Information Security Management

GESTS 483 - 2017

Brussels, 30 March 2017

Copy of this document is distributed to students

Speaker

OPDEBEECK Jean-sébastien

- Owner of http://www.vulpoint.be
- Twitter: @k4l4m4r1s
- CISO, DPO, Hacker, …
- Certified CISM, CISSP, CEH, ISO 2700x implementer

Working at

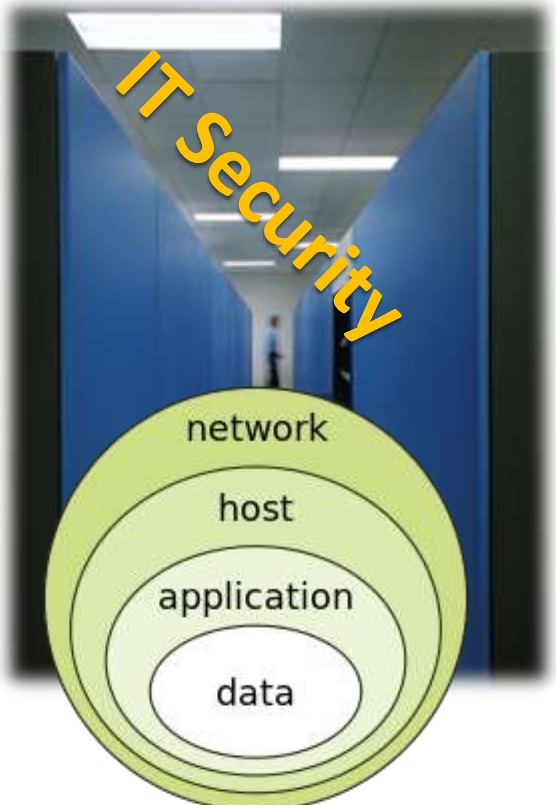
ICTC.eu - http://www.ictcontrol.eu/

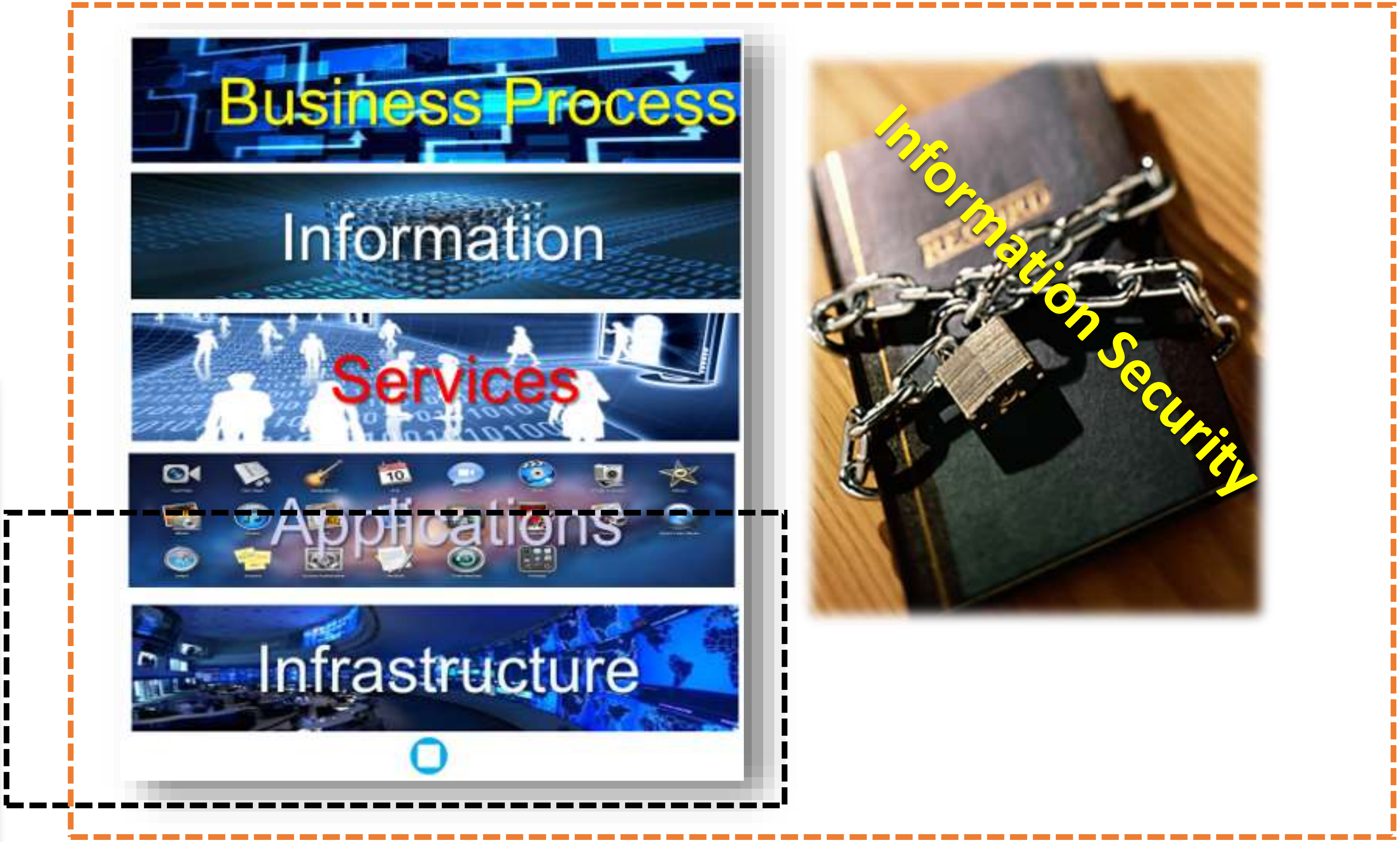
ICT CONTROL

Your Trusted Advisor

What is Information Security ?

Aspects


IT Security
network
host
application
data


Business Process
Information
Services
Applications
Infrastructure
Information Security

Major Focus

Information is:

- handled,
- processed,
- transported,
- stored.

Reach:

- integration,
- process assurance,
- overall security,
- overall privacy.

Universe of :

- risks,
- benefits,
- processes.

new generation of IT m
Master in ICT Audit & Securit
Join the Security year... and
Executive Programme in Info

Chief **Information Security** Officer

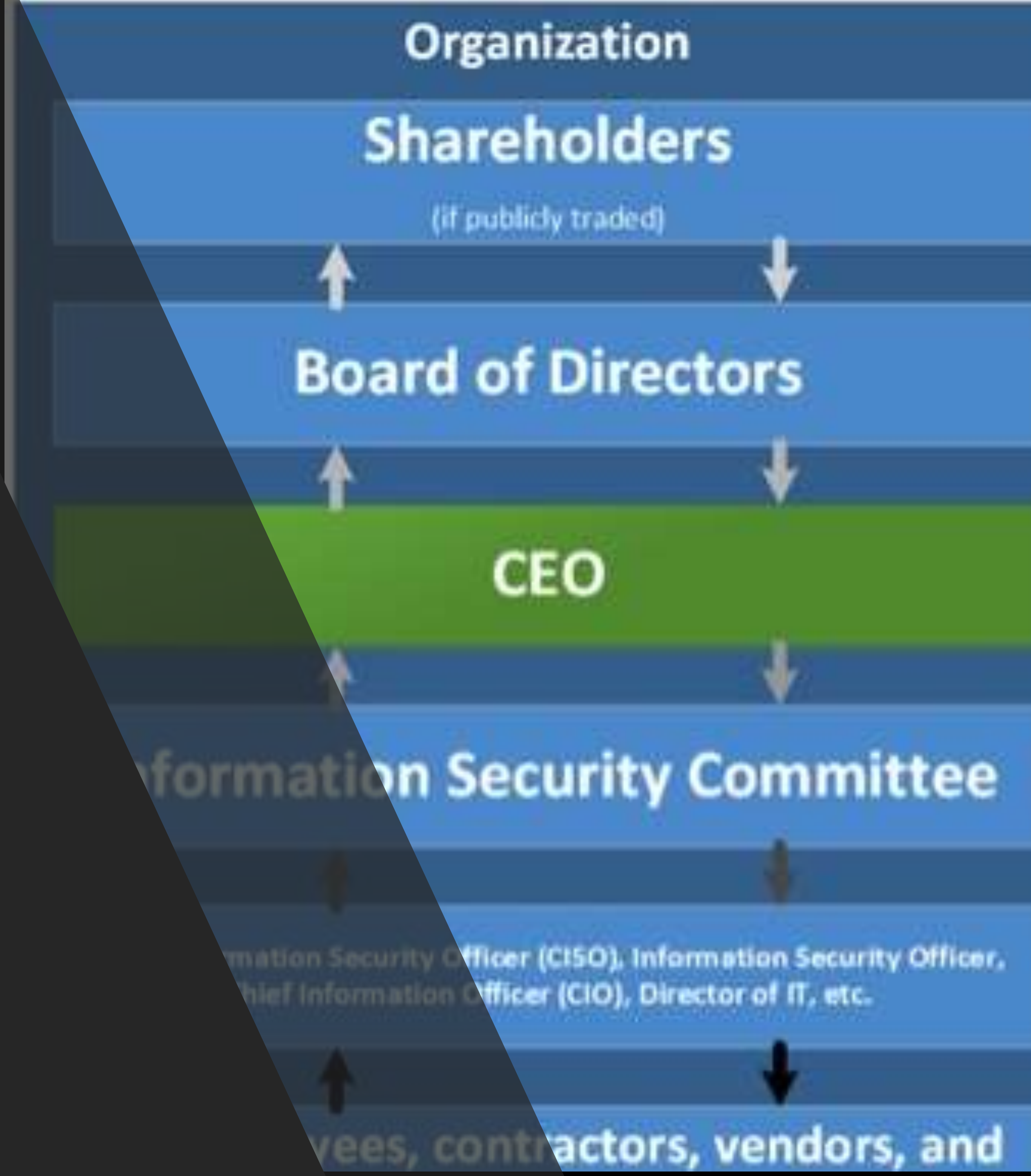
Main topics of today:

- **Information Security Governance**
- **Information Risk Management & Compliance**
- **Information Security Program Development & Management**
- **Information Security Incident Management**

Photo from www.tomsitpro.com

IS Governance

“It is because you have breaks on your car, …
… you can drive faster.”


Organization
Shareholders
(if publicly traded)
Board of Directors
CEO
formation Security Committee
mation Security Officer (CISO), Information Security Officer,
hief Information Officer (CIO), Director of IT, etc.
yees, contractors, vendors, and

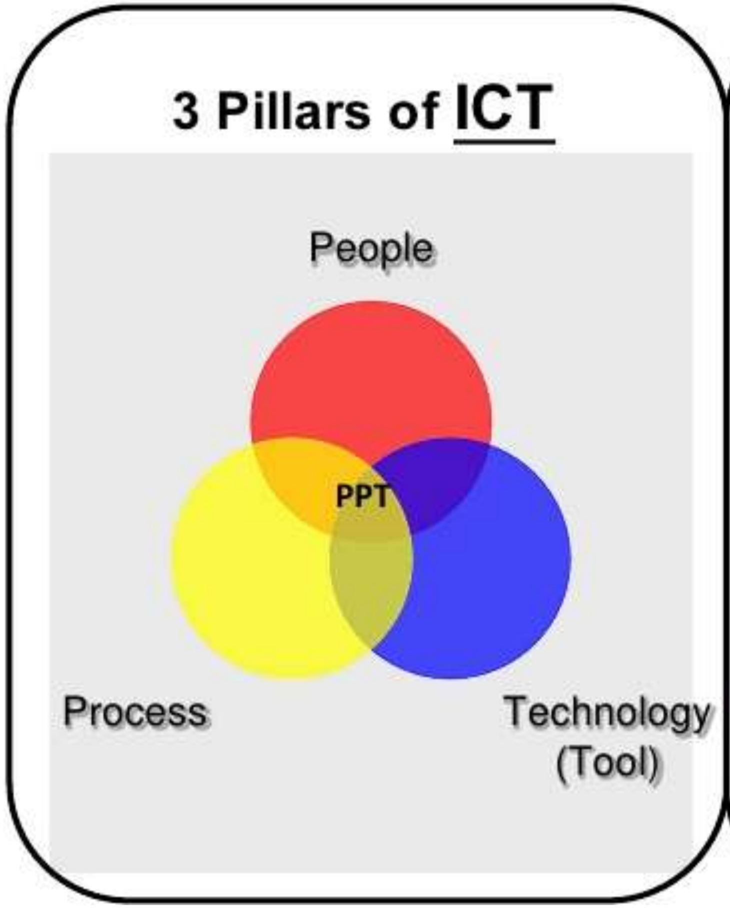
CIA … and Friends

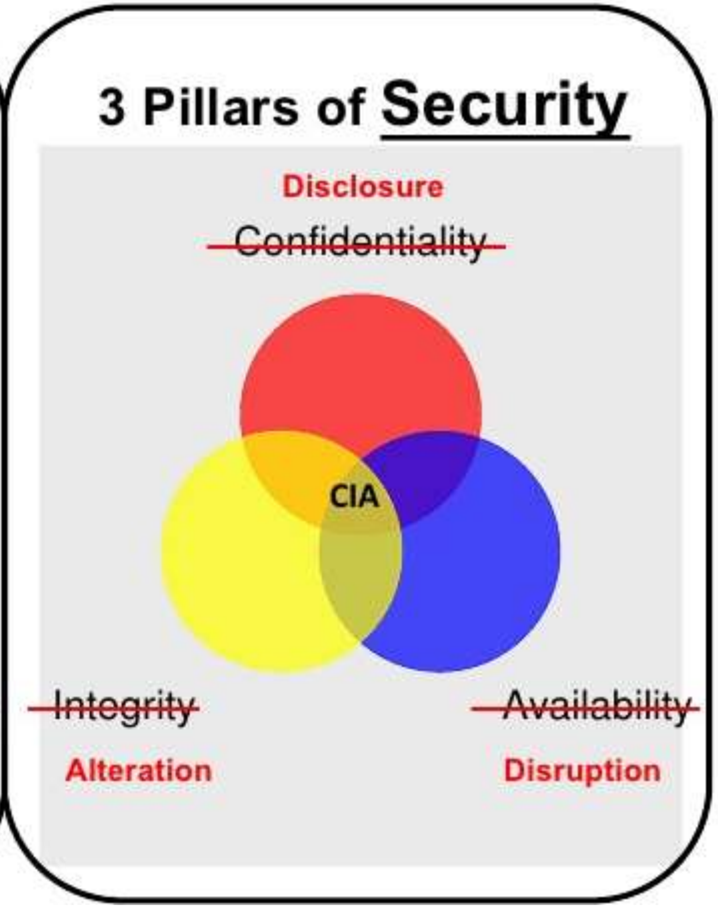
C. Confidentiality.
I. Integrity.
A. Availability.

P. Privacy

N. Non-repudiation.
A. Authentication.

Accountable
Trust
Compliance





Benefits

Protection for legal liability

Increased predictability

Policy and compliance

Optimise resources

Risk management,

Process improvement,

Rapid incident response

Reduced losses

Improved reputation

Information and related information systems must be categorised on the basis of their security needs, i.e. levels of confidentiality, integrity and availability, using a systematic process based on their value to the Commission, criticality and sensitivity. *.

Reference: ISO 27002
(Good Practices)

* *IMPLEMENTING RULES FOR COMMISSION DECISION C(2006) 3602 of 16.8.2006*

Boston Consulting Group estimated that by 2016 the cyber-related economy will reach US $4.2 trillion in the G20 economies.

Globally, the estimated reported average financial loss from cybersecurity incidents was $2.7 million*

** PWC survey 2015*

Cyber Security in Belgium

751,000 hacked computers*

614 notifications of hacking

Belgacom / Proximus

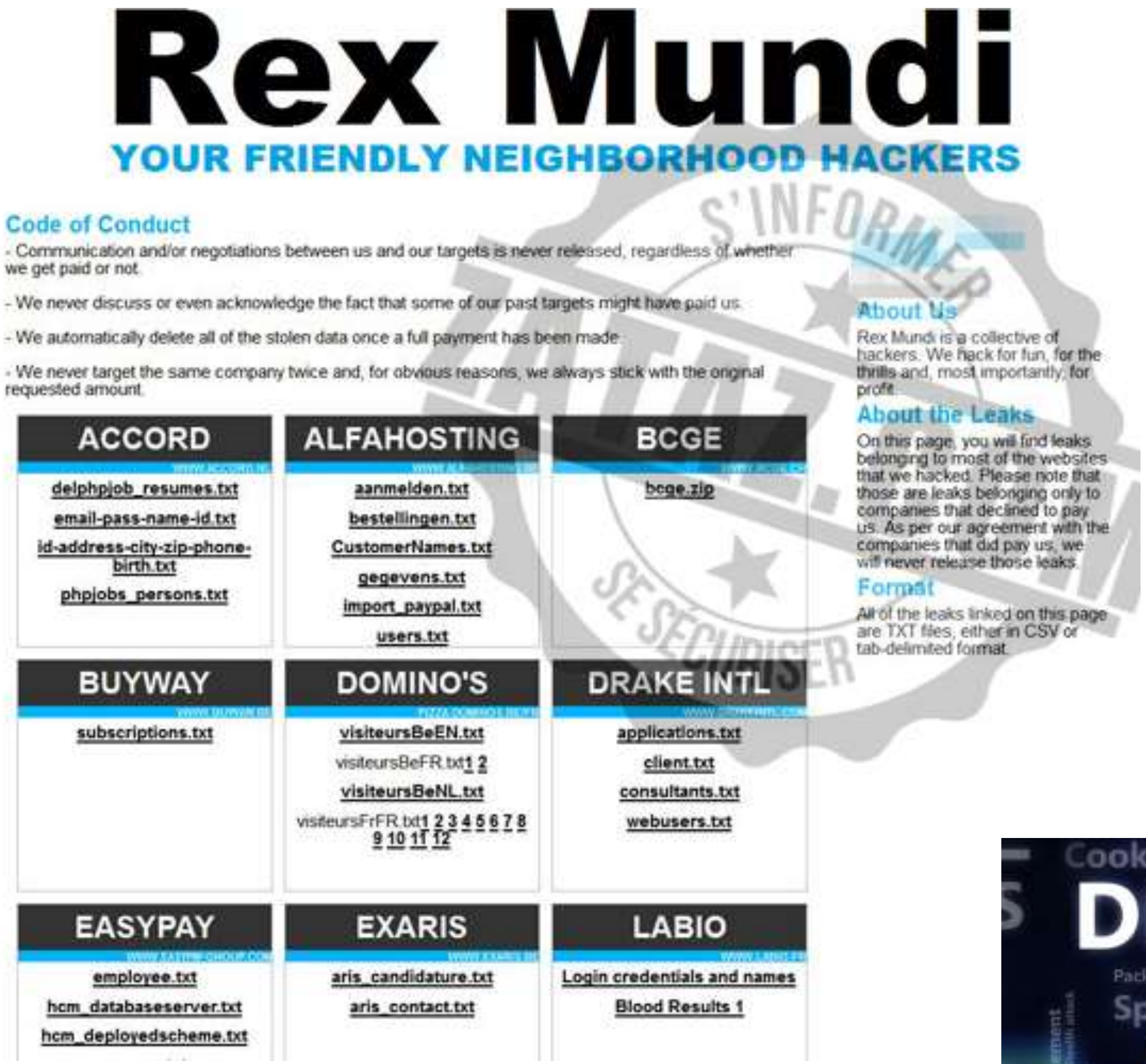
SNCB

…

From VBO study, companies :

- Do not know how to handle efficiently a cyber attack
- Are confused on cyber regulations and authorities

*Source : Cert.be



Rex Mundi

YOUR FRIENDLY NEIGHBORHOOD HACKERS

Code of Conduct

- Communication and/or negotiations between us and our targets is never released, regardless of whether we get paid or not

- We never discuss or even acknowledge the fact that some of our past targets might have paid us

- We automatically delete all of the stolen data once a full payment has been made

- We never target the same company twice and, for obvious reasons, we always stick with the original requested amount

ACCORD

delphpjob_resumes.txt
email-pass-name-id.txt
id-address-city-zip-phone-birth.txt
phpjobs_persons.txt

ALFAHOSTING

aanmelden.txt
bestellingen.txt
CustomerNames.txt
gegevens.txt
import_paypal.txt
users.txt

BCGE

bcge.zip

BUYWAY

subscriptions.txt

DOMINO'S

visiteursBeEN.txt
visiteursBeFR.txt1 2
visiteursBeNL.txt
visiteursFrFR.txt1 2 3 4 5 6 7 8 9 10 11 12

DRAKE INTL

applications.txt
client.txt
consultants.txt
webusers.txt

EASYPAY

employee.txt
hcm_databaseserver.txt
hcm_deployedscheme.txt

EXARIS

aris_candidature.txt
aris_contact.txt

LABIO

Login credentials and names
Blood Results 1

About Us

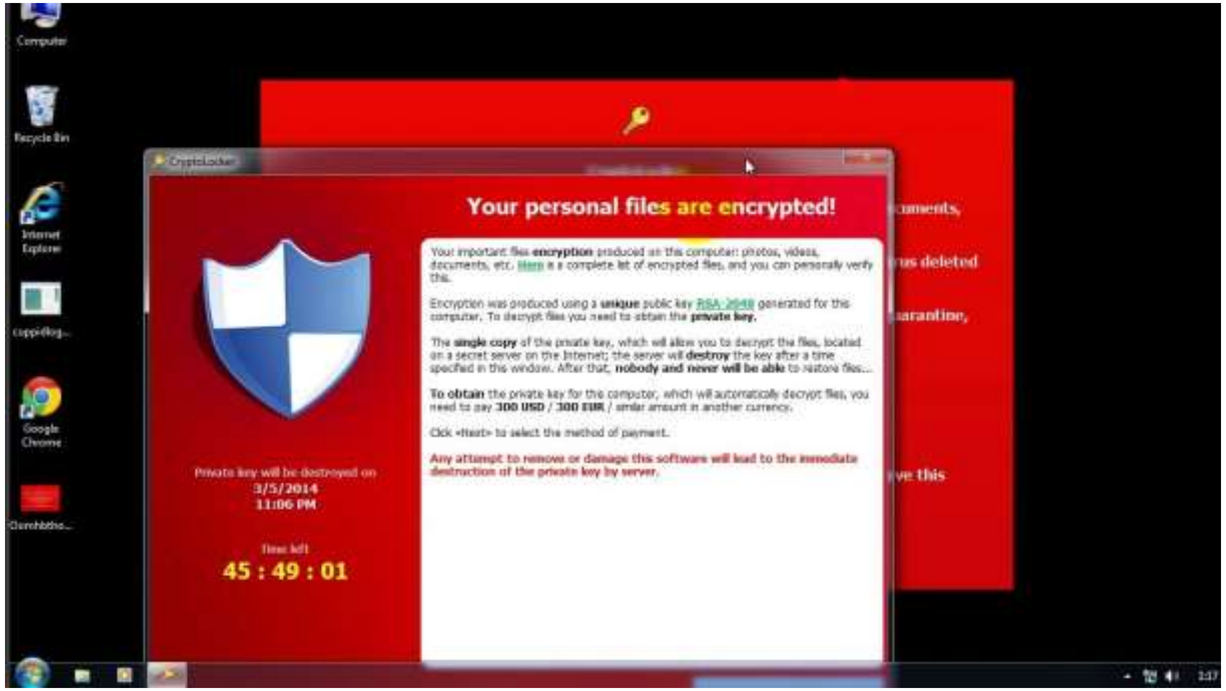
Rex Mundi is a collective of hackers. We hack for fun, for the thrills and, most importantly, for profit.

