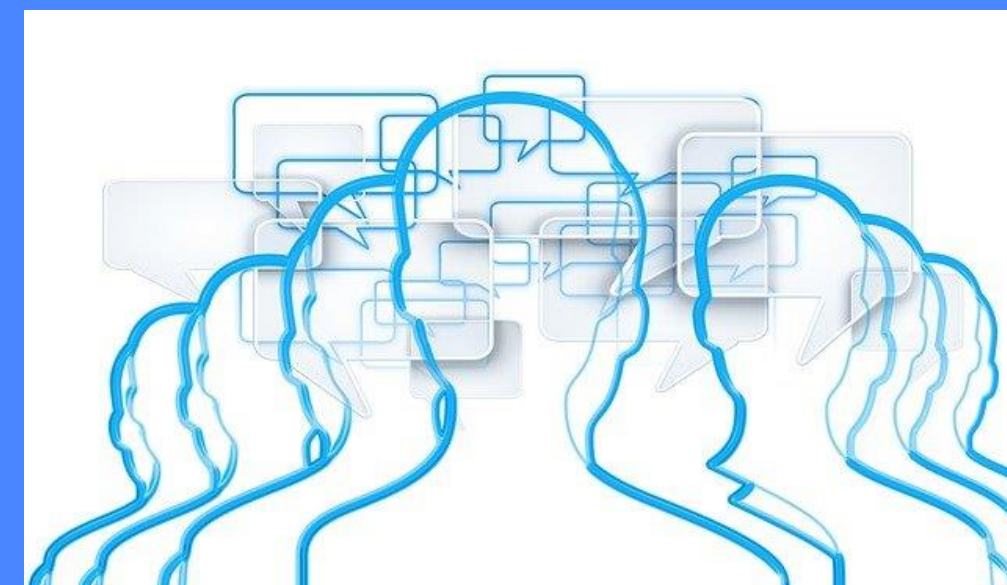




GRC Be Connected

Information Security Management

23 March 2021



Programme

Time	Topic	Speaker
10:00 am -10:05 am	Welcome	Prof. Georges Ataya Vice-chairman Cyber Security Coalition
10:05 am - 10:35 am	The real strategic value of CISM	Mr. Marc Vael CISO ESKO
10:35 am – 11:15 am	Practical implemental of security in critical infrastructures (hospitals)	Mr. Taco Mulder CISO CHU-UVC Brugmann - HUDERF
11:15 am -11:55 am	Why and how implement an information security management system?	Mr. Gaël Hachez Director Cyber & Privacy Department PwC Belgium
11:55 am - noon	Wrap-up & closure of the meeting	Prof. Georges Ataya Vice-chairman Cyber Security Coalition

