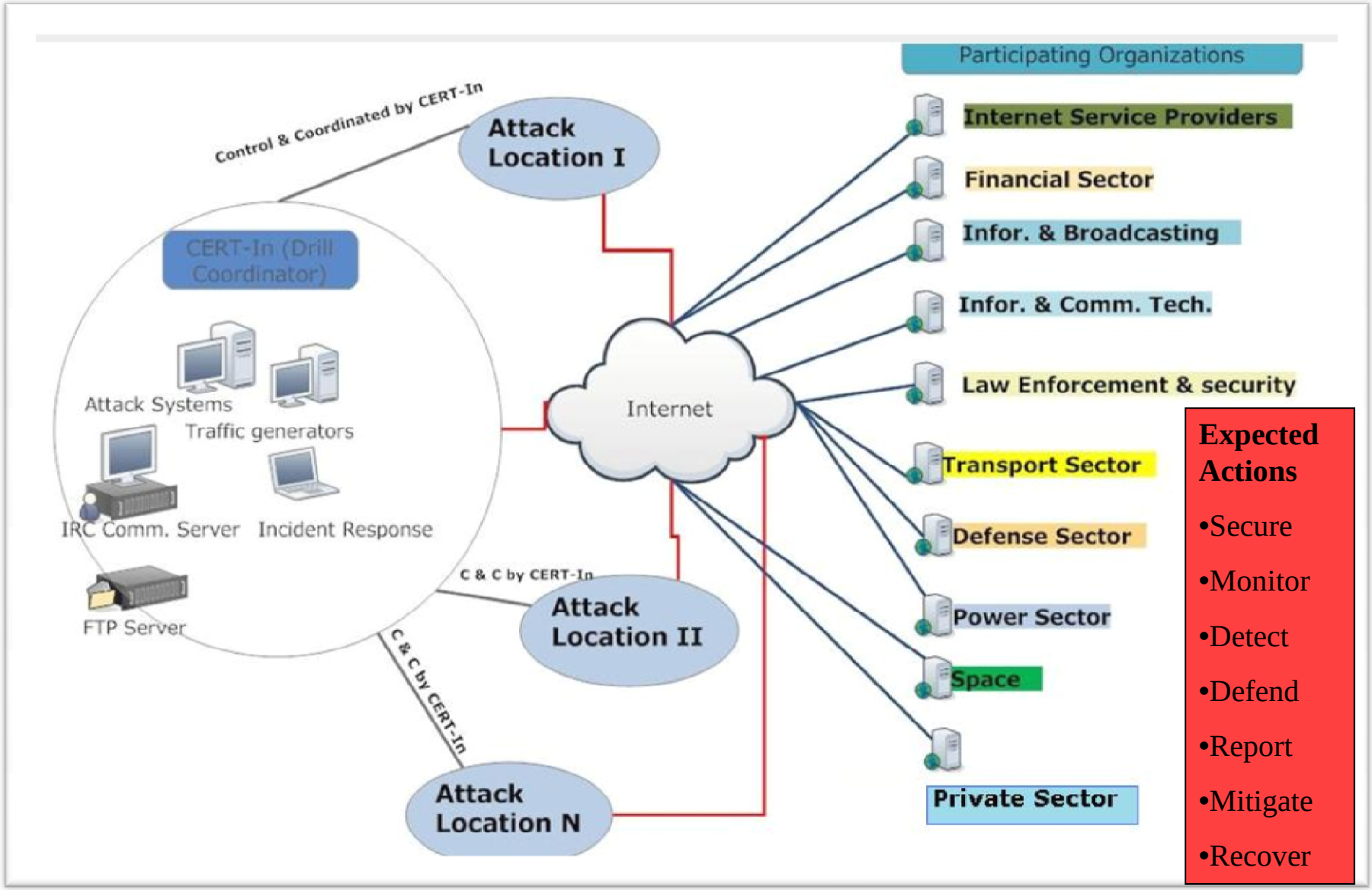
Organisation level CMP – Points for action

- Identify a member of senior management as a 'Chief Information Security Officer (CISO)' to coordinate security policy compliance efforts across the organisation and interact regularly with CERT-In and sectoral 'Point of Contact'
- Establish a Crisis Management Group, on the lines of Sectoral Crisis Management Committee, with head of organisation as its Chairman
- Prepare a list of contact persons complete with up-to-date contact details
- Prepare an Organisational level CMP on the lines of CMP of CERT-In, outlining roles, responsibilities of organisational stakeholders, CMP coordination process
- Implement the CMP, including security best practices and specific action points as outlined below:
    - Prepare a Security plan and implement Security control measures as per ISO 27001 and other guidelines/standards as appropriate
    - Carry out periodic IT security risk assessments and determine acceptable level of risks, consistent with business impact assessment and criticality of business functions