About the Leaks

On this page, you will find leaks belonging to most of the websites that we hacked. Please note that those are leaks belonging only to companies that declined to pay us. As per our agreement with the companies that did pay us, we will never release those leaks.

Format

All of the leaks linked on this page are TXT files, either in CSV or tab-delimited format.



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
3/5/2014
11:06 PM

Time left
45 : 49 : 01

Implementing adequate Information Security Management

Resources 😉

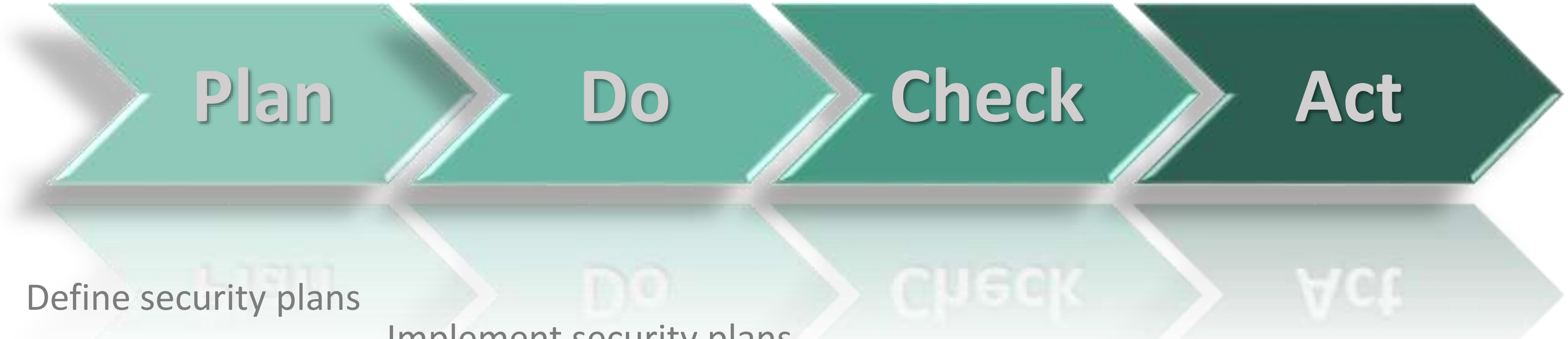
- Policies
- Standards
- Processes
- Methods
- Controls
- Technologies
- People
- Skills
- Training
- Education
- Organizational support and
- Assurance providers

Constraints 😢

- Resources
- Law
- Physical
- Ethics
- Culture
- Costs
- Personnel
- Resources
- Capabilities
- Time
- Risk tolerance

Information systems security Framework

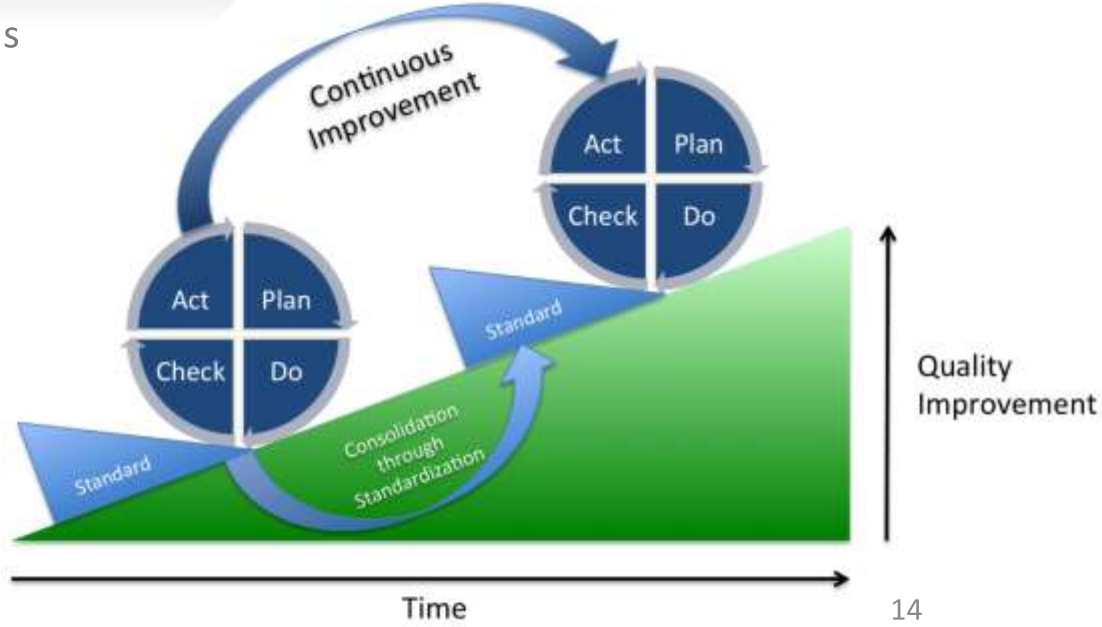
Review and improve the security plans



Define security plans

Implement security plans

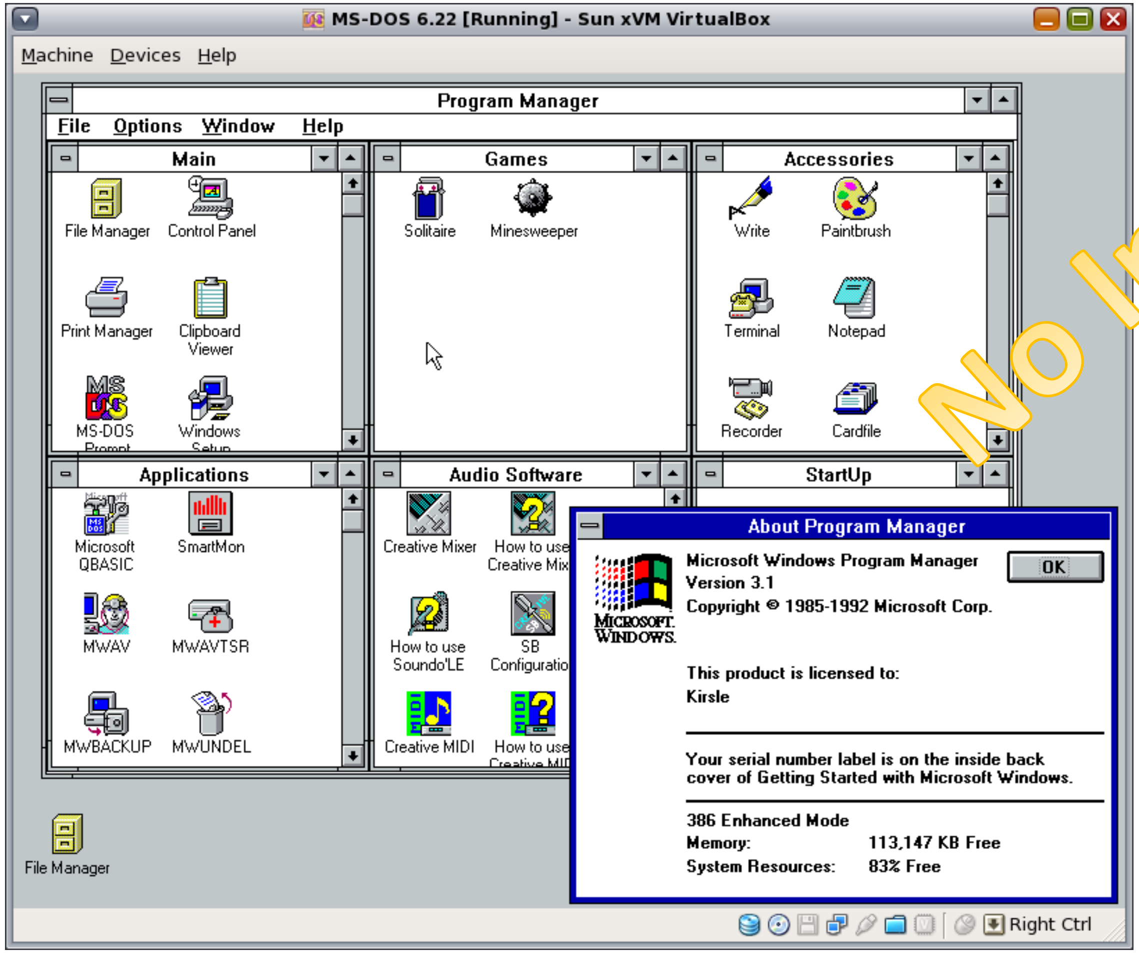
Monitor effectiveness of plans



Reference: ISO 27001 (ISMS)

APT (Advanced Persistent Threats)

From



About Program Manager

Microsoft Windows Program Manager
Version 3.1
Copyright © 1985-1992 Microsoft Corp.

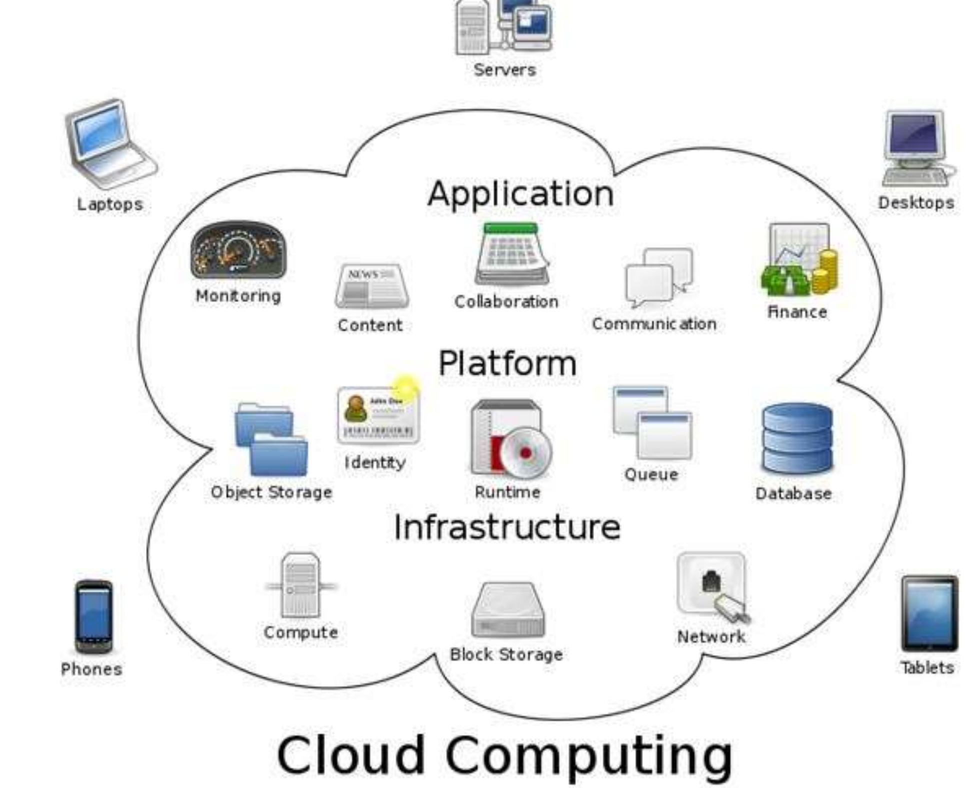
OK

This product is licensed to:
Kirsle

Your serial number label is on the inside back cover of Getting Started with Microsoft Windows.