Marc Vael
CISO
Esko



My experience as CISO managing information security

Marc Vael

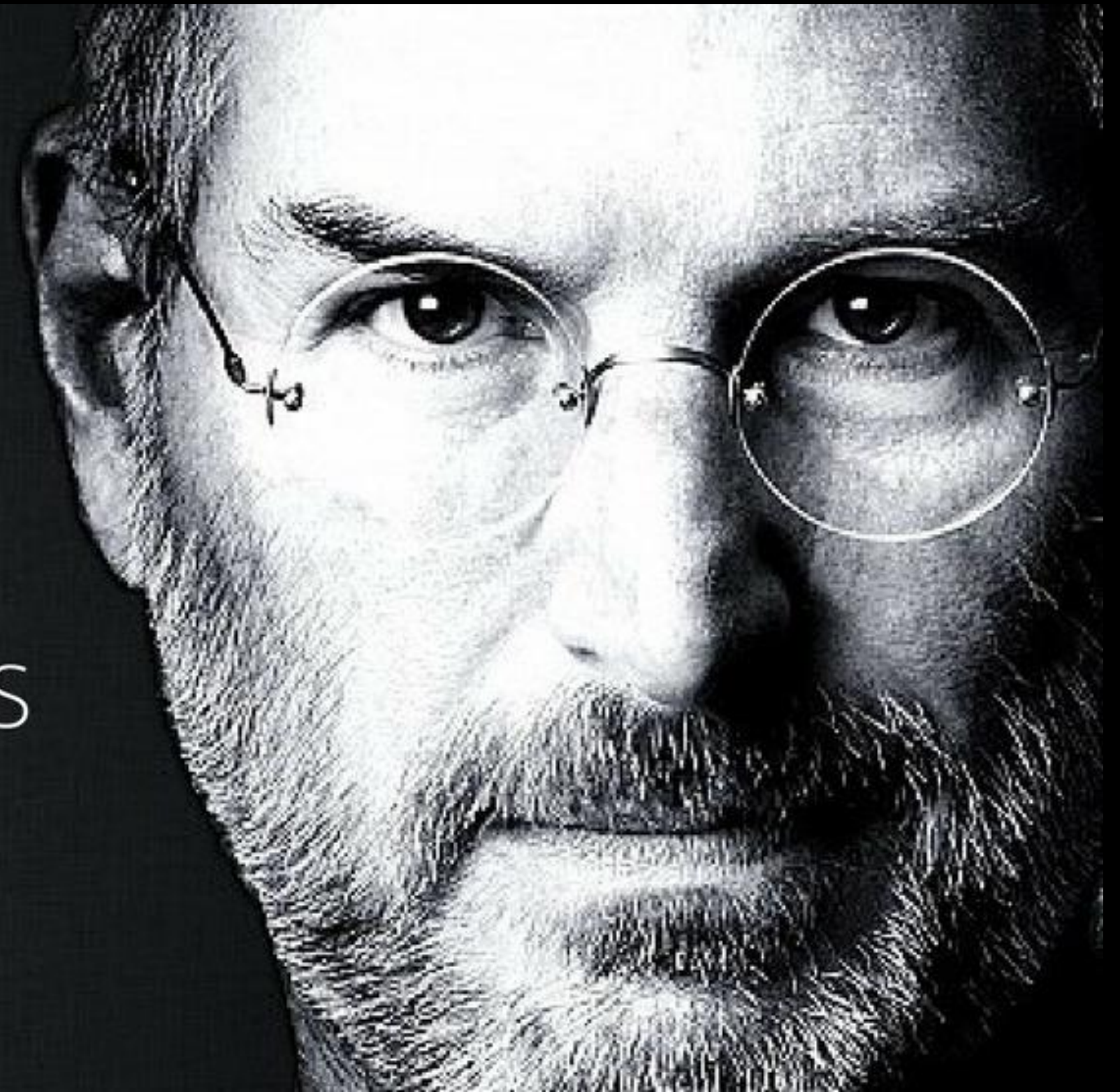
Tuesday 23rd of March 2021

How to become a CISO

1. Self-analysis

“THE ONLY WAY TO DO GREAT
WORK IS TO LOVE WHAT YOU DO.
IF YOU HAVEN'T FOUND IT YET,
KEEP LOOKING. DON'T SETTLE.”

STEVE JOBS



How to become a CISO

1. Self-analysis



How to become a CISO

2. Education

**ONCE YOU EDUCATE
YOURSELF, YOU'RE LEFT
WITH CHOICES**

YVON CHOUINARD

How to become a CISO

2. Education



How to become a CISO

3. Career path





QUALITY CONTROL

The IBM logo, consisting of the letters 'IBM' in a bold, sans-serif font with horizontal stripes.