Organisation level CMP – Points for action

- Develop and implement a business continuity strategy and contingency plan for IT systems
- Develop and implement ICT disaster recovery and security incident management processes
- Periodically test and evaluate the adequacy and effectiveness of technical security control measures, especially after each significant change to the IT applications/systems/networks and it can include:
    - Penetration testing *(both announced and unannounced)*
    - Vulnerability assessment
    - Application security testing
    - Web security testing
- Carry out audit of information infrastructure on an annual basis and when there is a major upgradation/change in IT infrastructure, by an independent IT security auditing organisation *(Ref. to list of CERT-In empanelled IT security auditors on CERT-In web site at http://www.cert-in.org.in)*
- Report to CERT-In cyber security incidents as and when they occur and status of cyber security periodically and take part in cyber security mock drills

Cyber Security Drills



Cyber security enabling assistance

Organisations can help CERT-In in securing the cyber space by:

- Duly reporting security incidents and sharing all relevant information that can support real-time incident analysis & rapid response
- Collaborating with CERT-In to keep a watch on cyber space to look for malicious traffic, virus/worm infections and visible signs of build-up or emergence DDoS attacks
- Regularly participating in CERT-In trainings/workshops on contemporary topics/issues to remain updated on technology and security best practices

Compliance assurance efforts and assurance

Compliance assurance efforts involve layers of actions such as

- In view of the growing cyber threats to the organisation's assets, it is essential for an organisation to ensure legal compliance to the security best practices and guidelines.
- Self-assessment by user organisations with the help of tools developed for self-assessment.
- Develop a continuous programme to monitor compliance with internal policies and procedures and compliance with the codes of practice and guidance published externally.
- Second party audits by customer entities
- Third party audits conducted by CERT-In empanelled auditors on a commercial basis on Government & organisations in critical sectors

CERT-In

&

Other Security guidelines

CERT-In Security Guidelines

Some of the guidelines published by CERT-In are as follows:

- Security Guidelines for Web Servers: Provides step by step approach for securely designing, implementing and operating Web servers, including related network infrastructure issues.

- Security Guidelines for Database Servers: States procedures and regulations needed to maintain a desired level of Database Server security in terms of server security, database connections, table access control and restricting database access.

- Security Guidelines for Intrusion Detection System: States procedures for deployment of secure IDS for specific system & network environments and managing its output.

- Security Guidelines for emails: Provides recommendations to be followed by a user for using email in a secure way.

CERT-In Security Guidelines (contd…)

- Security Guidelines for credit cards: Provides safety measures for credit card users to safely make the transactions in order to minimize the risk and save them from financial frauds.
- Security Guidelines for Router: Provides guidelines for the security of routers at perimeter and internal network level.
- Security Guidelines for Standalone systems, networked systems and home computers
- IT Security policies for Government and critical sector organisations: Suggests the framework to provide the basis for an organization to develop its own IT Security Policy.

The detailed security guidelines documents are available at the CERT-In site:

http://www.cert-in.org.in/ -> KnowledgeBase-> Guidelines

Other Security Guidelines

- Ministry of Home Affairs reviews the overall preparedness of respective Ministries and critical sector organizations under these Ministries with respect to physical security and crisis management.

- Intelligence Bureau issues overall guidelines to Ministries and critical sectors in respect of security matters in general. IB sensitizes the administrative departments and critical sector organizations on latest threats and issues security guidelines from time to time to secure IT and physical infrastructure.

- DeitY has ciculated Cyber Security policies for Government of India along with Standard Operating Procedures (SoPs) for the networks/systems handling unclassified information. These policies aim at providing secure and acceptable use of the cyber resources.

Other Security Guidelines

Some of the guidelines published by NIC are as follows:

- Guidelines for Indian Government Websites : It recommends policies and guidelines for Indian Govt. Websites and portals, at any organizational level, for making Indian Govt. websites citizen centric and visitor friendly. (http://darpg.nic.in/darpgwebsite_cms/Document/file/Guidelines_for_Government_websites.pdf)

- Secure Programming Guidelines: It is aimed towards presenting secure programming guidelines for web site and application developers. (http://www.mp.nic.in/SecureProgrammingGuidelines.pdf)

Reference Standards & Guidelines

In addition to CMP of CERT-In, the following docs can be referred:

- Information security management system standard - ISO 27001:2005
- Information security management system guideline – ISO 27002:2005
- Security risk assessment – ISO 27005:2008
- Business continuity management strategy – BS 25999-1:2006
- Contingency planning guide for IT systems – NIST SP 800-34
- ICT Disaster recovery process standard – ISO 24762:2008
- Security incident management process – ISO/IEC TR 18044
- ISMS security policy and procedures manual template
- Business impact analysis template
- Contingency planning template
- ISMS ISO 27001 self-assessment tool (Excel based)
- 20 most important security controls and metrics for effective cyber security and continuous security policy compliance (Prioritizing security baselines)
- SANS top 20 security vulnerabilities

“We want you Safe”

Thank you