386 Enhanced Mode
Memory: 113,147 KB Free
System Resources: 83% Free

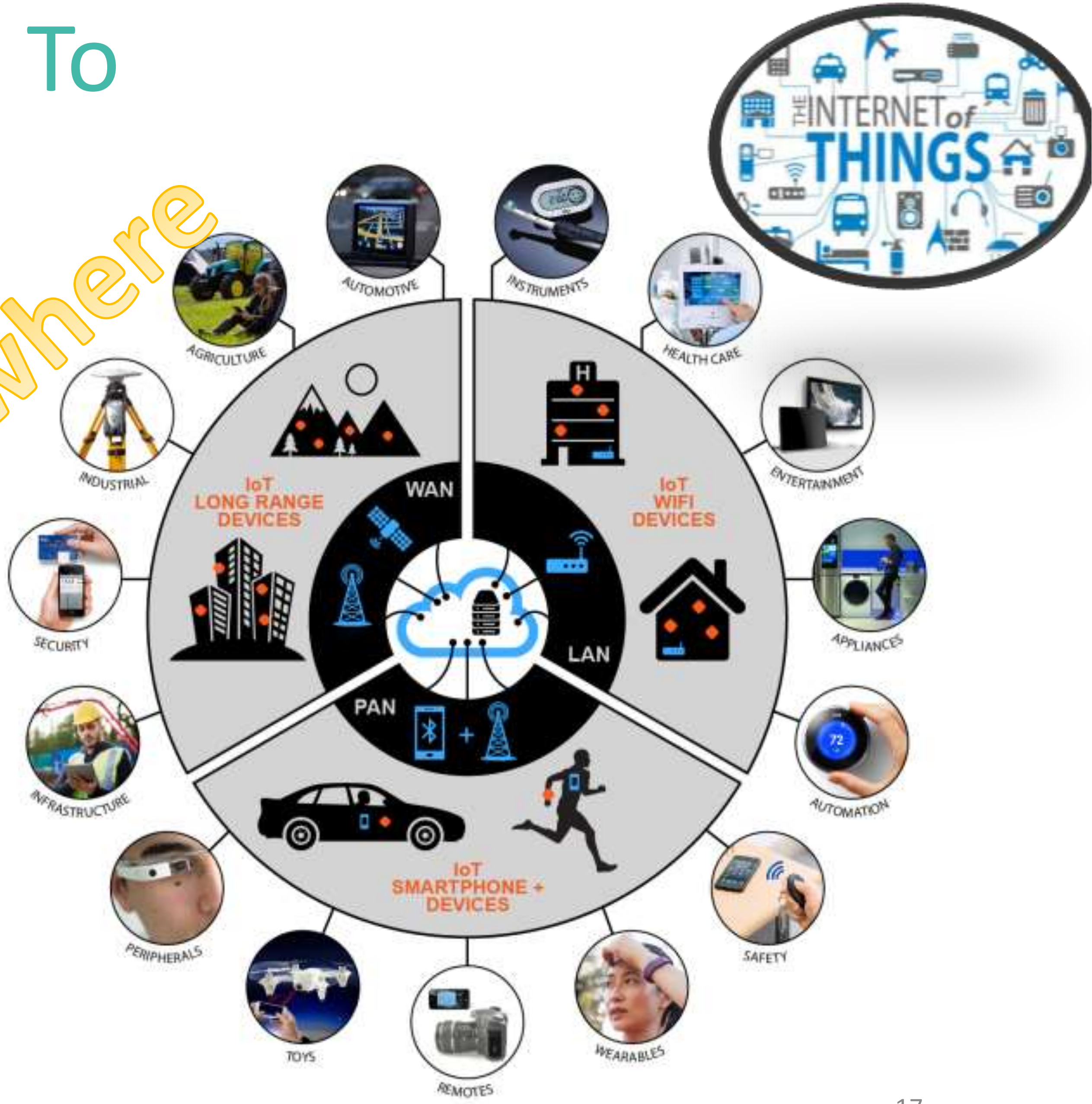
No Internet

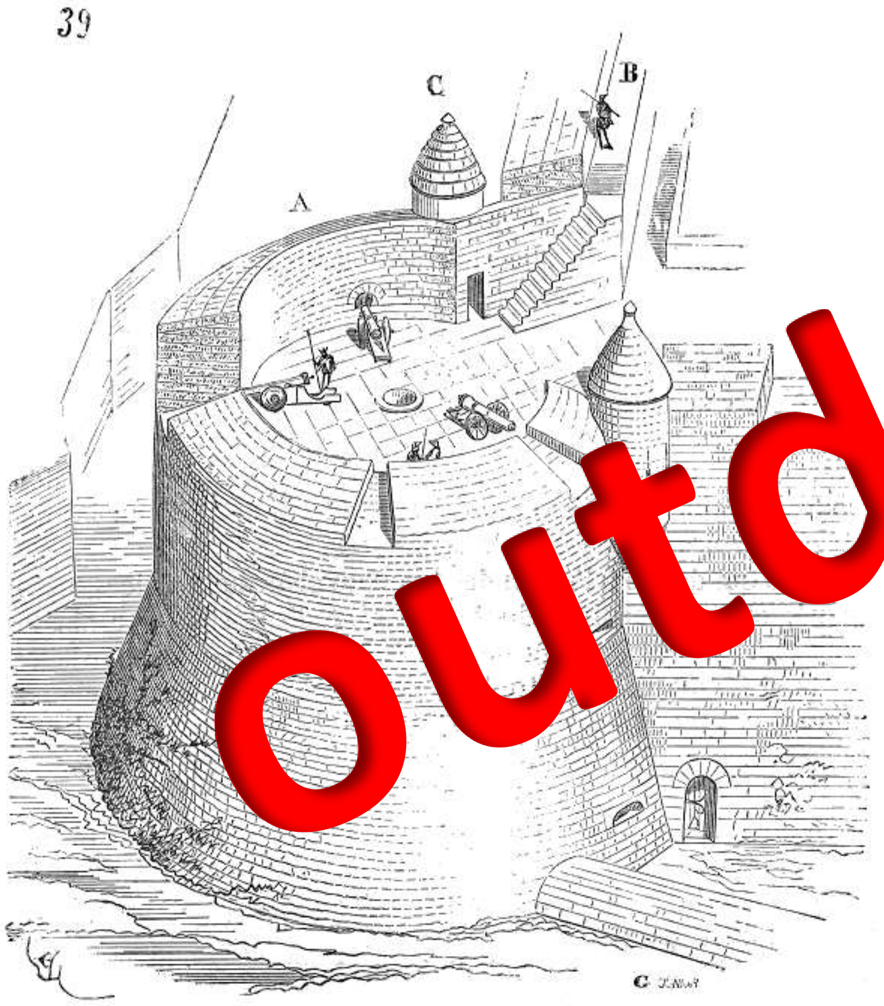


Cloud Computing

Data Everywhere

To

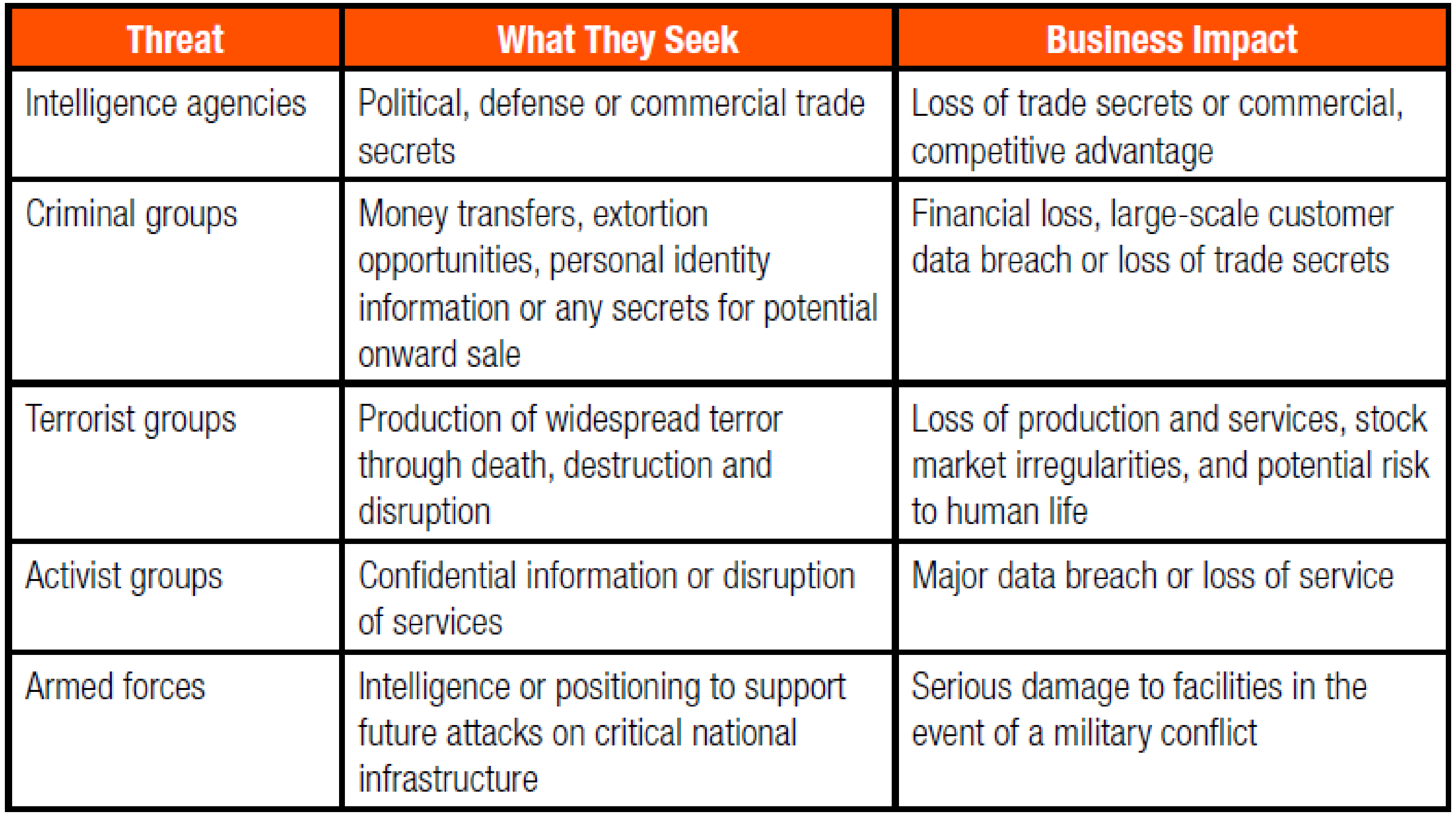




outdated

Building higher defensive walls and installing defense-in-depth solutions

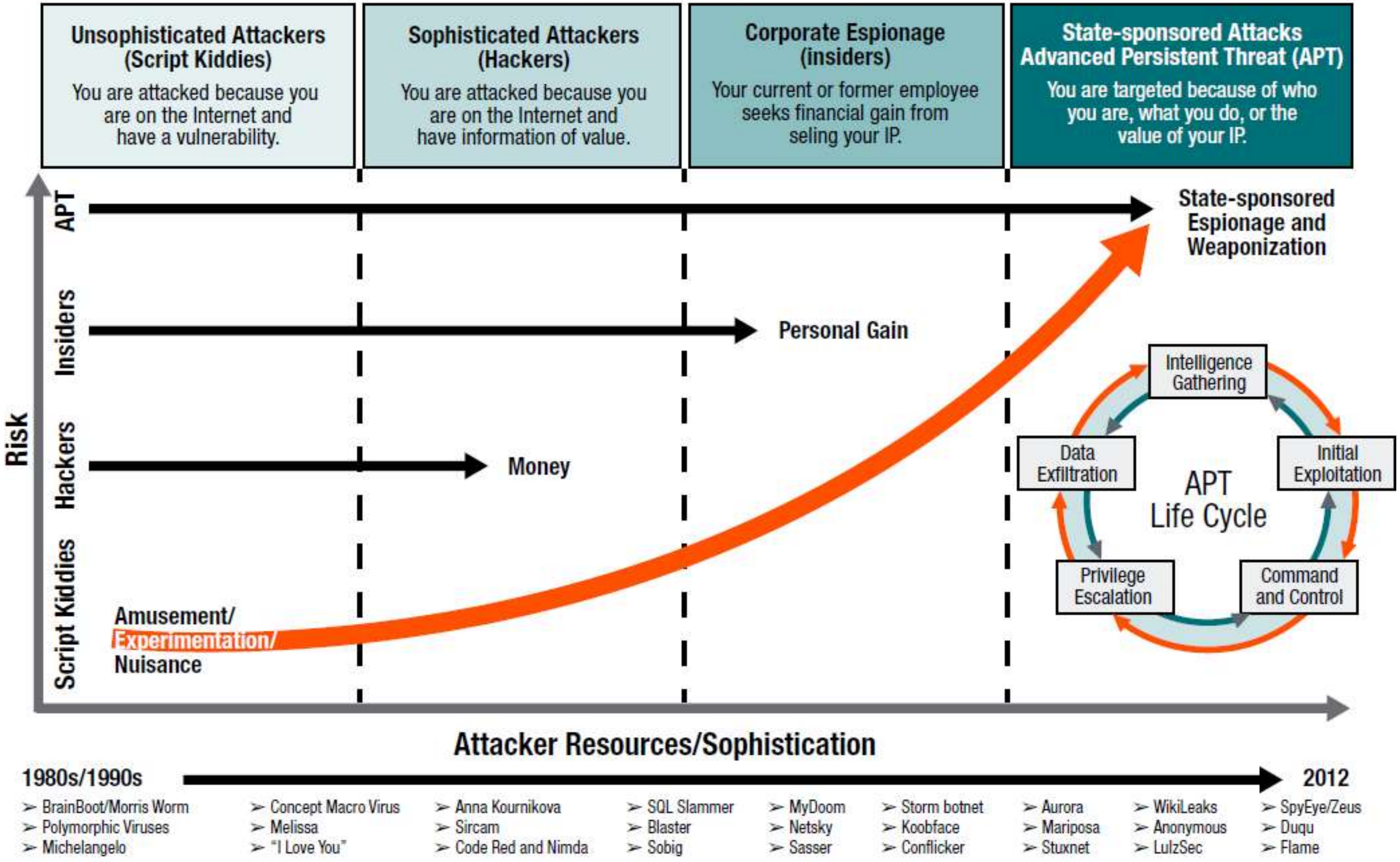
Sources of External Threats



Threat	What They Seek	Business Impact
Intelligence agencies	Political, defense or commercial trade secrets	Loss of trade secrets or commercial, competitive advantage
Criminal groups	Money transfers, extortion opportunities, personal identity information or any secrets for potential onward sale	Financial loss, large-scale customer data breach or loss of trade secrets
Terrorist groups	Production of widespread terror through death, destruction and disruption	Loss of production and services, stock market irregularities, and potential risk to human life
Activist groups	Confidential information or disruption of services	Major data breach or loss of service
Armed forces	Intelligence or positioning to support future attacks on critical national infrastructure	Serious damage to facilities in the event of a military conflict

Evolution of the Threat Landscape

ISACA.ORG



Unsophisticated Attackers (Script Kiddies)

You are attacked because you are on the Internet and have a vulnerability.

Sophisticated Attackers (Hackers)

You are attacked because you are on the Internet and have information of value.

Corporate Espionage (insiders)

Your current or former employee seeks financial gain from seling your IP.

State-sponsored Attacks Advanced Persistent Threat (APT)

You are targeted because of who you are, what you do, or the value of your IP.

- BrainBoot/Morris Worm
- Polymorphic Viruses
- Michelangelo

- Concept Macro Virus
- Melissa
- "I Love You"

- Anna Kournikova
- Sircam
- Code Red and Nimda

- SQL Slammer
- Blaster
- Sobig

- MyDoom
- Netsky
- Sasser

- Storm botnet
- Koobface
- Conflicker

- Aurora
- Mariposa
- Stuxnet

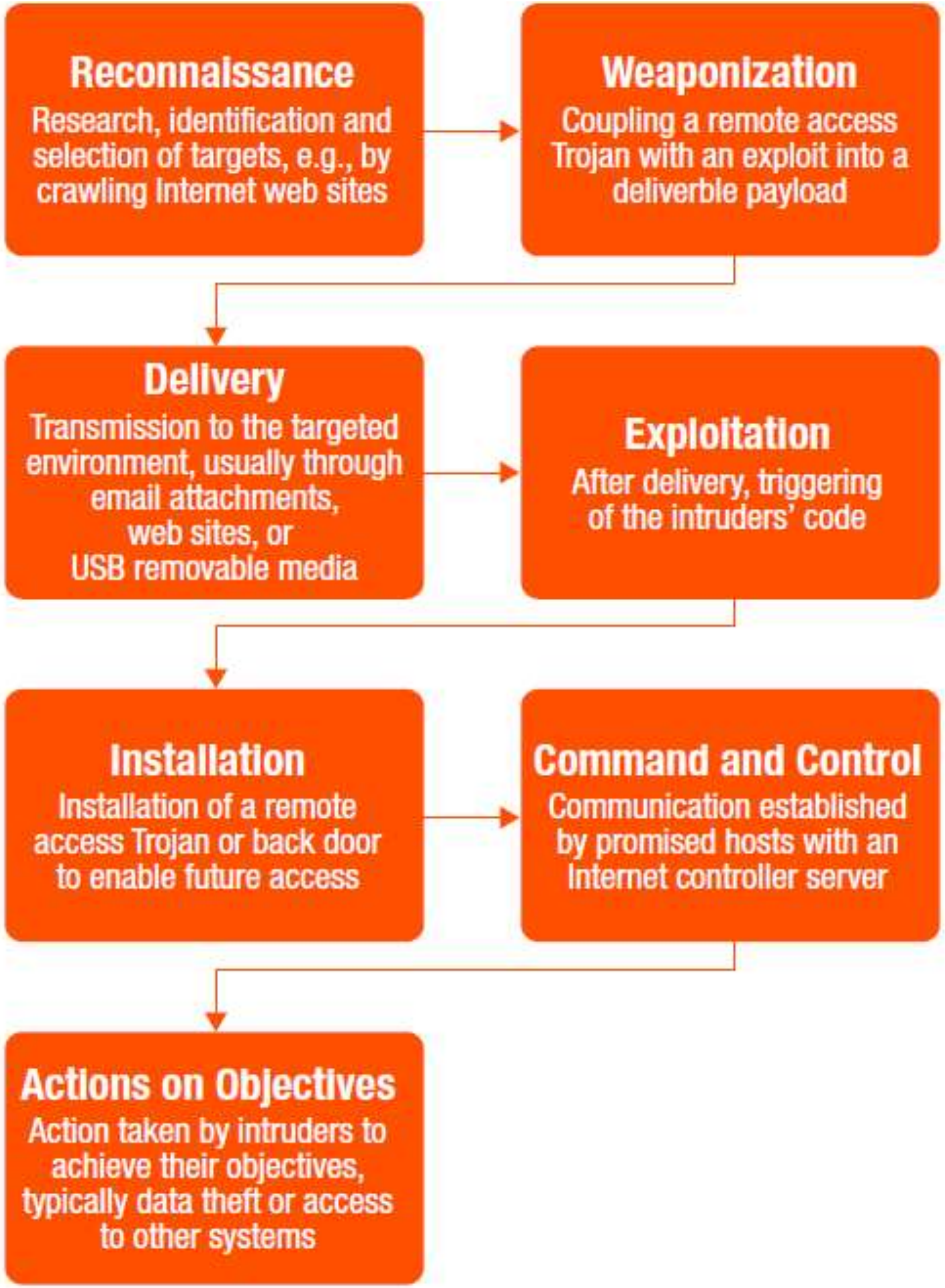
- WikiLeaks
- Anonymous
- LulzSec

- SpyEye/Zeus
- Duqu
- Flame

The “Cyber Kill Chain”

Sequence of activities conducted by an attacker to carry out an APT attack

For Your Info



Reconnaissance
Research, identification and selection of targets, e.g., by crawling Internet web sites

Weaponization
Coupling a remote access Trojan with an exploit into a deliverble payload

Delivery
Transmission to the targeted environment, usually through email attachments, web sites, or USB removable media

Exploitation
After delivery, triggering of the intruders' code

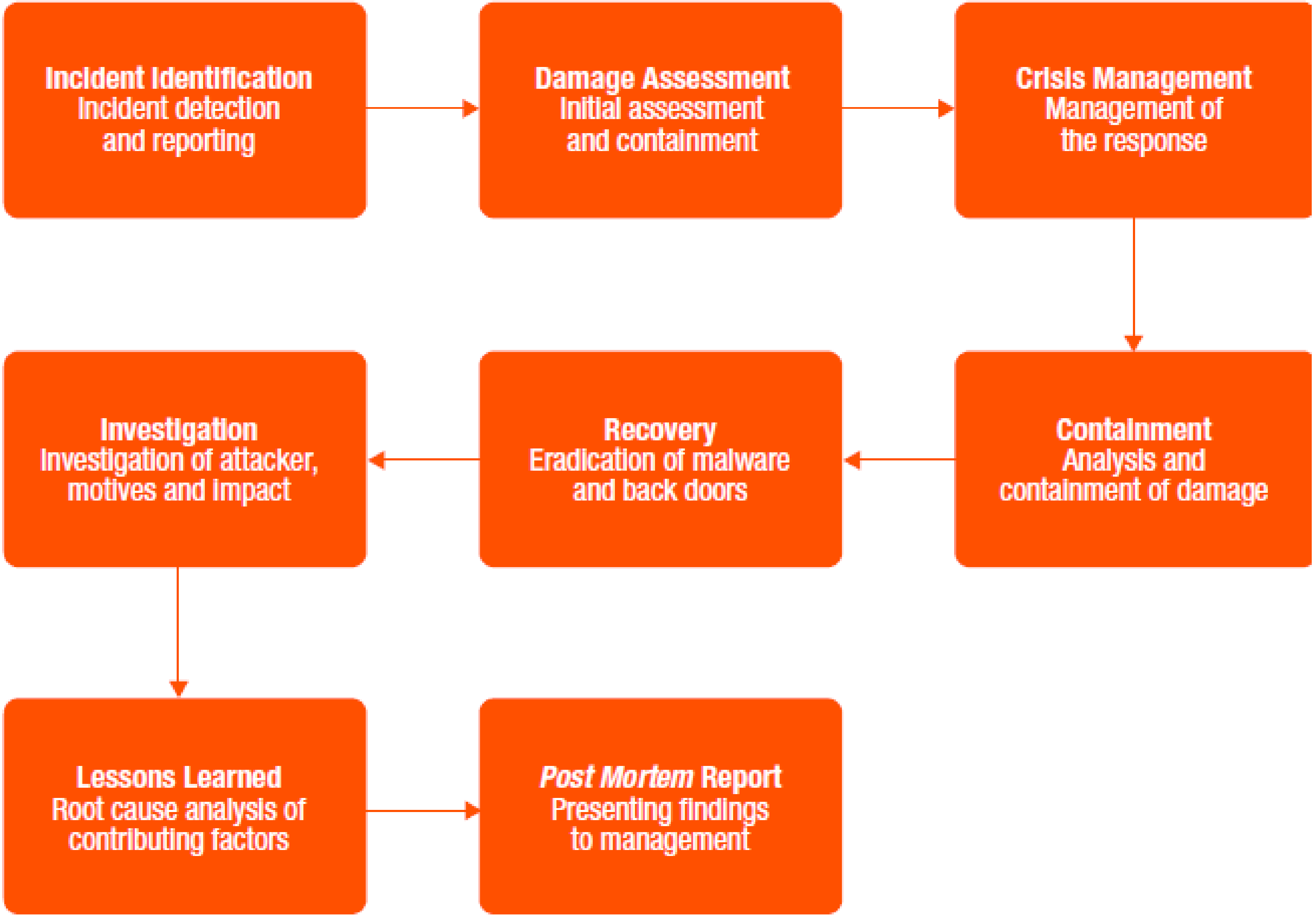
Installation
Installation of a remote access Trojan or back door to enable future access

Command and Control
Communication established by promised hosts with an Internet controller server

Actions on Objectives
Action taken by intruders to achieve their objectives, typically data theft or access to other systems

Managing an APT Incident

For Your Info



Incident Identification
Incident detection
and reporting

Damage Assessment
Initial assessment
and containment

Crisis Management
Management of
the response

Containment
Analysis and
containment of damage

Recovery
Eradication of malware
and back doors

Investigation
Investigation of attacker,
motives and impact

Lessons Learned
Root cause analysis of
contributing factors

***Post Mortem* Report**
Presenting findings
to management

Information Security

Program Development & Management

Program and Development

Full Management Support

<u>Business Vision + Threats => IS Vision</u>

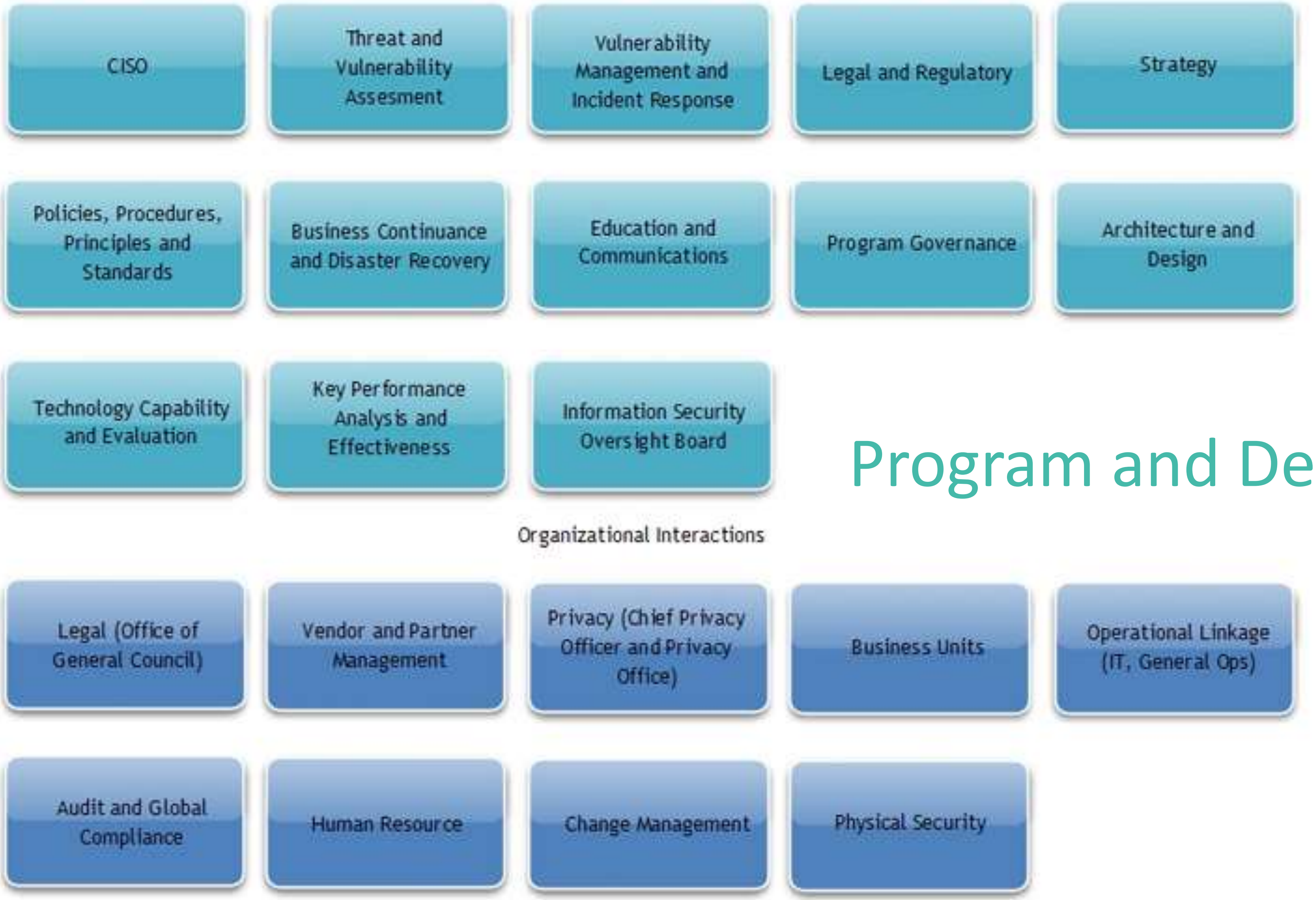
<u>IS Strategy</u>

- Strategy
- Policies
- Committees
- Projects and Resources (Time, Money, FTE)

<u>Setup / OPS</u>

- Business Projects (Revue, Security by Design, Security by Default, …)
- IS dedicated projects,
  - Priorities
  - Regulation,
  - Threats, …

Program and Development



CISO

Threat and Vulnerability Assesment

Vulnerability Management and Incident Response

Legal and Regulatory

Strategy

Policies, Procedures, Principles and Standards

Business Continuance and Disaster Recovery

Education and Communications

Program Governance

Architecture and Design

Technology Capability and Evaluation

Key Performance Analysis and Effectiveness

Information Security Oversight Board

Organizational Interactions

Legal (Office of General Council)

Vendor and Partner Management

Privacy (Chief Privacy Officer and Privacy Office)

Business Units

Operational Linkage (IT, General Ops)