CYBER
SECURITY
CONSULTING
SERVICES



ARTHUR
ANDERSEN





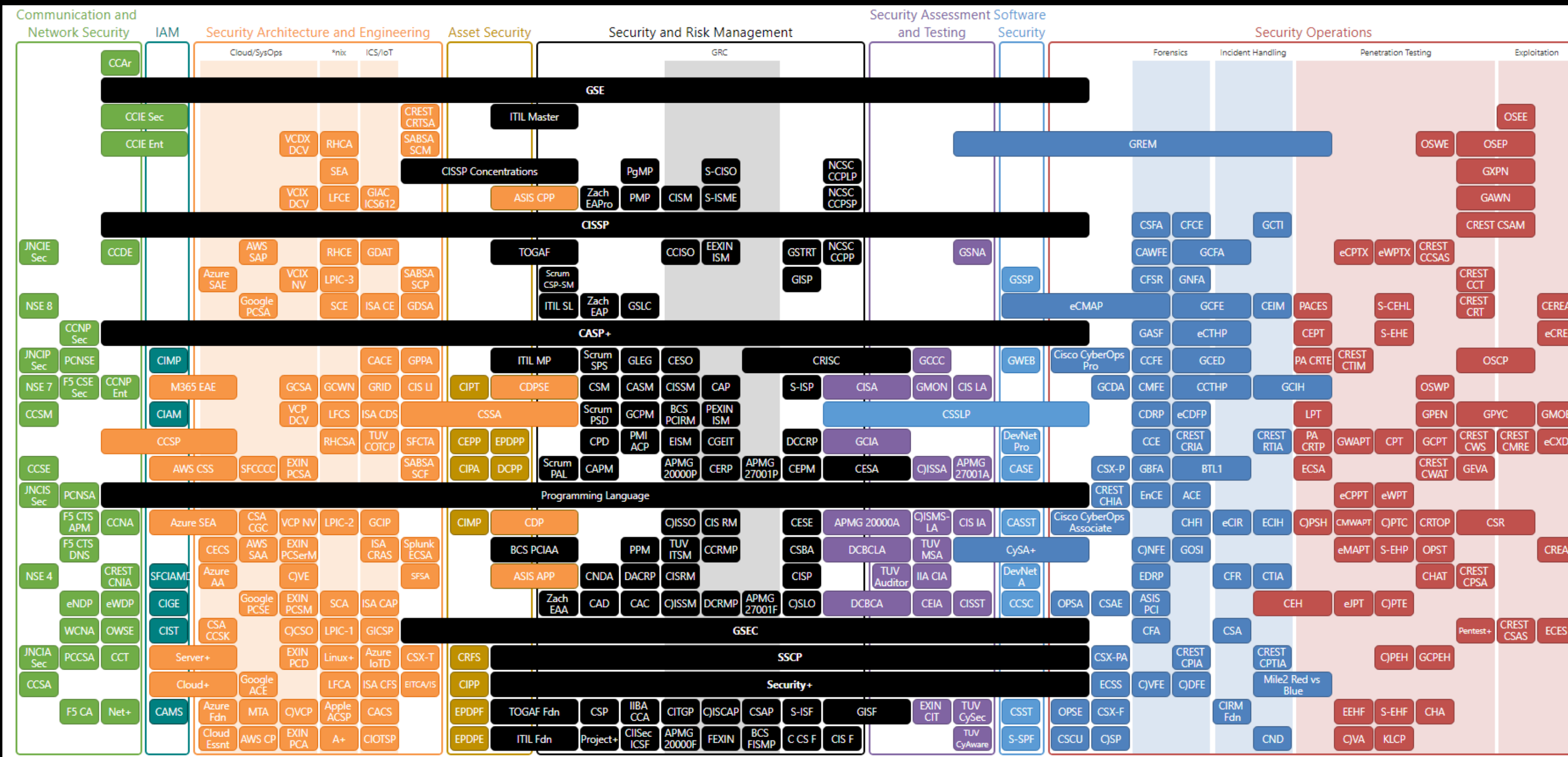
CHIEF INFORMATION SECURITY OFFICER

ESKO 



How to become a CISO

4. Professional certifications



How to become a CISO

4. Professional certifications



Certified Information
Systems Security Professional

1994

C
Certified

CISO
**Chief Information
Security Officer**

2003



2004



Certified Information Security Manager®

An ISACA® Certification



INFORMATION SECURITY
GOVERNANCE

INFORMATION RISK MANAGEMENT

INFORMATION SECURITY
PROGRAM DEVELOPMENT &
MANAGEMENT

INFORMATION
SECURITY INCIDENT
MANAGEMENT

Information Security Governance

Establish and/or maintain
an information security governance
framework & supporting processes
to ensure that
the information security strategy **is aligned**
with organizational goals & objectives.

Information Risk Management

Manage
information risk
to **an acceptable level**
based on **risk appetite**
in order to **meet**
organizational goals & objectives.