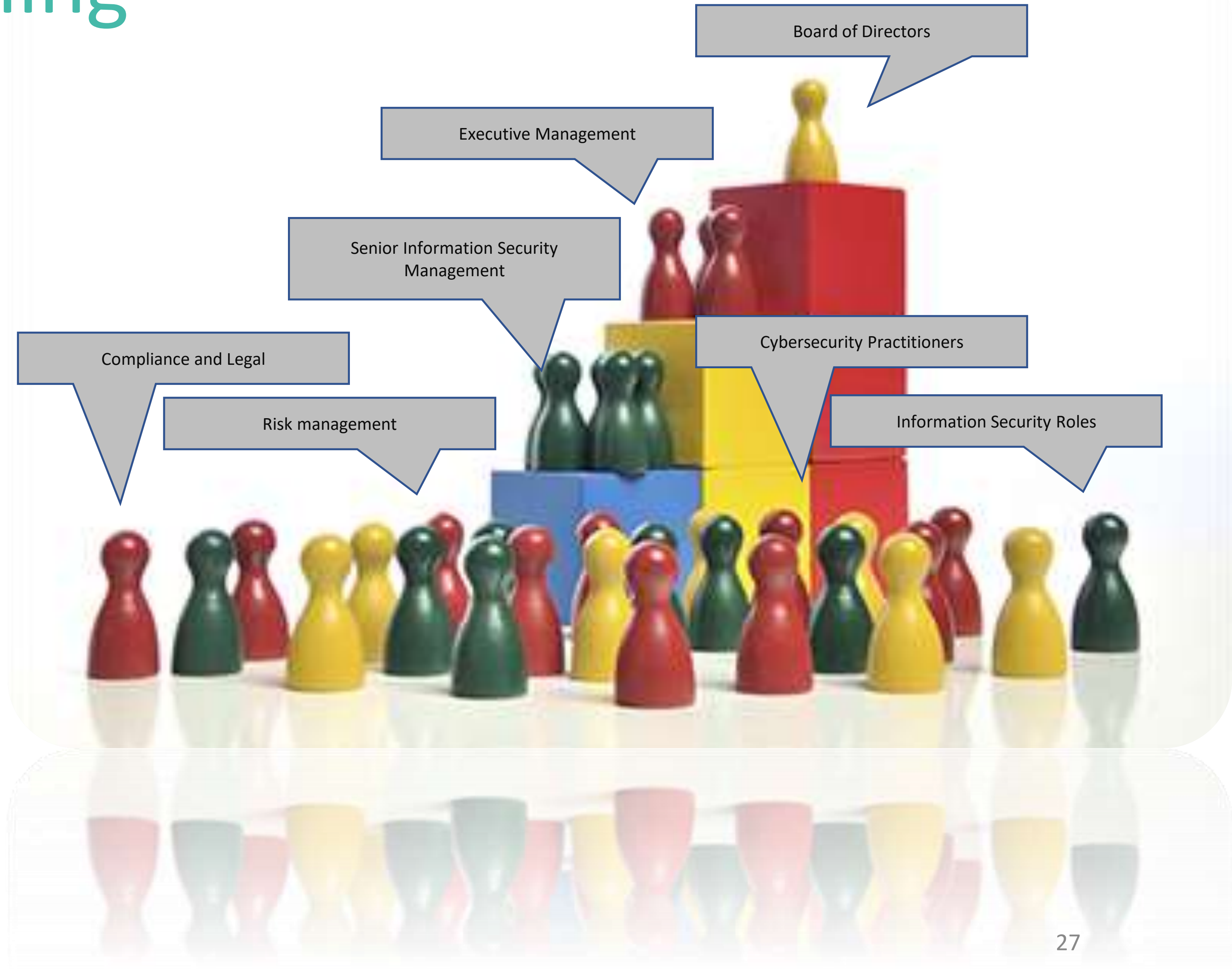
Audit and Global Compliance

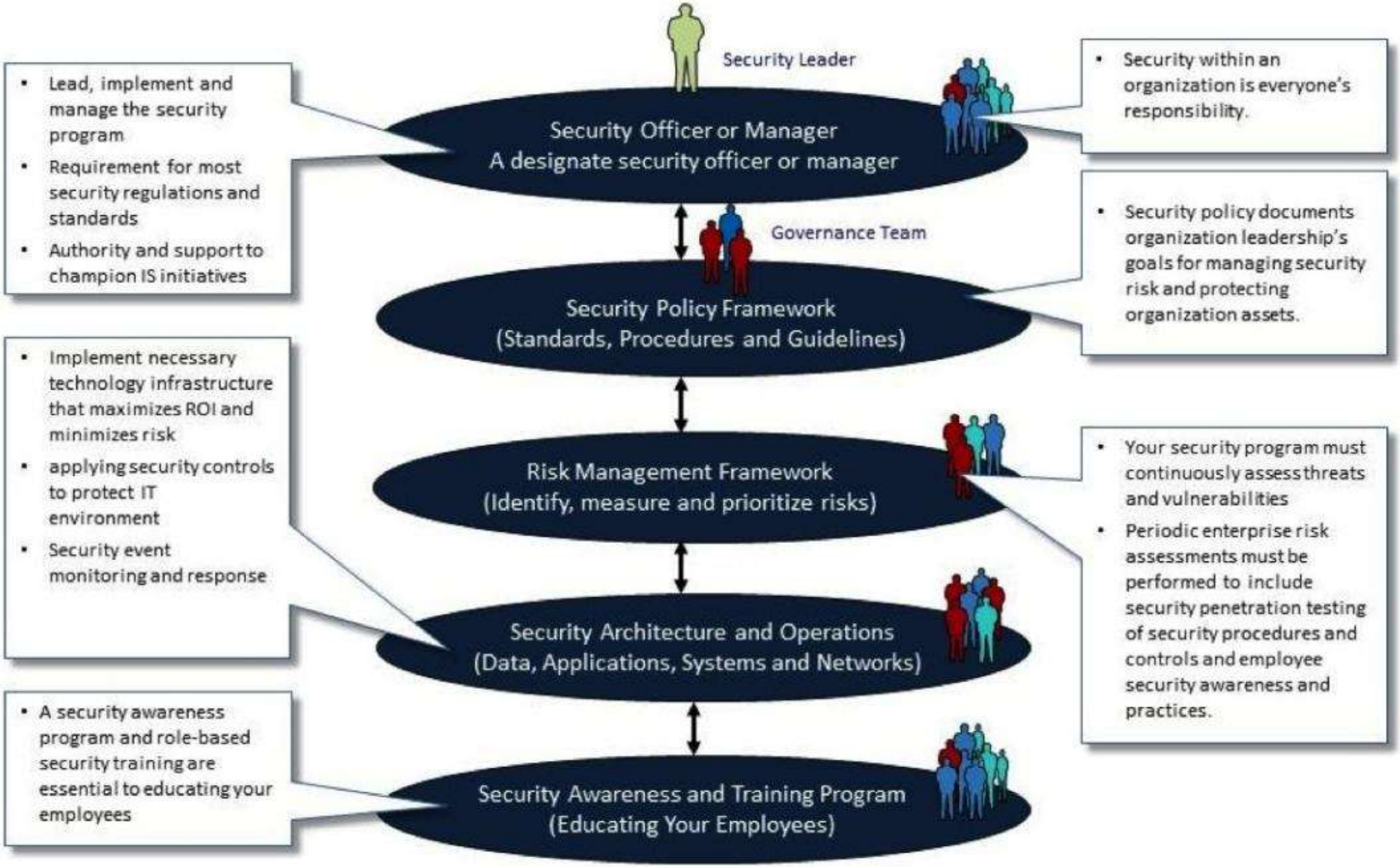
Human Resource

Change Management

Physical Security

Be Ready : Teaming


Board of Directors
Executive Management
Senior Information Security Management
Cybersecurity Practitioners
Compliance and Legal
Risk management
Information Security Roles



Security Leader

- Lead, implement and manage the security program
- Requirement for most security regulations and standards
- Authority and support to champion IS initiatives

Security Officer or Manager
A designate security officer or manager

- Security within an organization is everyone's responsibility.

Governance Team

Security Policy Framework
(Standards, Procedures and Guidelines)

- Security policy documents organization leadership's goals for managing security risk and protecting organization assets.

Risk Management Framework
(Identify, measure and prioritize risks)

- Your security program must continuously assess threats and vulnerabilities
- Periodic enterprise risk assessments must be performed to include security penetration testing of security procedures and controls and employee security awareness and practices.

- Implement necessary technology infrastructure that maximizes ROI and minimizes risk
- applying security controls to protect IT environment
- Security event monitoring and response

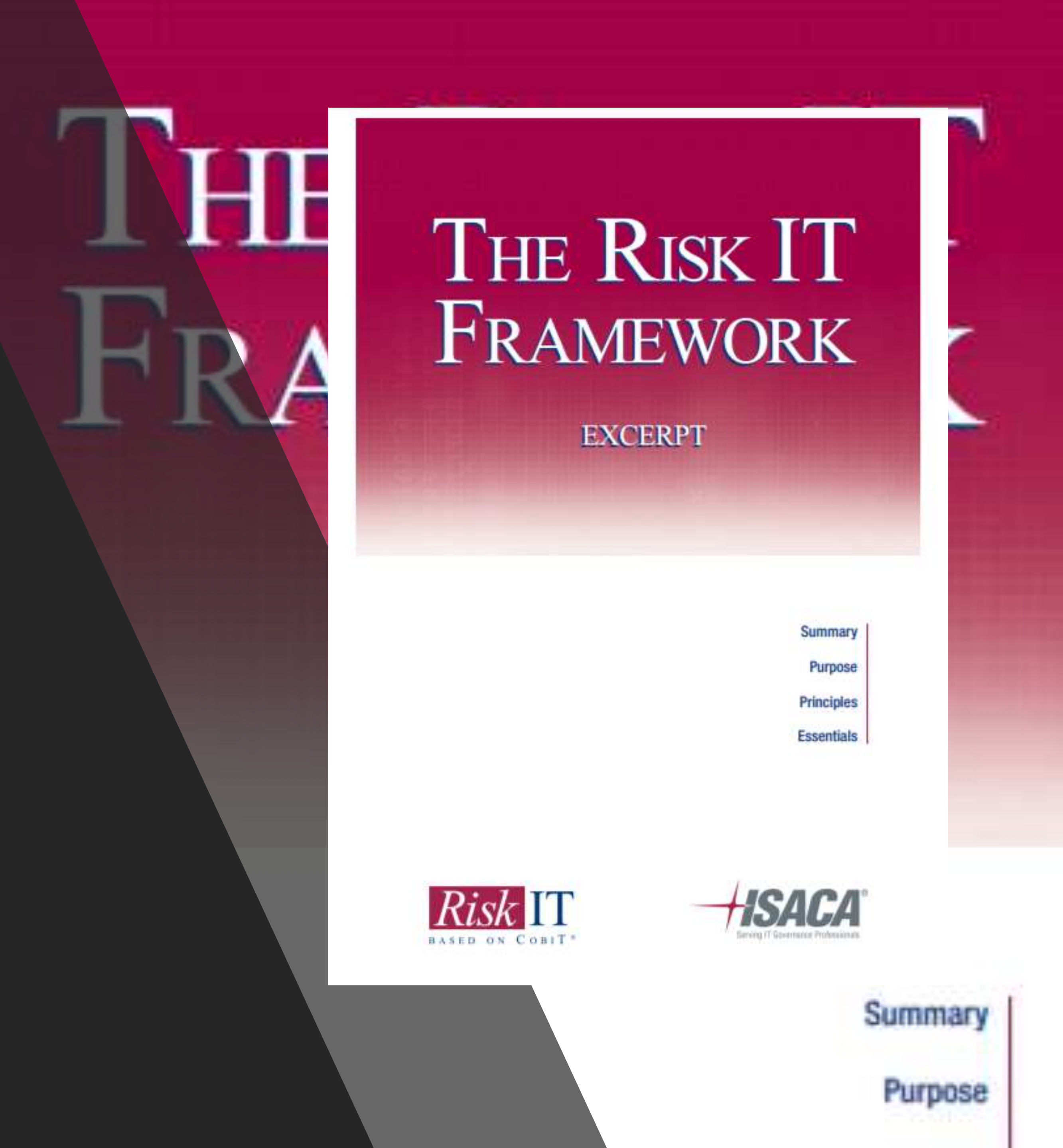
Security Architecture and Operations
(Data, Applications, Systems and Networks)

- A security awareness program and role-based security training are essential to educating your employees

Security Awareness and Training Program
(Educating Your Employees)

Information Security

Risk Management and Compliance



THE RISK IT FRAMEWORK

EXCERPT

Summary

Purpose

Principles

Essentials

Risk IT

BASED ON COBIT®

ISACA®

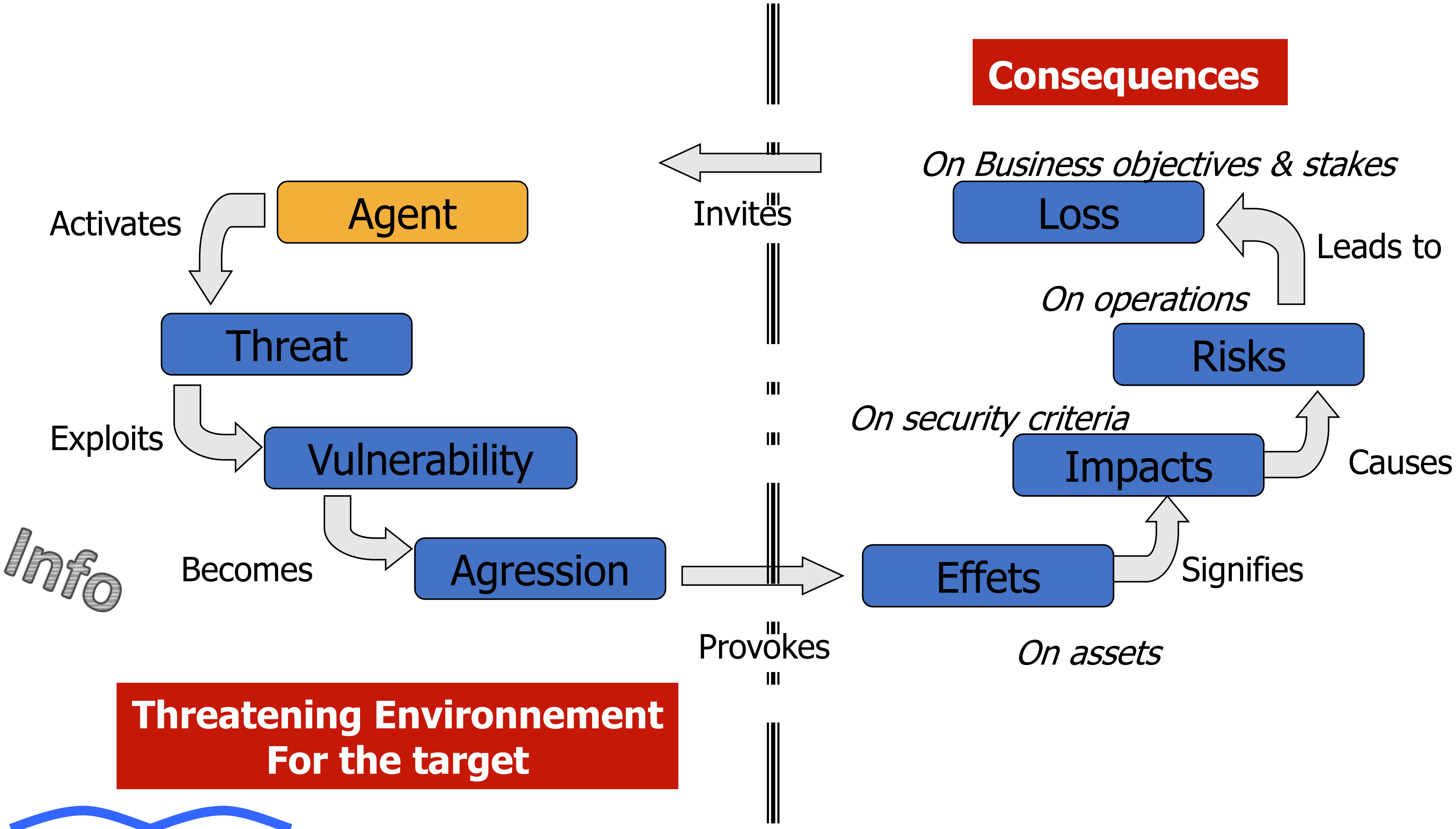
Serving IT Governance Professionals

THE RISK IT FRAMEWORK

Summary

Purpose

Risk Cycle



For Your Info

MISIS

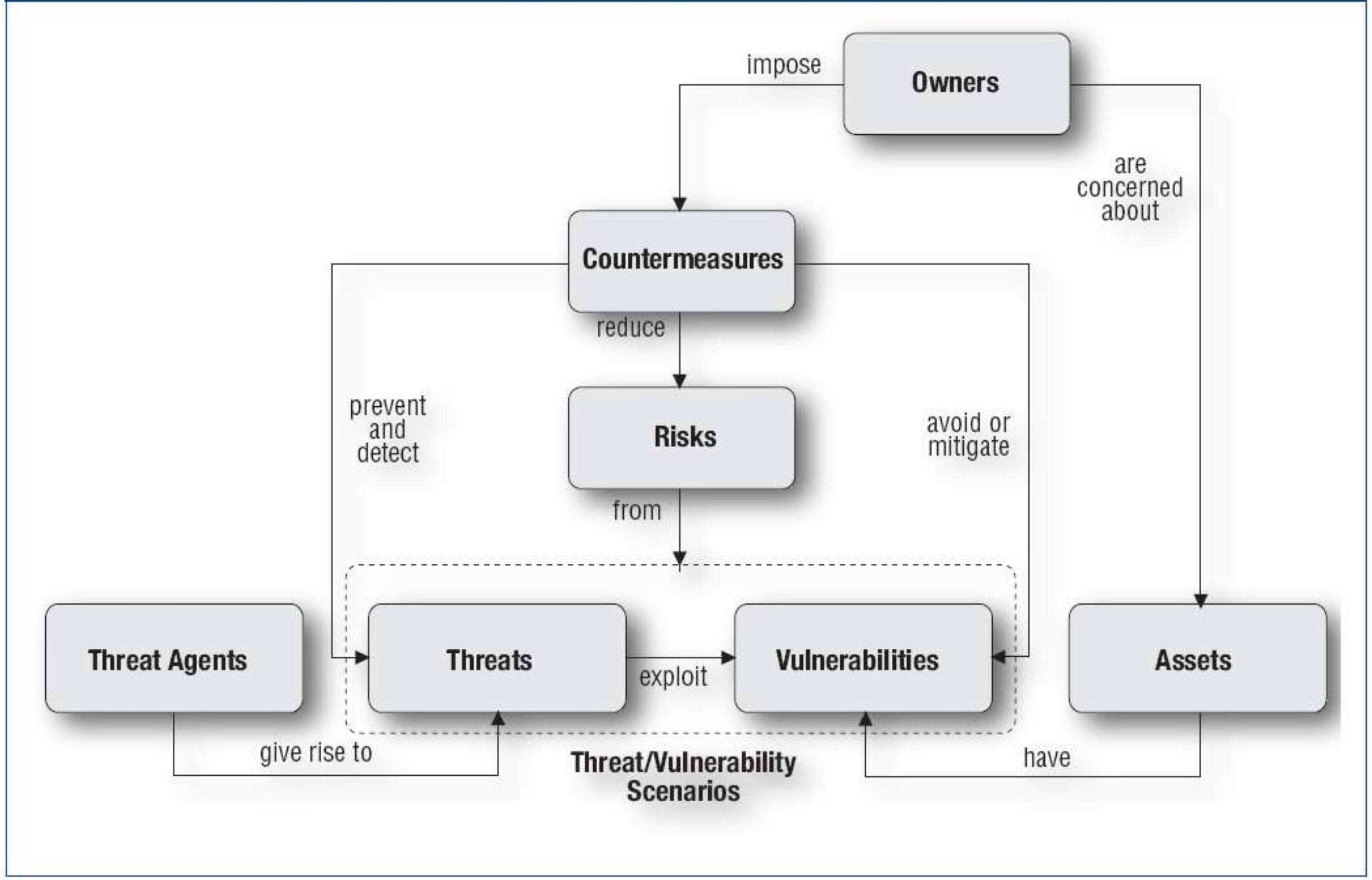
RA Components

IT ASSURANCE GUIDE

USING COBIT

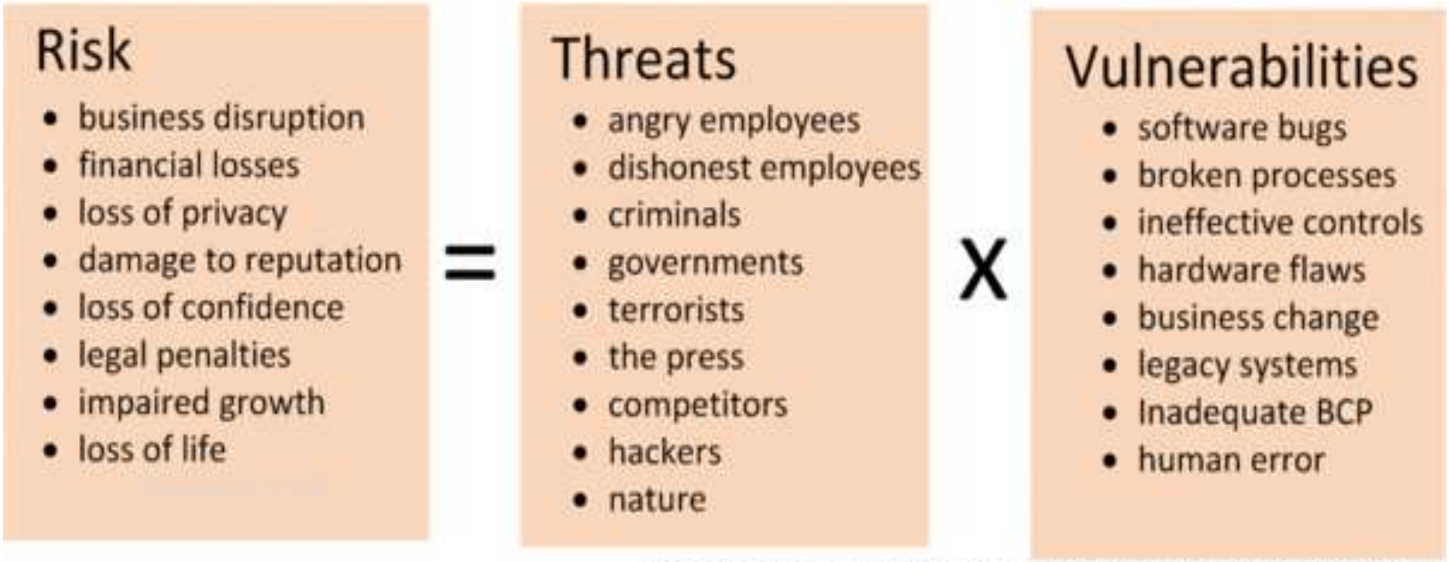
For Your Info

Figure 18–Relationship and Attributes of the Risk Analysis Components

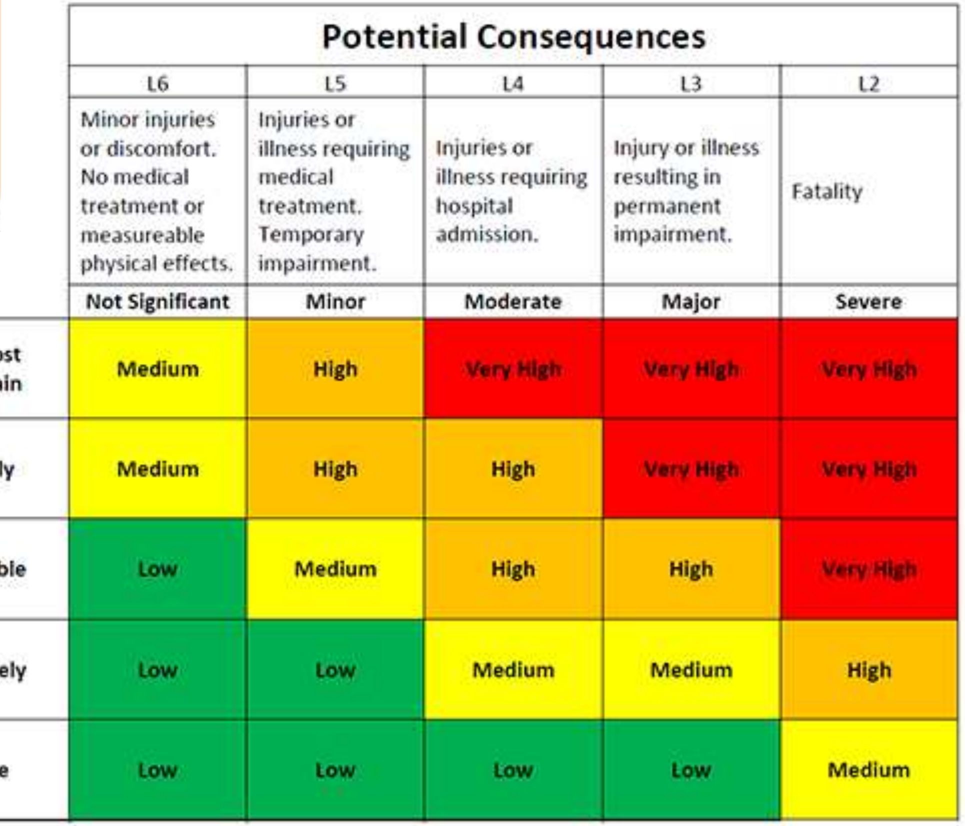


Source: IT Assurance Guide (itgi.org)

Information Security Risks



Information Security Risks, Threats and Vulnerabilities

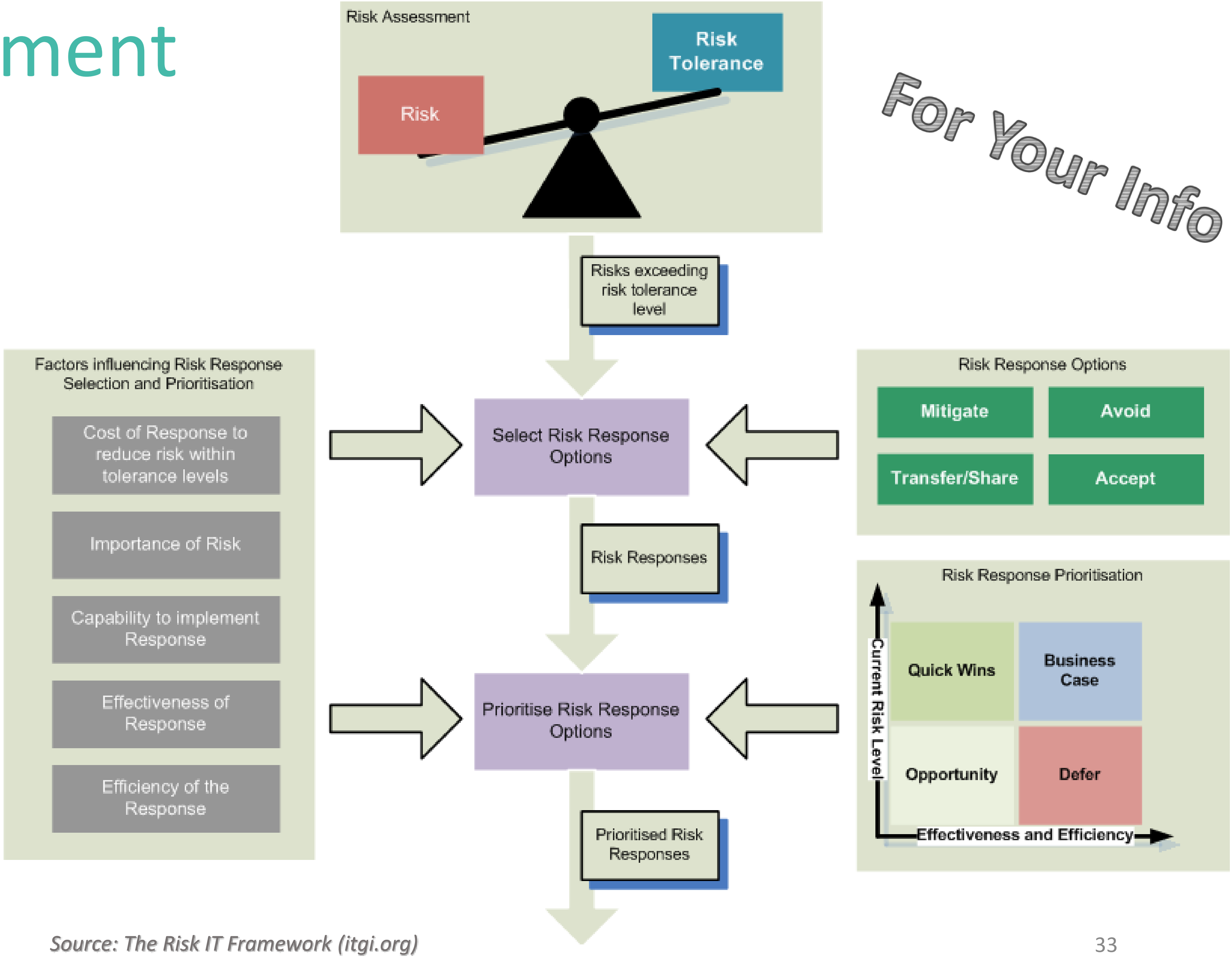


			Potential Consequences				
			L6	L5	L4	L3	L2
			Minor injuries or discomfort. No medical treatment or measureable physical effects.	Injuries or illness requiring medical treatment. Temporary impairment.	Injuries or illness requiring hospital admission.	Injury or illness resulting in permanent impairment.	Fatality
			Not Significant	Minor	Moderate	Major	Severe
Likelihood	Expected to occur regularly under normal circumstances	Almost Certain	Medium	High	Very High	Very High	Very High
	Expected to occur at some time	Likely	Medium	High	High	Very High	Very High
	May occur at some time	Possible	Low	Medium	High	High	Very High
	Not likely to occur in normal circumstances	Unlikely	Low	Low	Medium	Medium	High
	Could happen, but probably never will	Rare	Low	Low	Low	Low	Medium

Risk Management Model

For Your Info

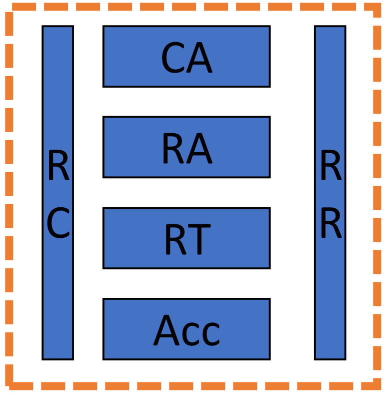
Information Security Risks List
Abuse of rights
Breach of information system maintainability
Breach of personnel availability
Corruption of data
Data from untrustworthy sources
Denial of actions
Disclosure
Equipment failure or malfunction
Error in use
Fraudulent copying of software
Hacking
Illegal processing of data
Loss of essential services
Malicious code and Virus
Natural events
Physical / Accidental damage
Remote spying, and Eavesdropping
Retrieval of recycled or discarded media
Saturation of the information system and Ddos
Software malfunction
Theft of equipment, media or documents
Unauthorised use of equipment
Use of counterfeit or copied software

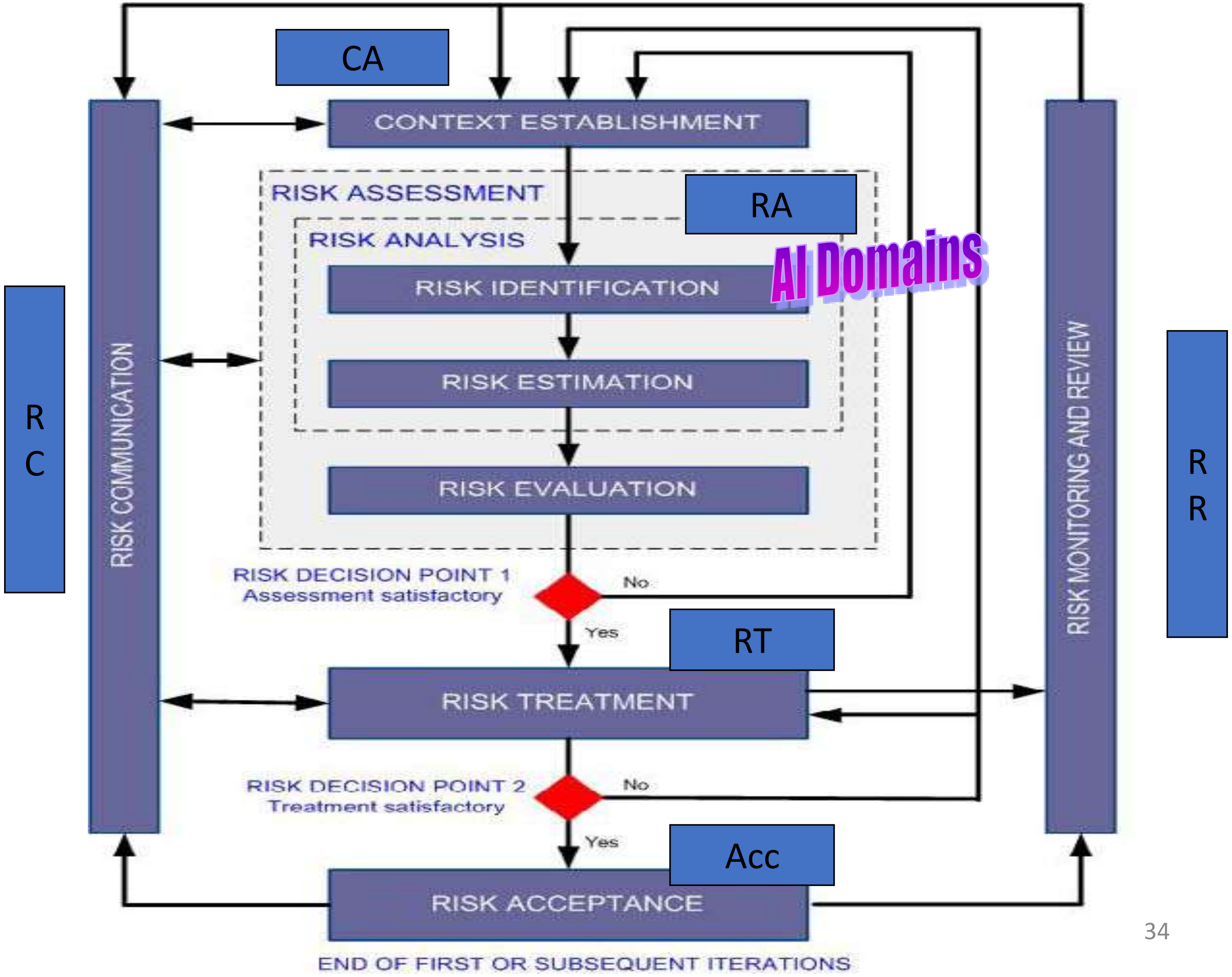


Risk Assessment
Risk
Risk Tolerance
Risks exceeding risk tolerance level
Factors influencing Risk Response Selection and Prioritisation
Cost of Response to reduce risk within tolerance levels
Importance of Risk
Capability to implement Response
Effectiveness of Response
Efficiency of the Response
Select Risk Response Options
Risk Responses
Prioritise Risk Response Options
Prioritised Risk Responses
Risk Response Options
Mitigate
Avoid
Transfer/Share
Accept
Risk Response Prioritisation
Current Risk Level
Quick Wins
Business Case
Opportunity
Defer
Effectiveness and Efficiency

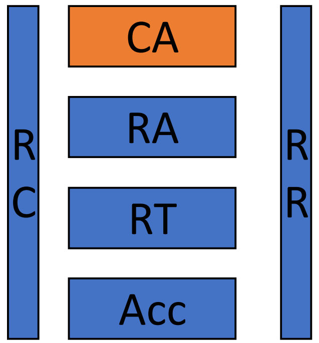
Source: The Risk IT Framework (itgi.org)

Information Risk Management Steps





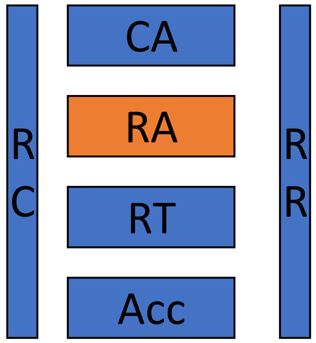
Context Establishment



- Determine and describe
  - Scope (perimeter) of the process
    - A full system or one of its components
    - Content and aim
  - Purpose of the process
    - Definition of security objectives
    - ISMS
    - Certification
  - Constraints and risk factors
    - For acceptability, capability, etc.
    - Need for security (e.g. BIA)

For Your Info

Risk Assessment


RC

CA

RA

RT

Acc

RR

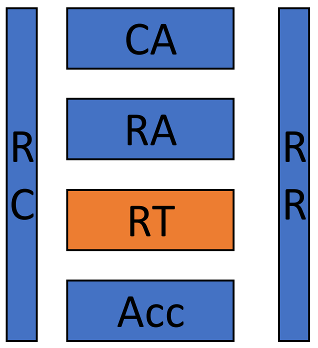
- Identify risks
  - To scope (what prevents to reach scope's aim)
- Estimate risks
  - Measure identified risks (realistic and relevant)
- Assess risks
  - Compare to risk factors
    - Risk aversion
    - Acceptance criteria and level
- Establish ranked list of 'to be dealt with' risks

For Your Info

Look for:

1. What is critical, obvious and can easily be dealt with
2. What needs further investigations
   - More precise measurement
   - More precise control
3. Loop

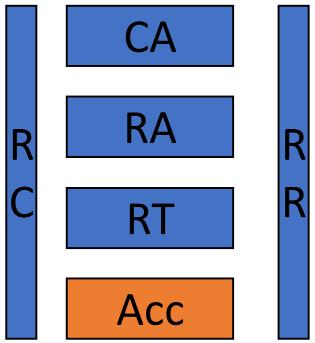
Risk Treatment



- Determine option
  - Avoidance, Transfer, Reduction, Sharing, Retain (= accept without doing anything)
- Determine treatment capability
  - Resources, skills, budget
  - Motivation of users
- Look for best ‘measure’ to
  - Break risk cycle (min 1 place, better 2 or 3)
  - SMART solution
  - Cost calculation
  - ‘effect’ computation on the risk figure

For Your Info

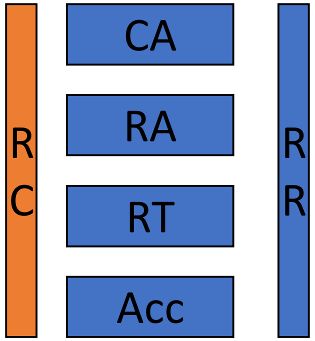
Risk Acceptance



- Make an decision
  - Motivated and official
  - To accept the solutions
  - To accept the ‘residual level of risk’
  - Allocate the means and ressources
  - Prepare a programme/plan to implement the controls

For Your Info

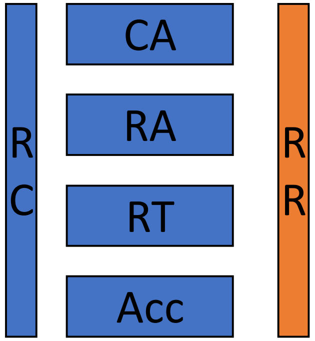
Risk Communication



- At all stages of the process
- With all ‘shareholders’
  - Asset owners
  - Users
  - Actors who will ‘handle’ the assets and the security mechanisms
  - Stake holders who will provide means & resources
- With ‘externals’
  - Partners & customers
  - Auditors
  - Regulators

For Your Info

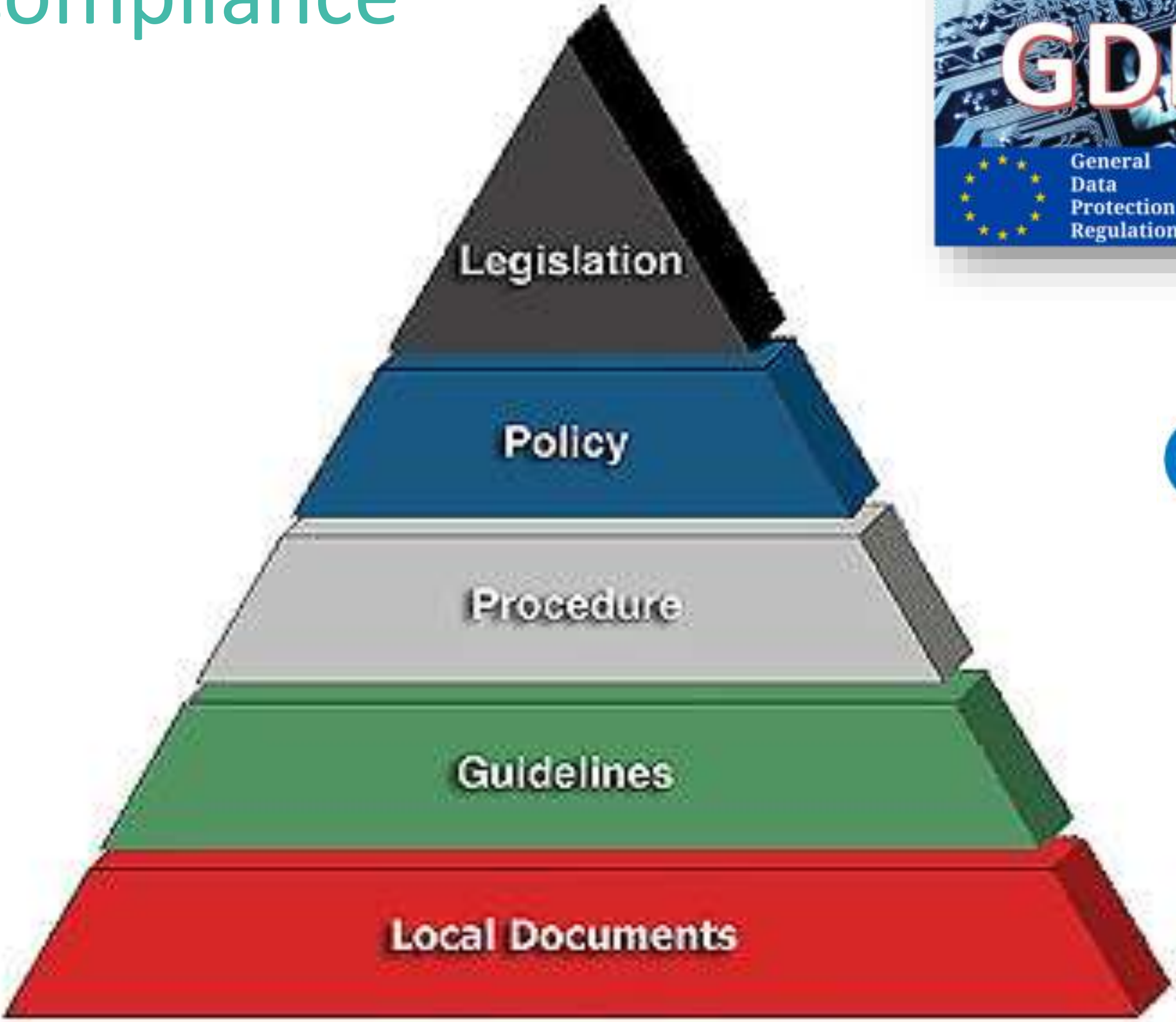
Risk Monitoring and Review



- Make sure the ‘criteria’ and ‘level’ used to make a decision are still valid
- Make sure the method used is still applicable and we have the resources to implement it
- Monitor current effect of the controls on the ‘security level’
- Monitor effectiveness of controls
- Use feedback of ‘security watch’

For Your Info

Compliance



Legislation

Policy

Procedure

Guidelines

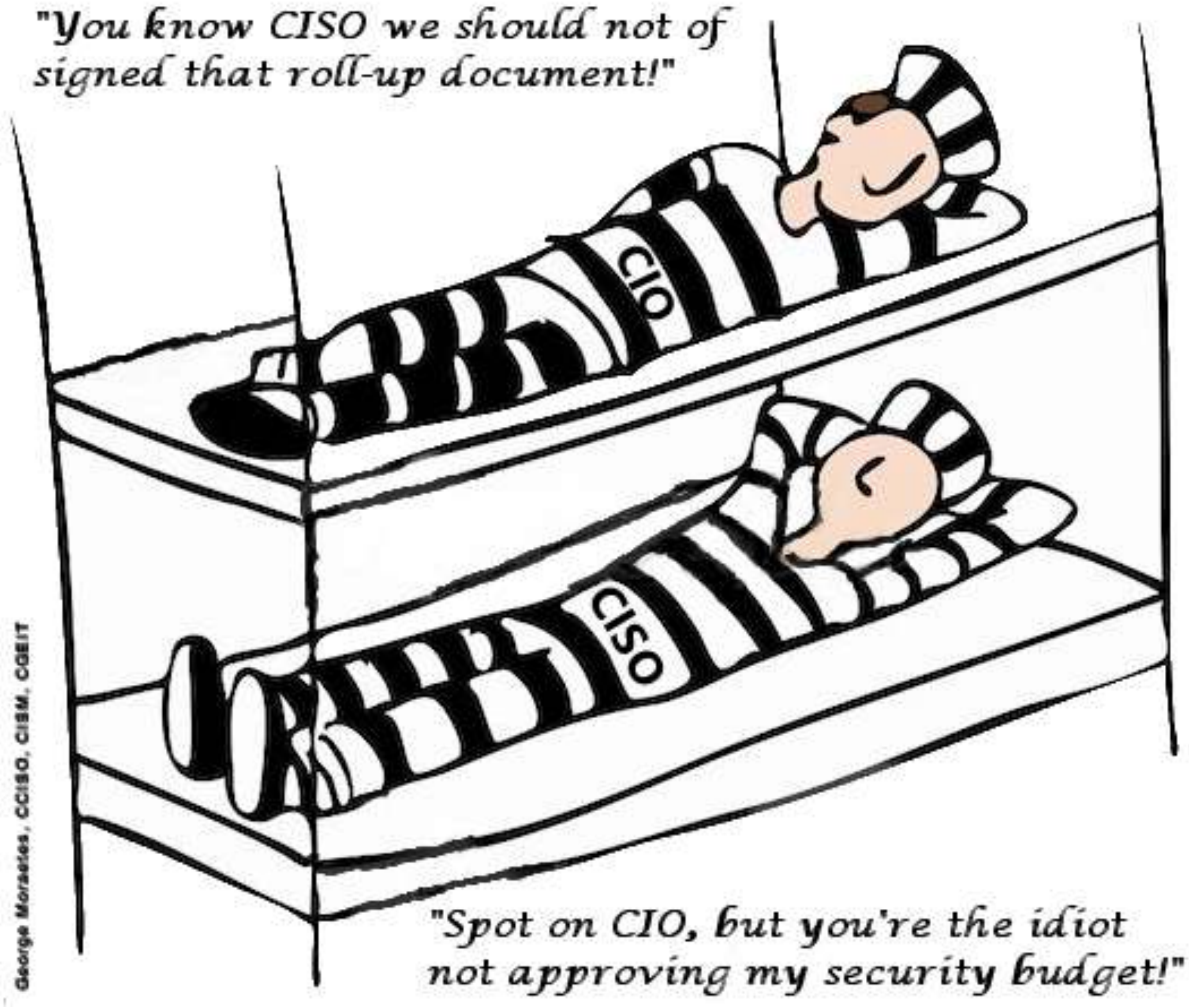
Local Documents

MiFID II

SARBANES-OXLEY

cssf
Commission de Surveillance
du Secteur Financier

Compliance vs Real-Life

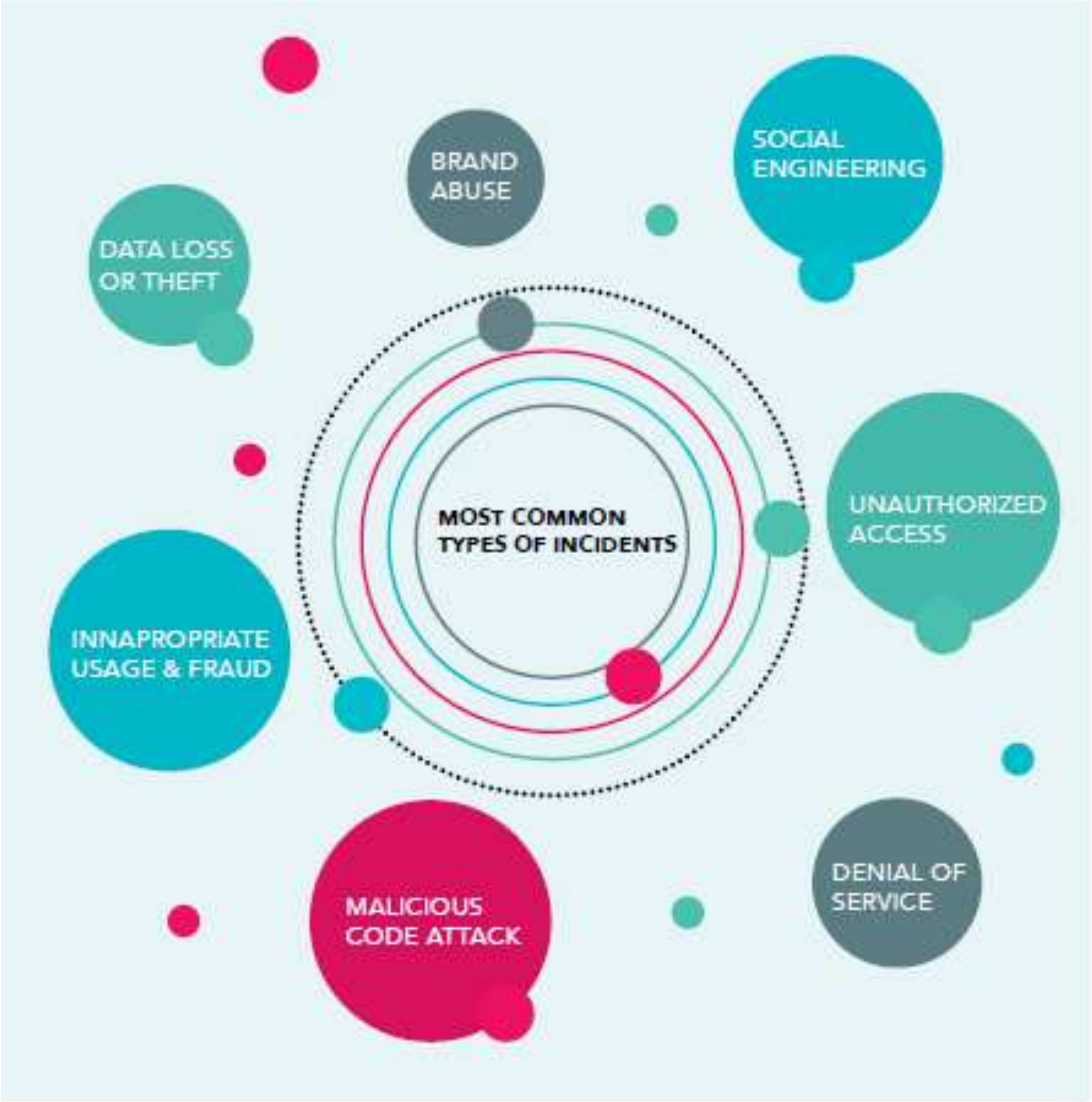

"You know CISO we should not of signed that roll-up document!"
CIO
CISO
"Spot on CIO, but you're the idiot not approving my security budget!"
George Moraetes, CCISO, CISM, CGEIT