Information Security Program Development & Management

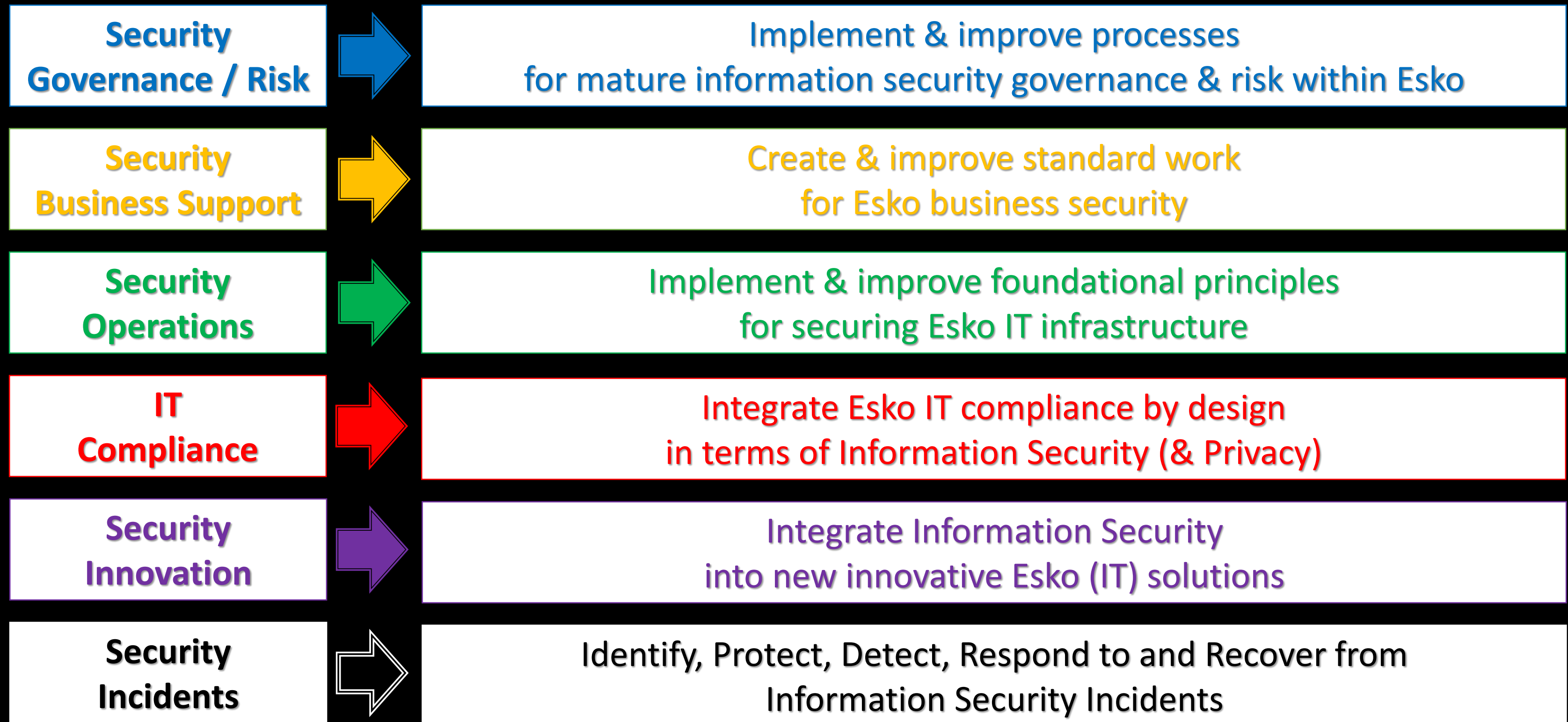
Develop & maintain
an information security program that
identifies, manages and protects
the organization's **assets** while **aligning**
to information security strategy & business
goals, thereby
supporting an effective **security posture.**

Information Security Incident Management

Plan, establish and manage
the capability
to detect, investigate, respond to and
recover from
information security incidents
to minimize business impact.

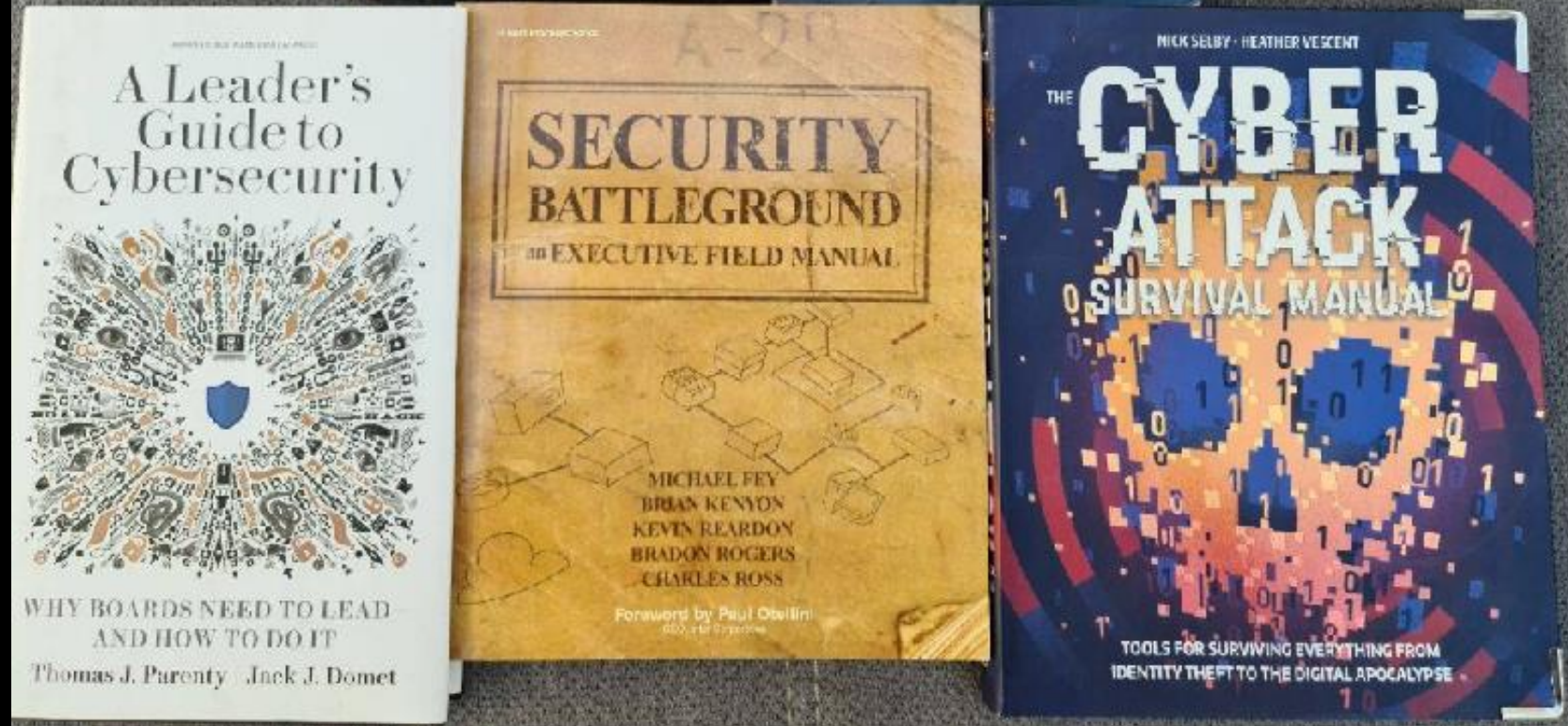
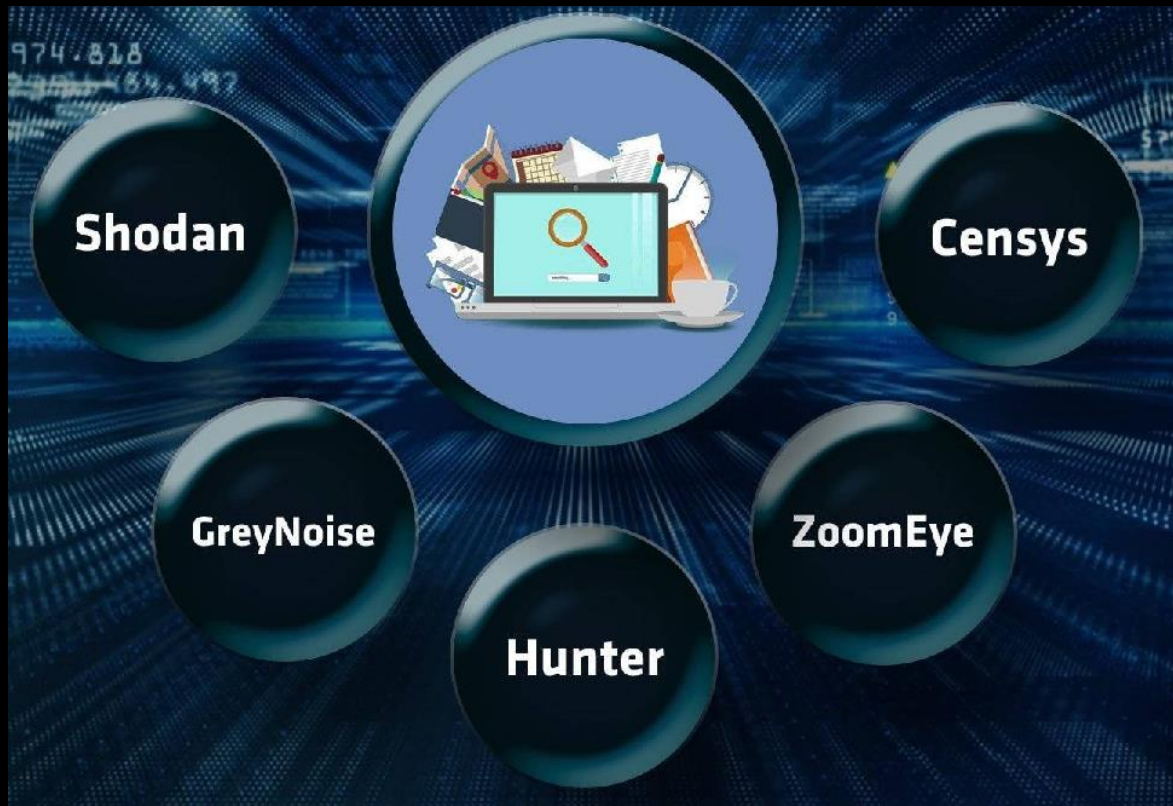