Incident Management

CYBER SECURITY
INCIDENT MANAGEMENT GUIDE

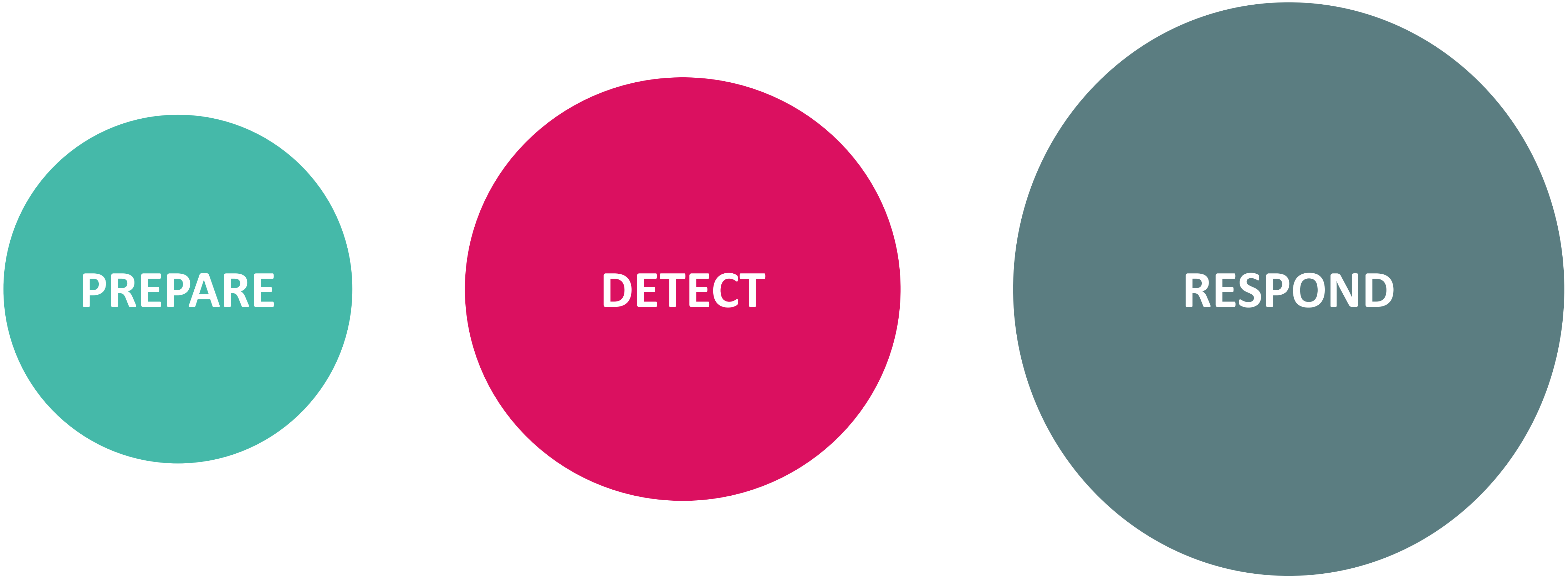
CYBER SECURITY COALITION
CENTER FOR CYBER SECURITY BELGIUM
Solvay Brussels School Economics & Management
IT MANAGEMENT Academy

CYBER SECURITY
INCIDENT MANAGEMENT GUIDE



Information Security Risks
Abuse of rights
Breach of information system maintainability
Breach of personnel availability
Corruption of data
Data from untrustworthy sources
Denial of actions
Disclosure
Equipment failure or malfunction
Error in use
Fraudulent copying of software
Hacking
Illegal processing of data
Loss of essential services
Malicious code and Virus
Natural events
Physical / Accidental damage
Remote spying, and Eavesdropping
Retrieval of recycled or discarded media
Saturation of the information system and Ddos
Software malfunction
Theft of equipment, media or documents
Unauthorised use of equipment
Use of counterfeit or copied software

⚠



PREPARE

DETECT

RESPOND

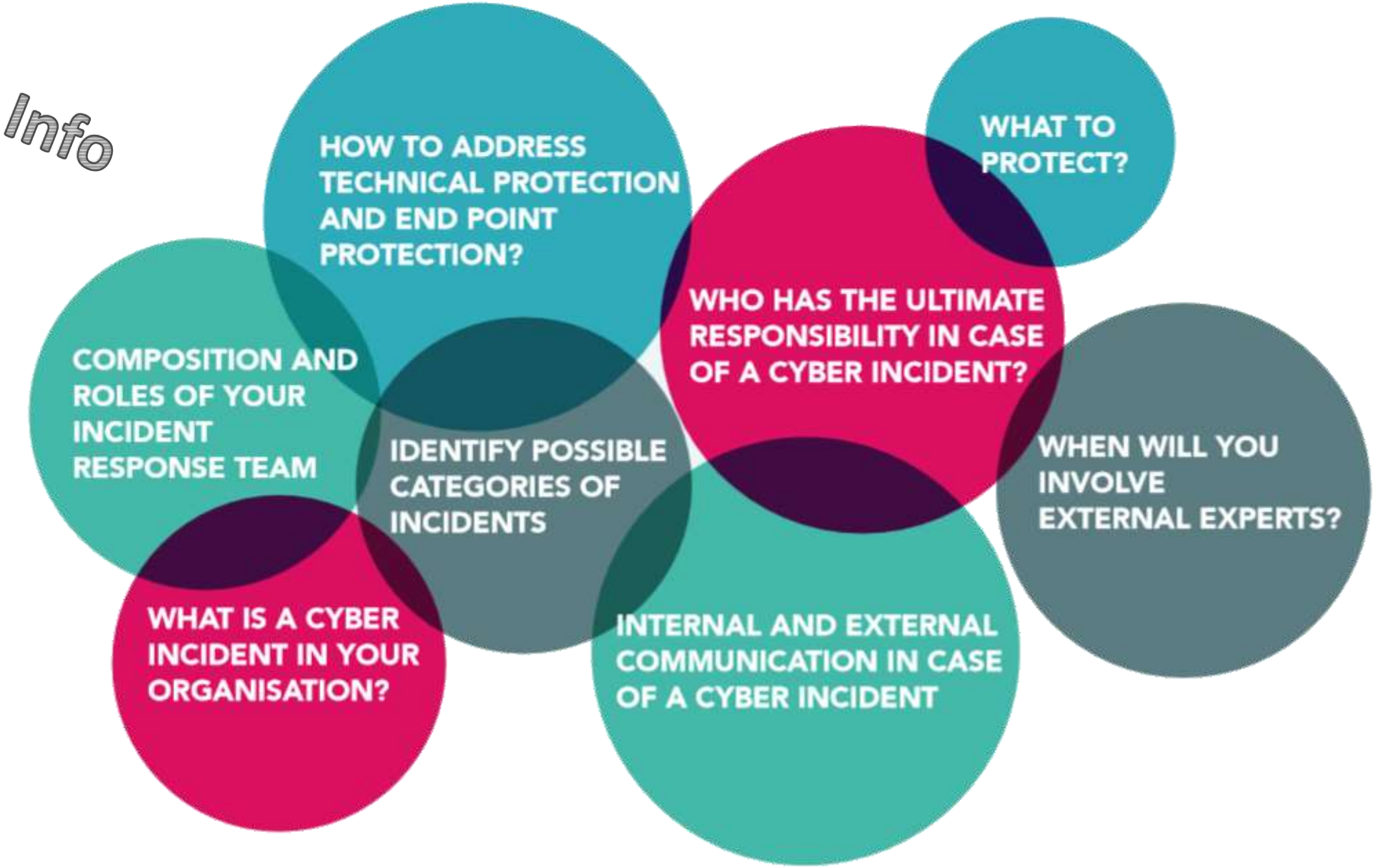
For Your Info

PREPARE

- Identify resources and risks
- Responsibilities and expertise
- Risk improvements plan
- Communication Strategy

For Your Info

KEY ELEMENTS OF A CYBER SECURITY INCIDENT RESPONSE PLAN



HOW TO ADDRESS TECHNICAL PROTECTION AND END POINT PROTECTION?

WHAT TO PROTECT?

WHO HAS THE ULTIMATE RESPONSIBILITY IN CASE OF A CYBER INCIDENT?

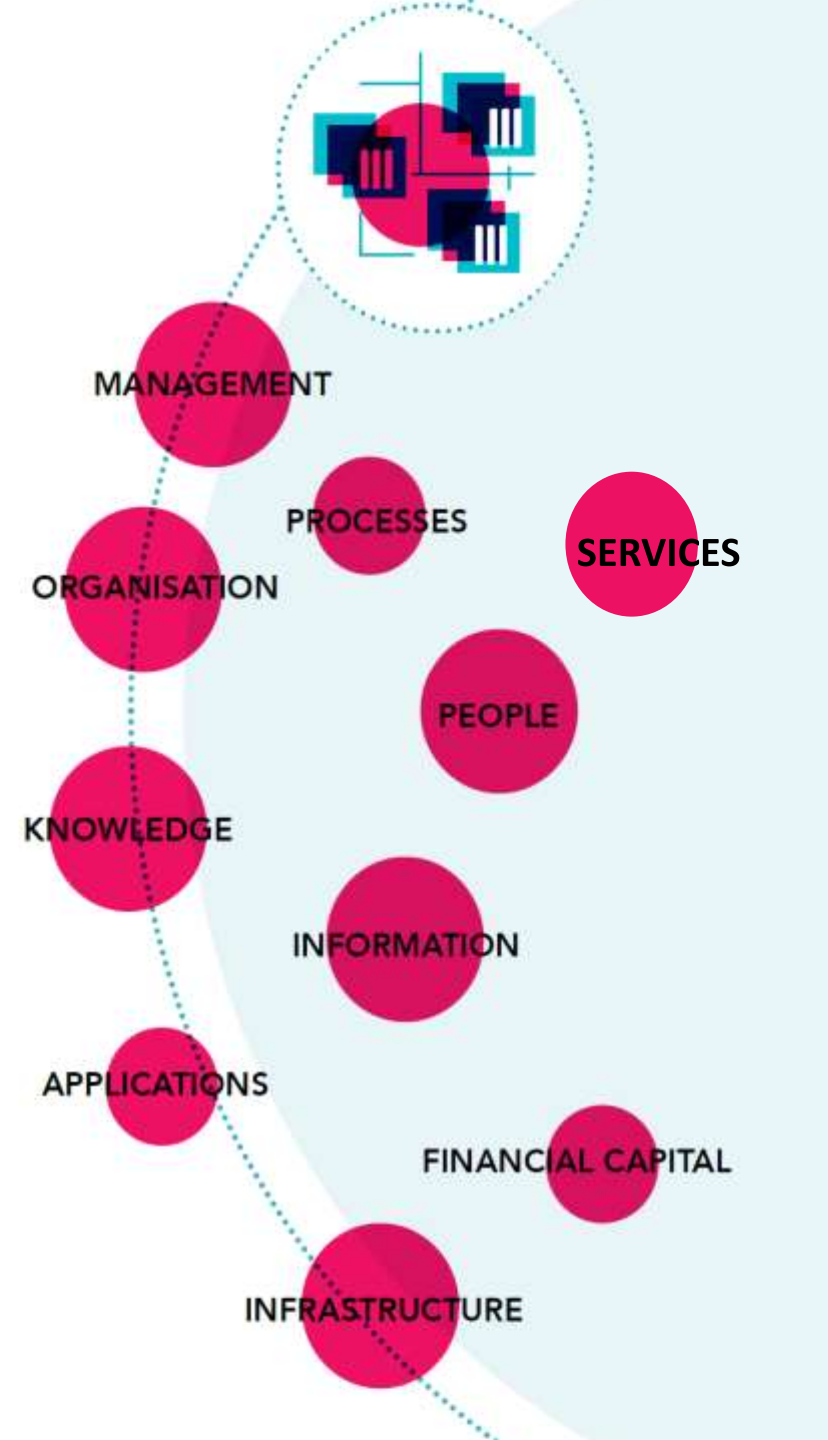
COMPOSITION AND ROLES OF YOUR INCIDENT RESPONSE TEAM

IDENTIFY POSSIBLE CATEGORIES OF INCIDENTS

WHEN WILL YOU INVOLVE EXTERNAL EXPERTS?

WHAT IS A CYBER INCIDENT IN YOUR ORGANISATION?

INTERNAL AND EXTERNAL COMMUNICATION IN CASE OF A CYBER INCIDENT



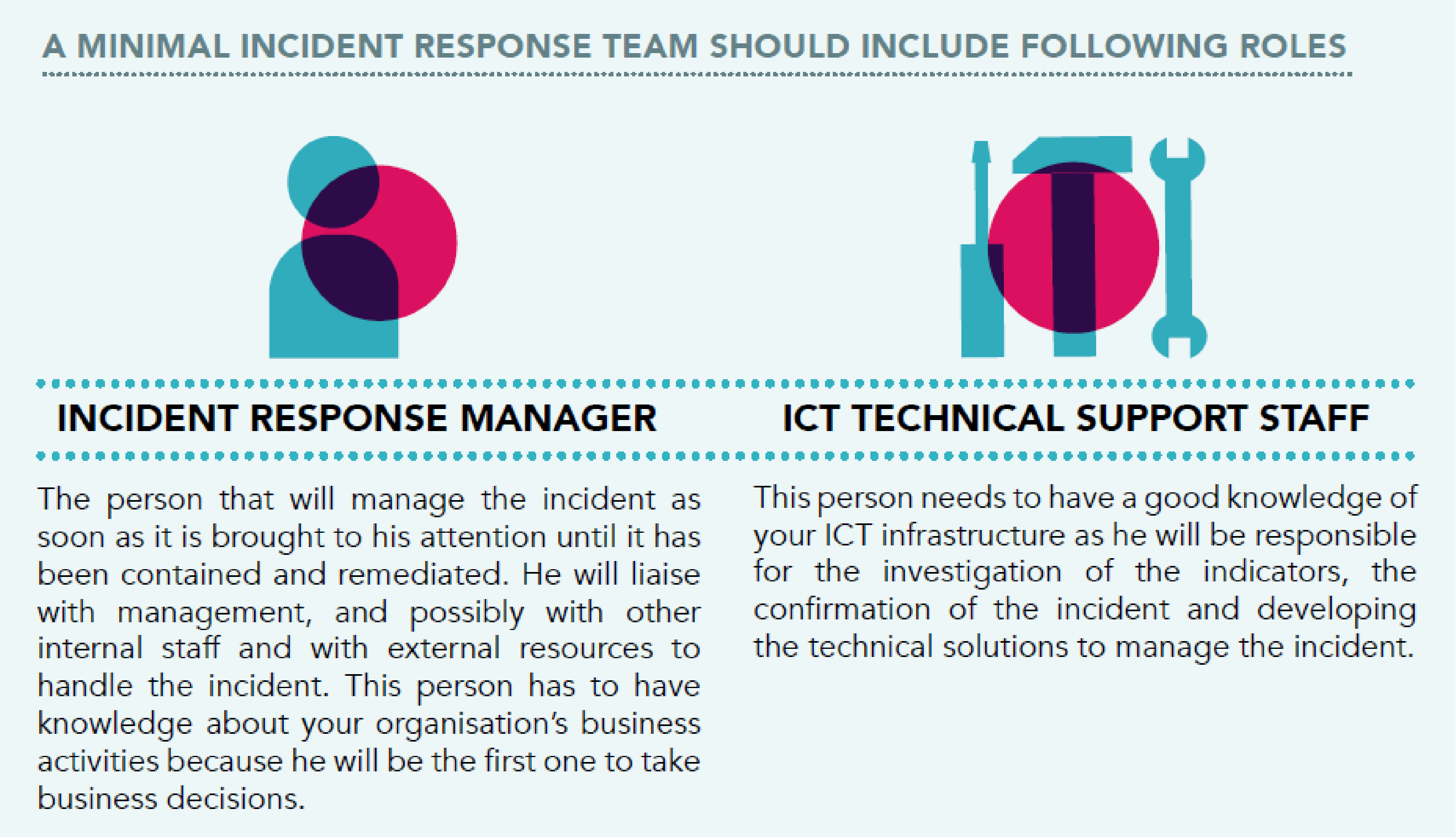
A. Identify the business and the resources that need to be protected

B. Determine what your crown jewels are

C. Assign business priorities for recovery

D. Document how your systems work and keep this documentation up to date

Incident Response Team



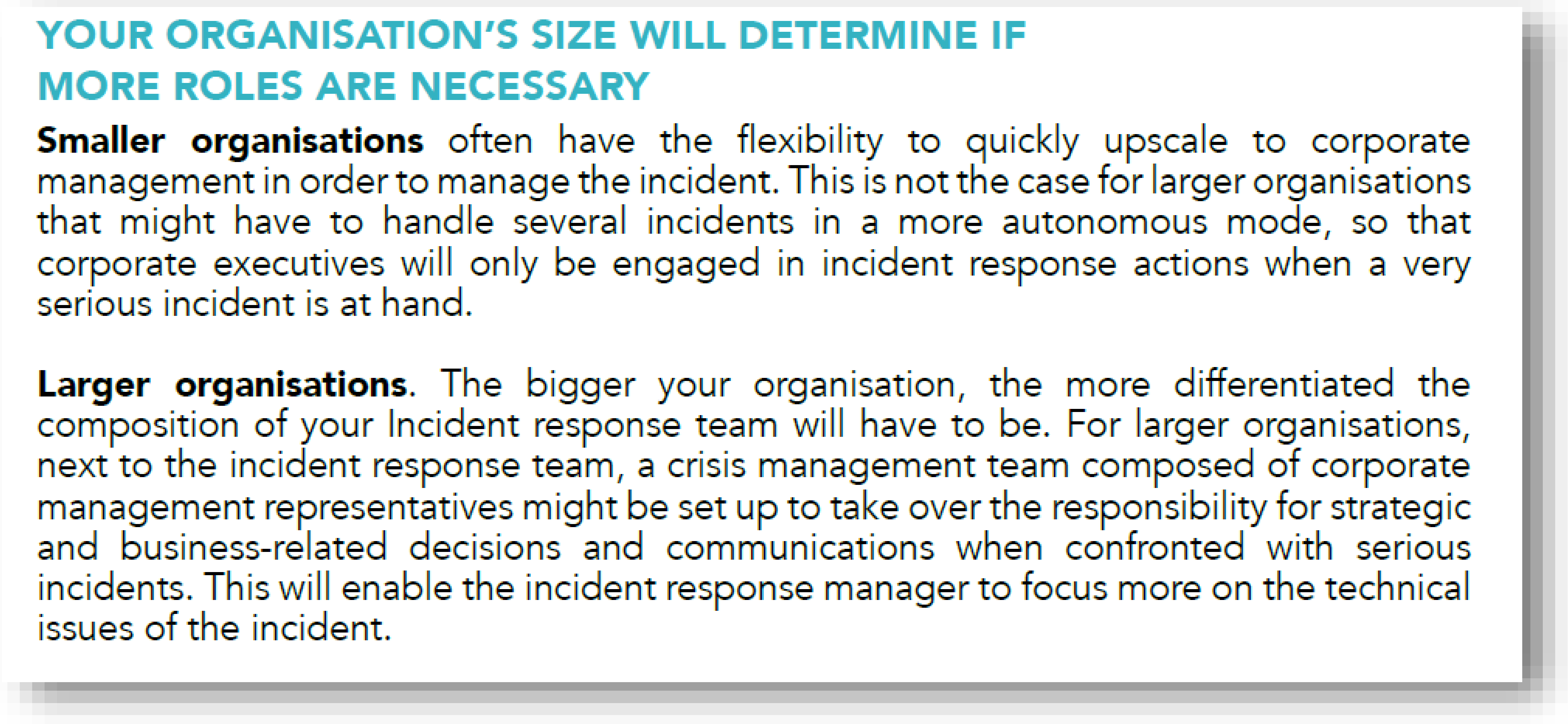
A MINIMAL INCIDENT RESPONSE TEAM SHOULD INCLUDE FOLLOWING ROLES

INCIDENT RESPONSE MANAGER

The person that will manage the incident as soon as it is brought to his attention until it has been contained and remediated. He will liaise with management, and possibly with other internal staff and with external resources to handle the incident. This person has to have knowledge about your organisation's business activities because he will be the first one to take business decisions.

ICT TECHNICAL SUPPORT STAFF

This person needs to have a good knowledge of your ICT infrastructure as he will be responsible for the investigation of the indicators, the confirmation of the incident and developing the technical solutions to manage the incident.

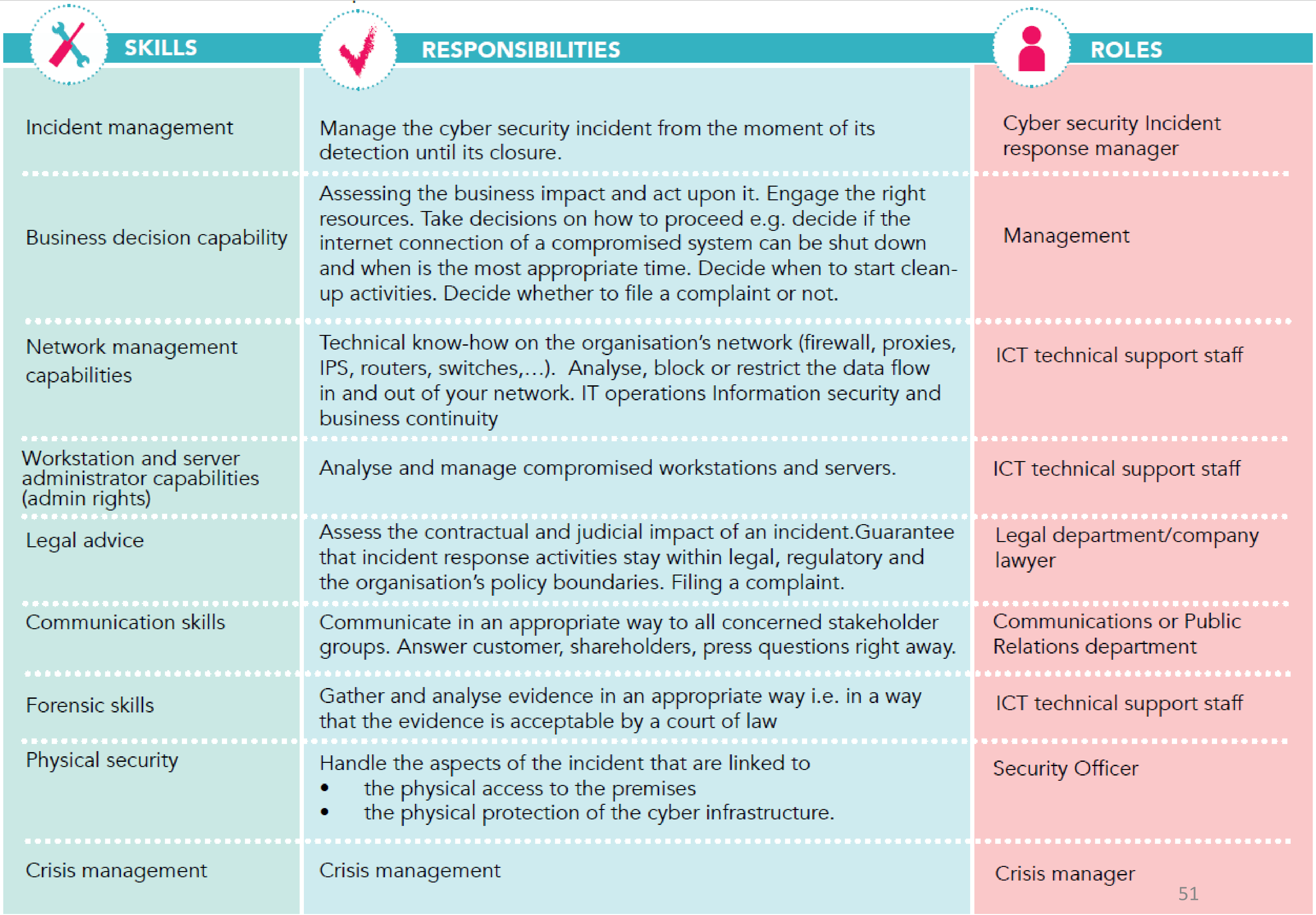


YOUR ORGANISATION'S SIZE WILL DETERMINE IF MORE ROLES ARE NECESSARY

Smaller organisations often have the flexibility to quickly upscale to corporate management in order to manage the incident. This is not the case for larger organisations that might have to handle several incidents in a more autonomous mode, so that corporate executives will only be engaged in incident response actions when a very serious incident is at hand.

Larger organisations. The bigger your organisation, the more differentiated the composition of your Incident response team will have to be. For larger organisations, next to the incident response team, a crisis management team composed of corporate management representatives might be set up to take over the responsibility for strategic and business-related decisions and communications when confronted with serious incidents. This will enable the incident response manager to focus more on the technical issues of the incident.

Skills



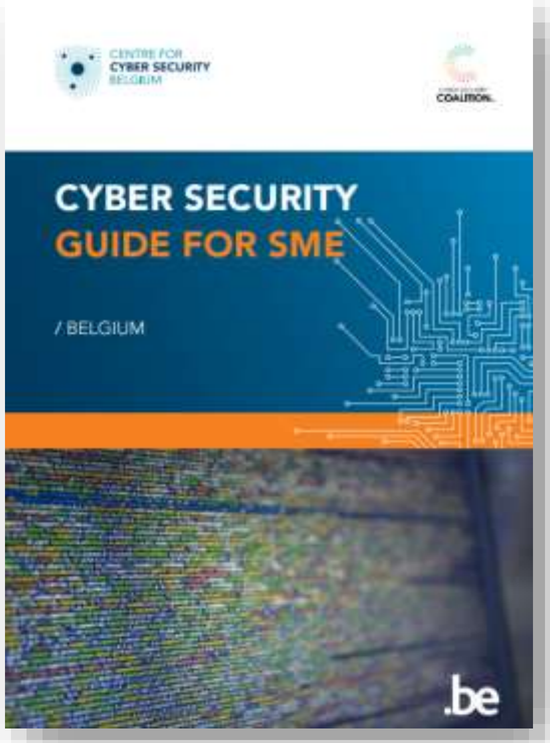
SKILLS	RESPONSIBILITIES	ROLES
Incident management	Manage the cyber security incident from the moment of its detection until its closure.	Cyber security Incident response manager
Business decision capability	Assessing the business impact and act upon it. Engage the right resources. Take decisions on how to proceed e.g. decide if the internet connection of a compromised system can be shut down and when is the most appropriate time. Decide when to start clean-up activities. Decide whether to file a complaint or not.	Management
Network management capabilities	Technical know-how on the organisation's network (firewall, proxies, IPS, routers, switches,…). Analyse, block or restrict the data flow in and out of your network. IT operations Information security and business continuity	ICT technical support staff
Workstation and server administrator capabilities (admin rights)	Analyse and manage compromised workstations and servers.	ICT technical support staff
Legal advice	Assess the contractual and judicial impact of an incident.Guarantee that incident response activities stay within legal, regulatory and the organisation's policy boundaries. Filing a complaint.	Legal department/company lawyer
Communication skills	Communicate in an appropriate way to all concerned stakeholder groups. Answer customer, shareholders, press questions right away.	Communications or Public Relations department
Forensic skills	Gather and analyse evidence in an appropriate way i.e. in a way that the evidence is acceptable by a court of law	ICT technical support staff
Physical security	Handle the aspects of the incident that are linked to • the physical access to the premises • the physical protection of the cyber infrastructure.	Security Officer
Crisis management	Crisis management	Crisis manager

BELGIAN CYBER SECURITY GUIDE

PROTECT YOUR INFORMATION

ICC FEB b-ccentre ISACA EY Microsoft

“Information security risk can be seen as the multiplication of three factors: assets, vulnerabilities and threats.”



CENTRE FOR CYBER SECURITY BELGIUM

COALITION

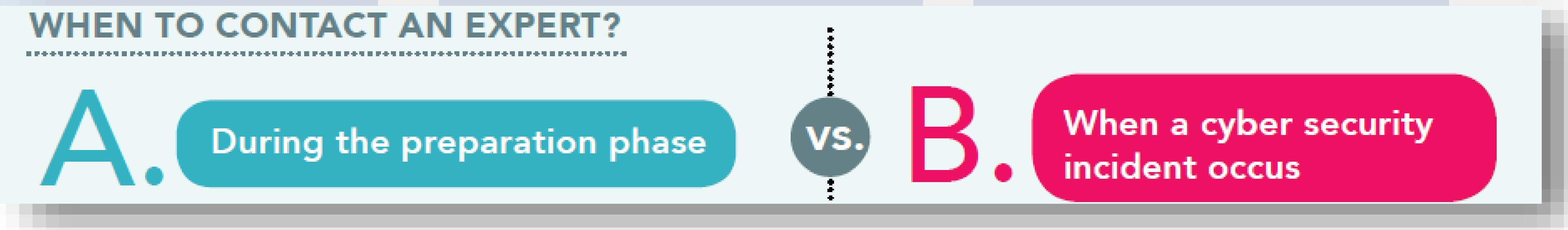
CYBER SECURITY GUIDE FOR SME

/ BELGIUM

.be

Additional expertise that may be required

Technical	Generic	Management
1. Malicious Code and Activity 2. Networks and Communications 3. PKI and Cryptography 4. Forensics and Investigation 5. Evolving technology: Clouds, IOT, Big Data 6. Web security 7. Payment systems Security 8. Mobile and wireless Security 9. Physical Environmental	1. Information Security Architecture 2. Privacy 3. Access Control (IAM) 4. Standards, Policies 5. Detection, Monitoring and Analysis (IDP) 6. Legal, compliance and regulatory 7. Incident and Crisis Response 8. Recovery activities 9. Business process controls 10. Data Loss Management	1. Organization, planning and frameworks 2. Risk analysis and mitigation 3. Security Operations and Administration 4. Awareness campaigns and communication 5. Disaster planning and Recovery 6. Skills, sourcing and third party



WHEN TO CONTACT AN EXPERT?

A. During the preparation phase

vs.

B. When a cyber security incident occus

Help from Authorities and Regulators

For Your Info

FCCU

economie

FOD Economie, K.M.O., Middenstand en Energie

CPVP

Commission de la protection de la vie privée

Assuralia

BIPT

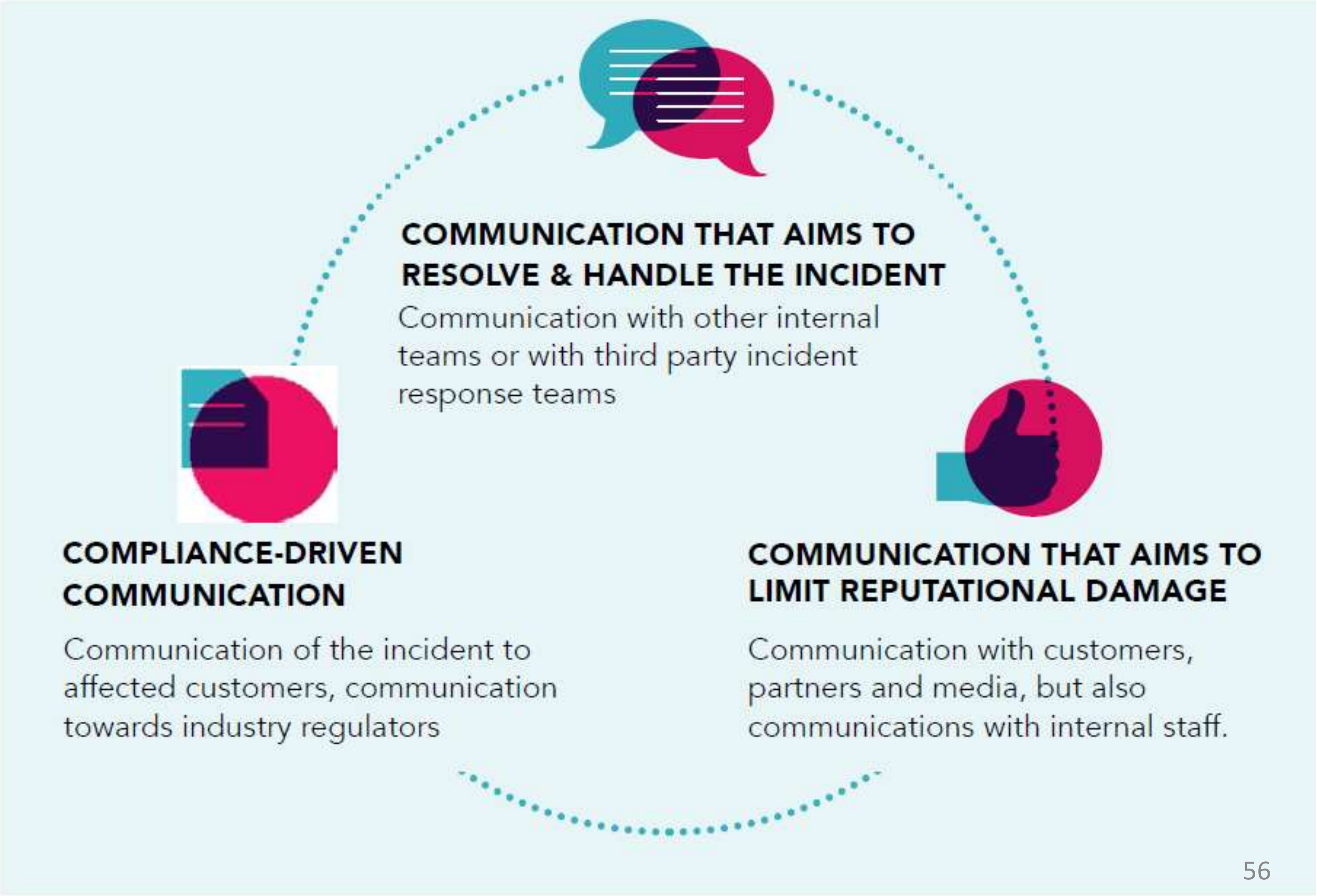
febelfin

CERT.be

The Federal Cyber Emergency Team

Communication

For Your Info



COMMUNICATION THAT AIMS TO RESOLVE & HANDLE THE INCIDENT

Communication with other internal teams or with third party incident response teams

COMPLIANCE-DRIVEN COMMUNICATION

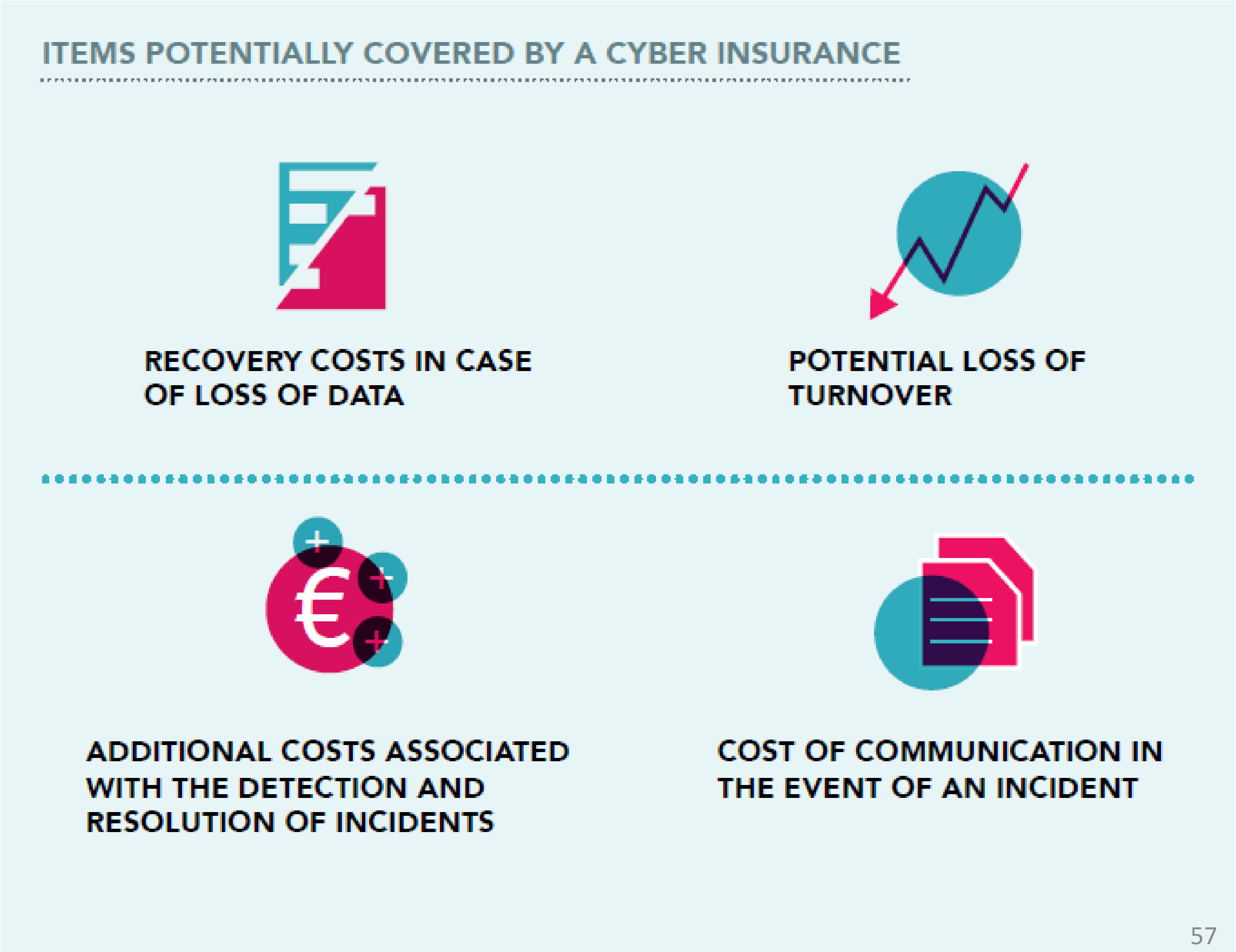
Communication of the incident to affected customers, communication towards industry regulators

COMMUNICATION THAT AIMS TO LIMIT REPUTATIONAL DAMAGE

Communication with customers, partners and media, but also communications with internal staff.

Insurance

For Your Info



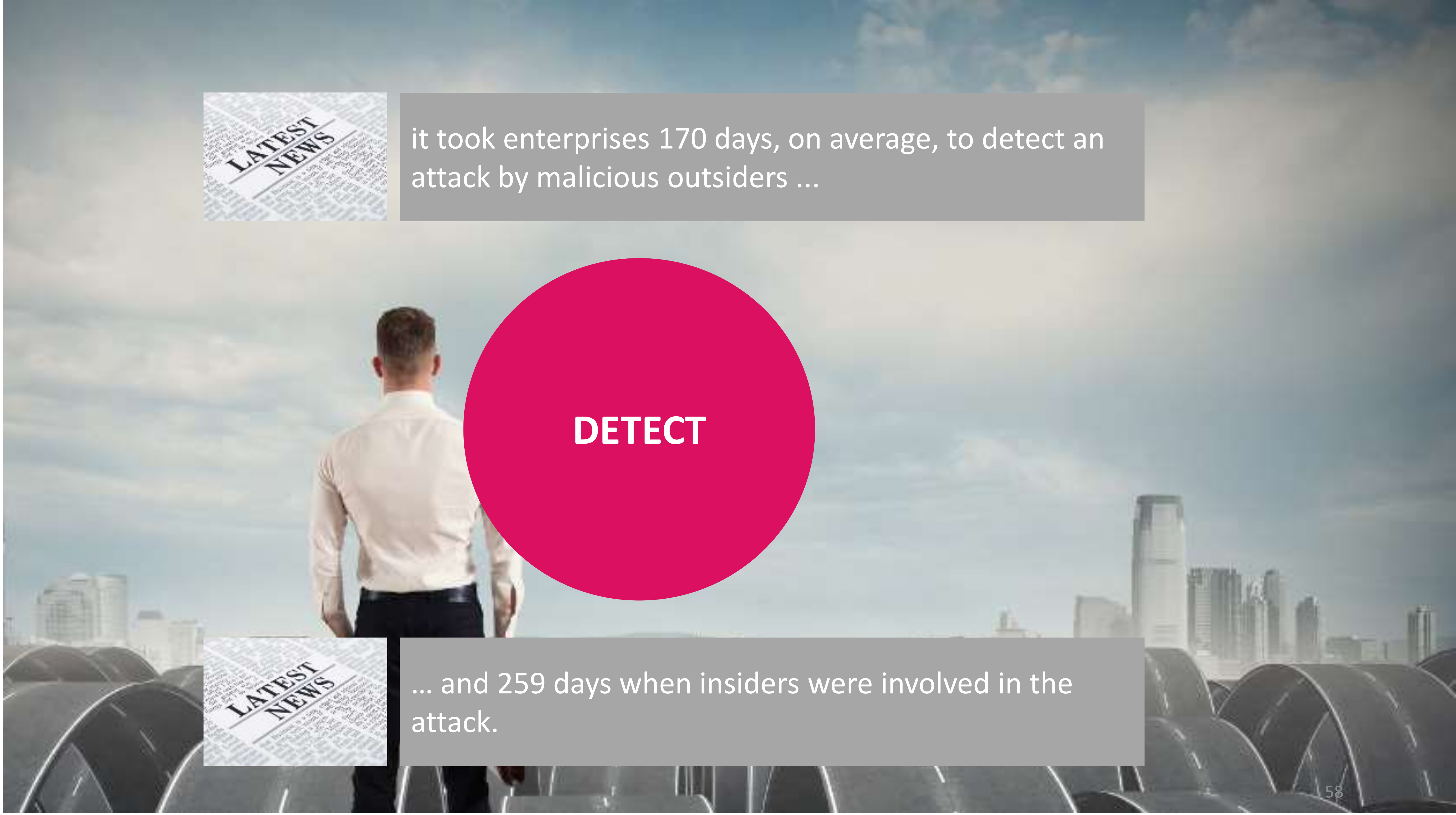
ITEMS POTENTIALLY COVERED BY A CYBER INSURANCE

RECOVERY COSTS IN CASE OF LOSS OF DATA

POTENTIAL LOSS OF TURNOVER

ADDITIONAL COSTS ASSOCIATED WITH THE DETECTION AND RESOLUTION OF INCIDENTS

COST OF COMMUNICATION IN THE EVENT OF AN INCIDENT



it took enterprises 170 days, on average, to detect an attack by malicious outsiders ...

DETECT

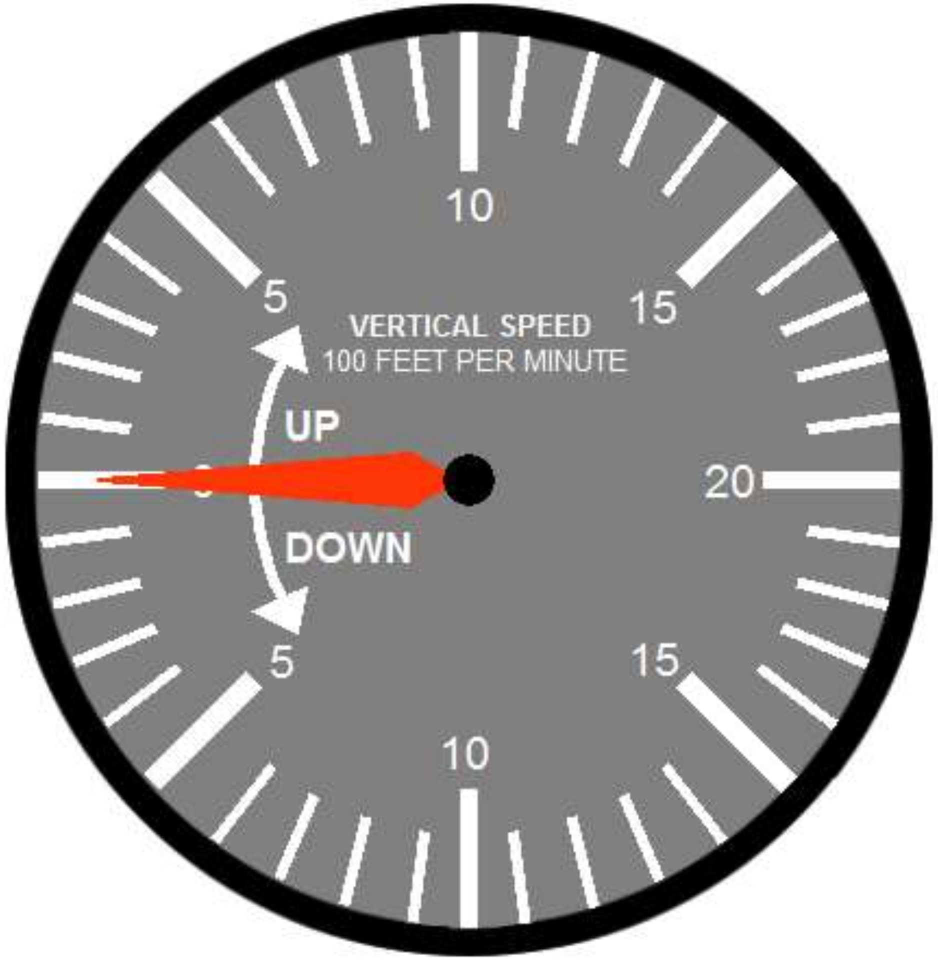
... and 259 days when insiders were involved in the attack.

Indicator(s)

An indicator is any piece of information that objectively describes an intrusion.

The concept is based on the assumption that many aspects of an APT, such as IP addresses, exploits and malware code, are likely to be reused in future attacks.

Once the complete kill chain is understood, then detecting just one aspect of an attack could be sufficient to identify and mitigate other aspects of the attack



Your organisation's personnel has Potential to detect

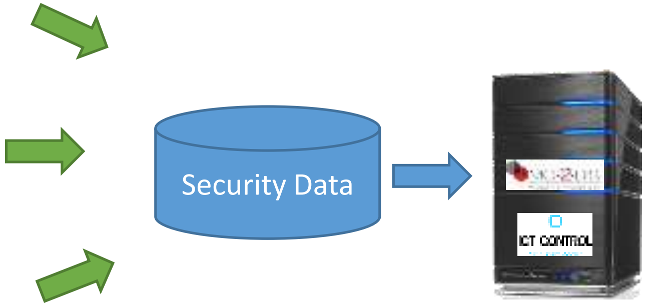
Detection Tools

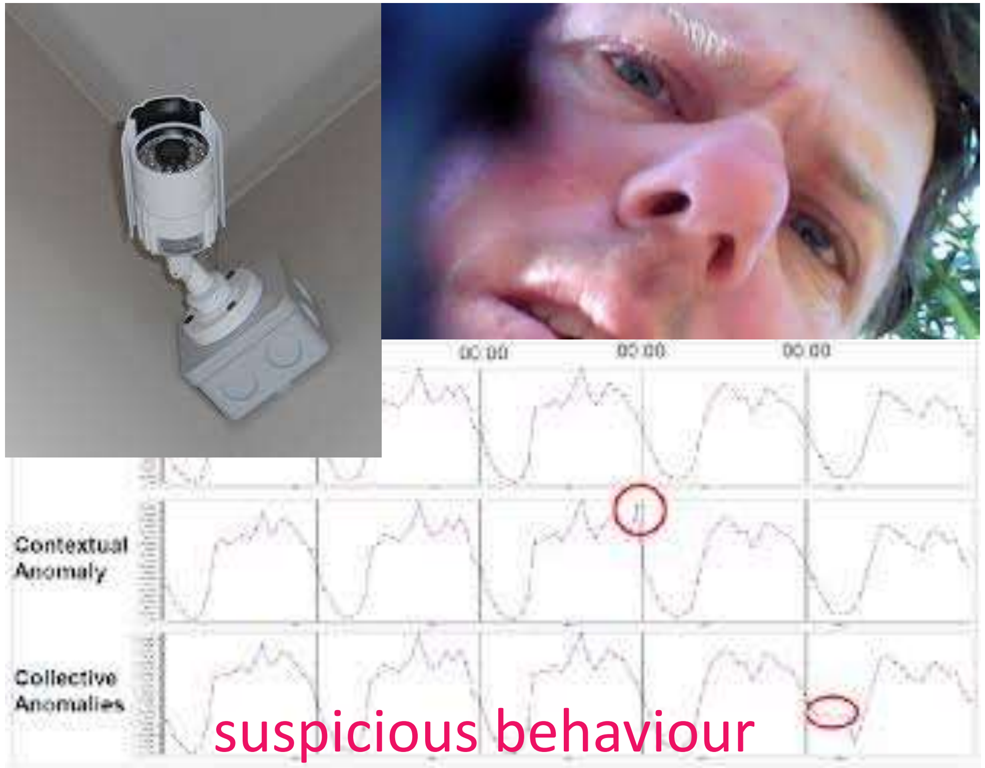
For Your Info

access logs to servers and appliances;

operational logs from systems (e.g. process creation);

firewall policy logs.





suspicious behaviour

NETWORK PERSPECTIVE

HOST PERSPECTIVE

CONTAIN

ERADICATE

RESPOND

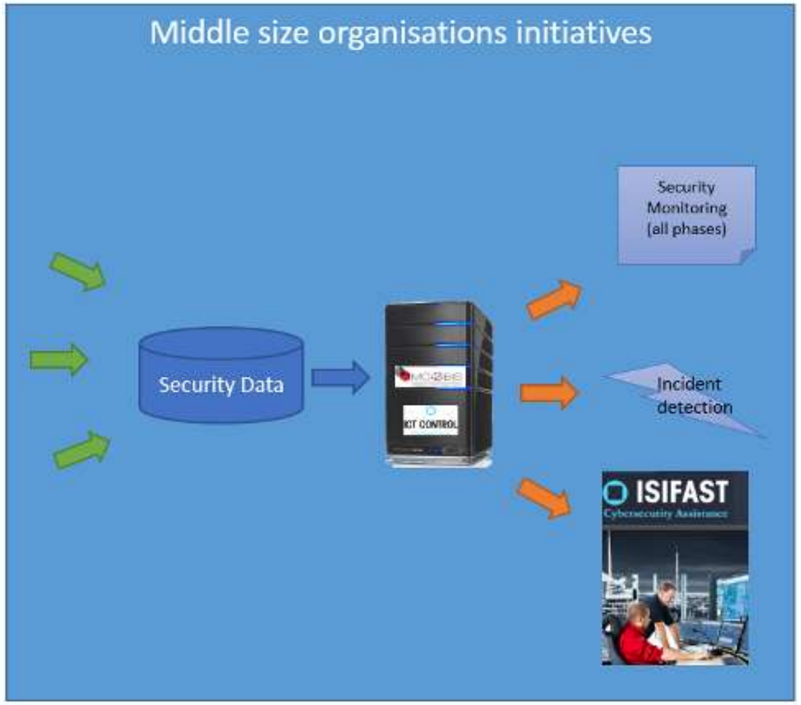
RECOVER

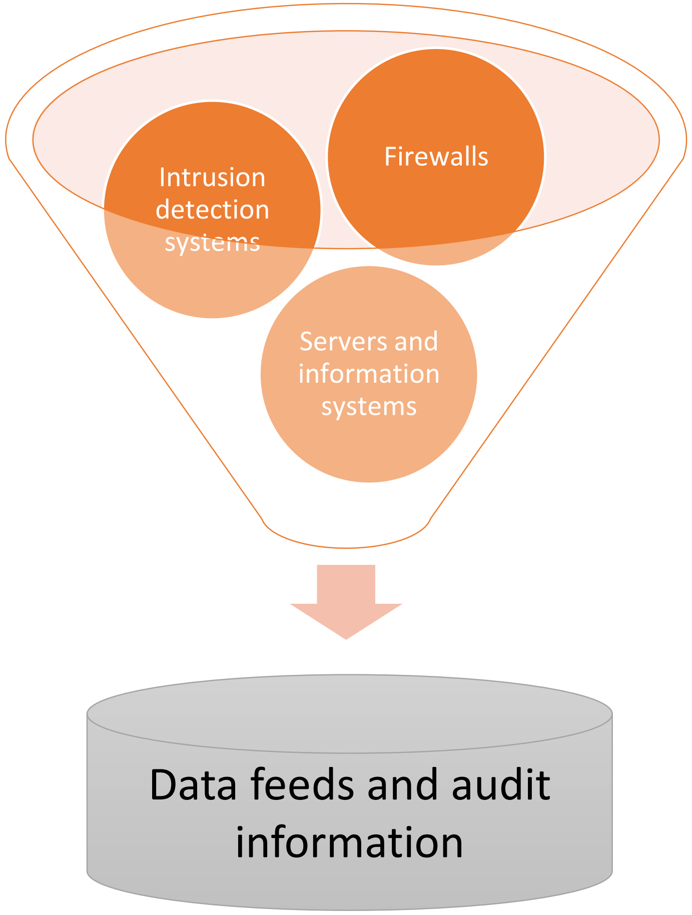
RESPOND

Creating a SOC:

Security Operations Center

Centrally located facility designed to monitor the security of an enterprise’s IT infrastructure and information systems



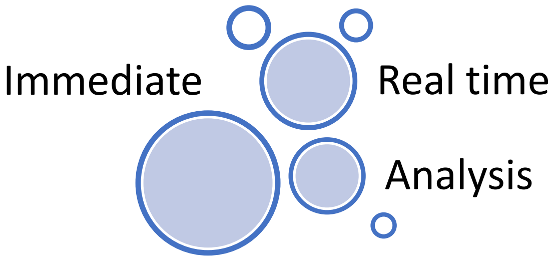


Intrusion detection systems

Firewalls

Servers and information systems

Data feeds and audit information



Immediate

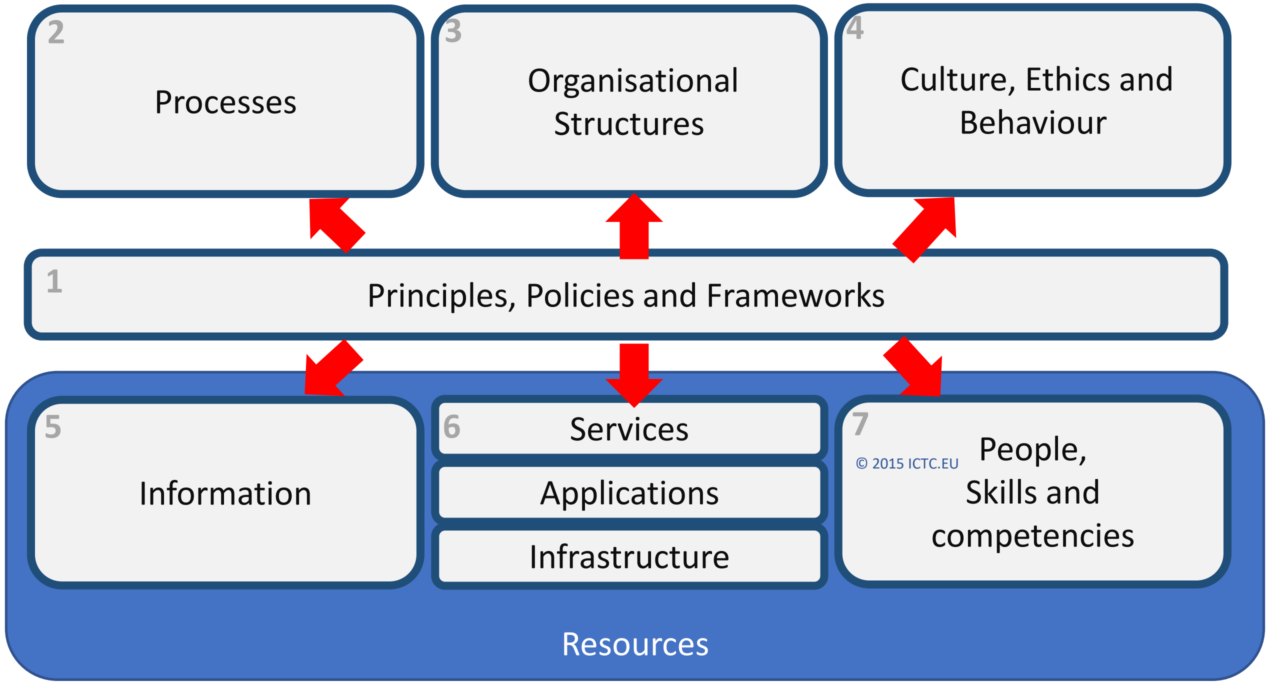
Real time

Analysis

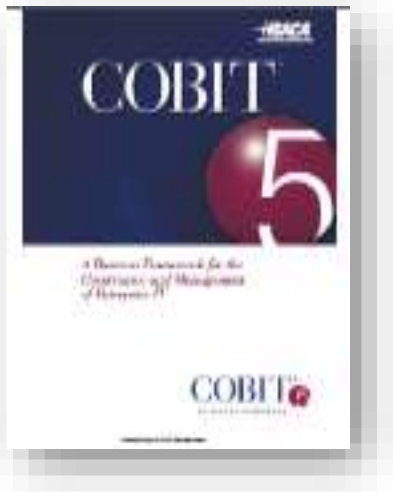
RESPOND

Enablers for cyber security incident management

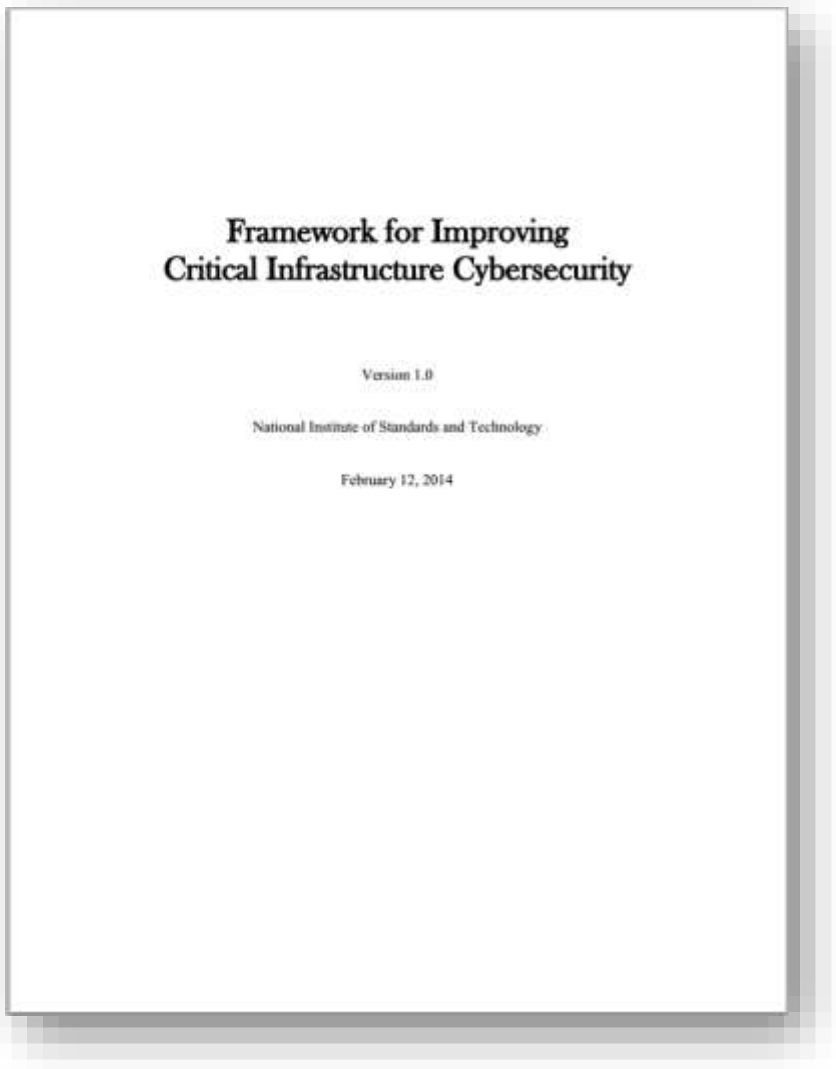
For Your Info


2
Processes
3
Organisational Structures
4
Culture, Ethics and Behaviour
1
Principles, Policies and Frameworks
5
Information
6
Services
Applications
Infrastructure
7
© 2015 ICTC.EU
People, Skills and competencies
Resources

© 2015 ICTC.EU



Cyber-Security Processes



Framework for Improving
Critical Infrastructure Cybersecurity

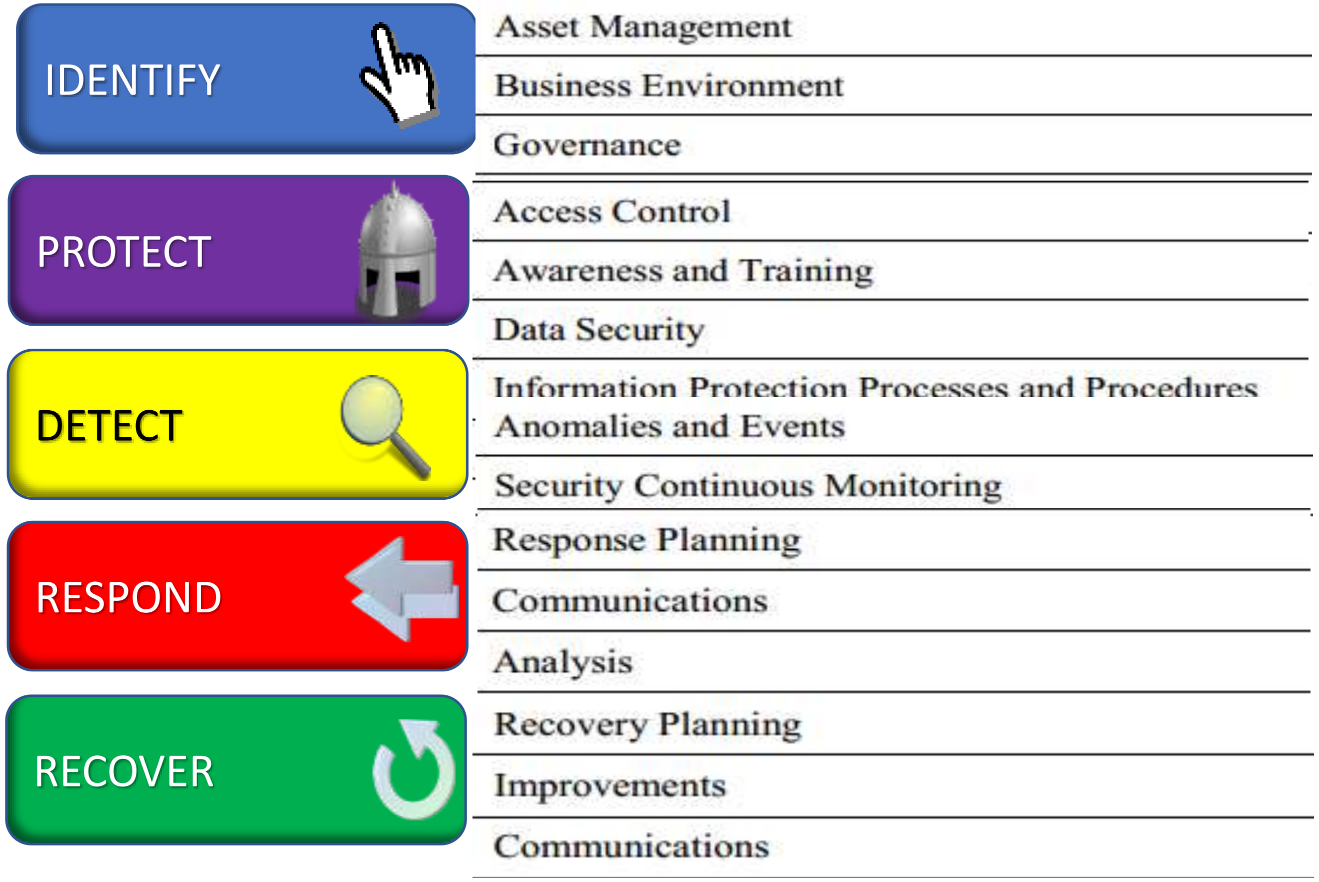
Version 1.0

National Institute of Standards and Technology

February 12, 2014

Functions

Develop and implement



IDENTIFY
- Asset Management
- Business Environment
- Governance

PROTECT
- Access Control
- Awareness and Training
- Data Security
- Information Protection Processes and Procedures

DETECT
- Anomalies and Events
- Security Continuous Monitoring

RESPOND
- Response Planning
- Communications
- Analysis

RECOVER
- Recovery Planning
- Improvements
- Communications

Questions ??