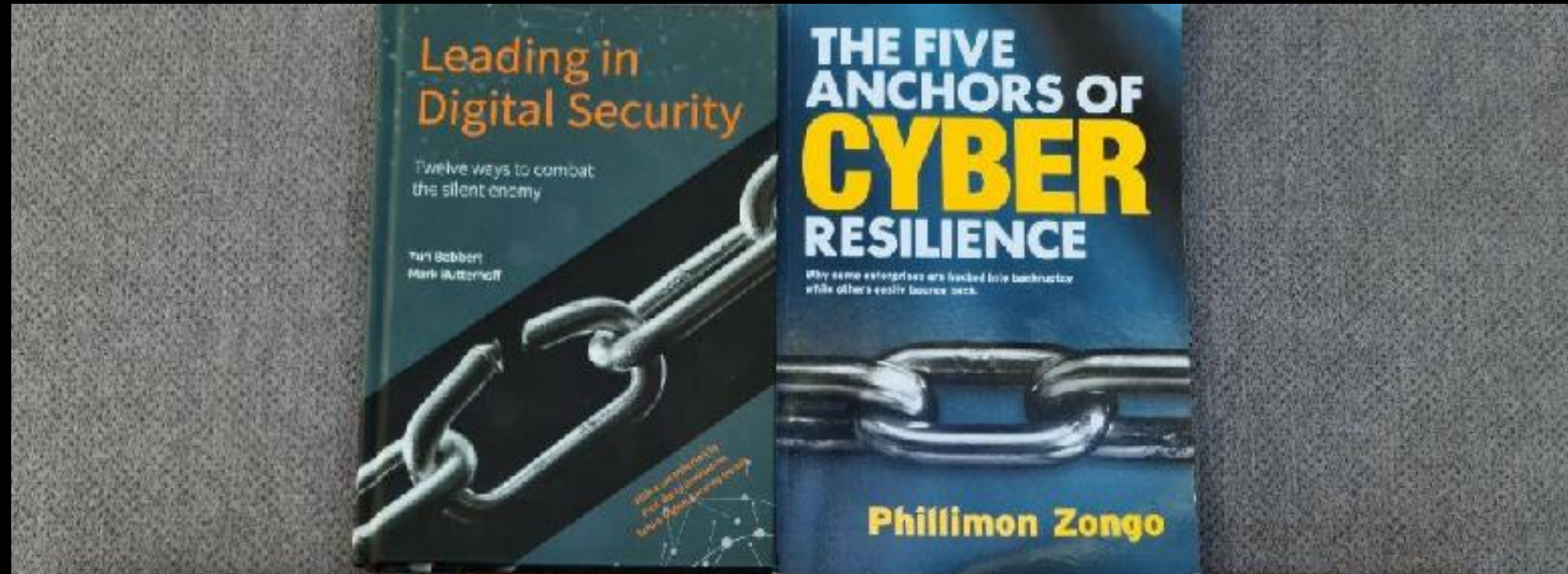
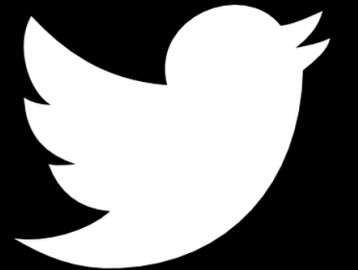


Information Security Management

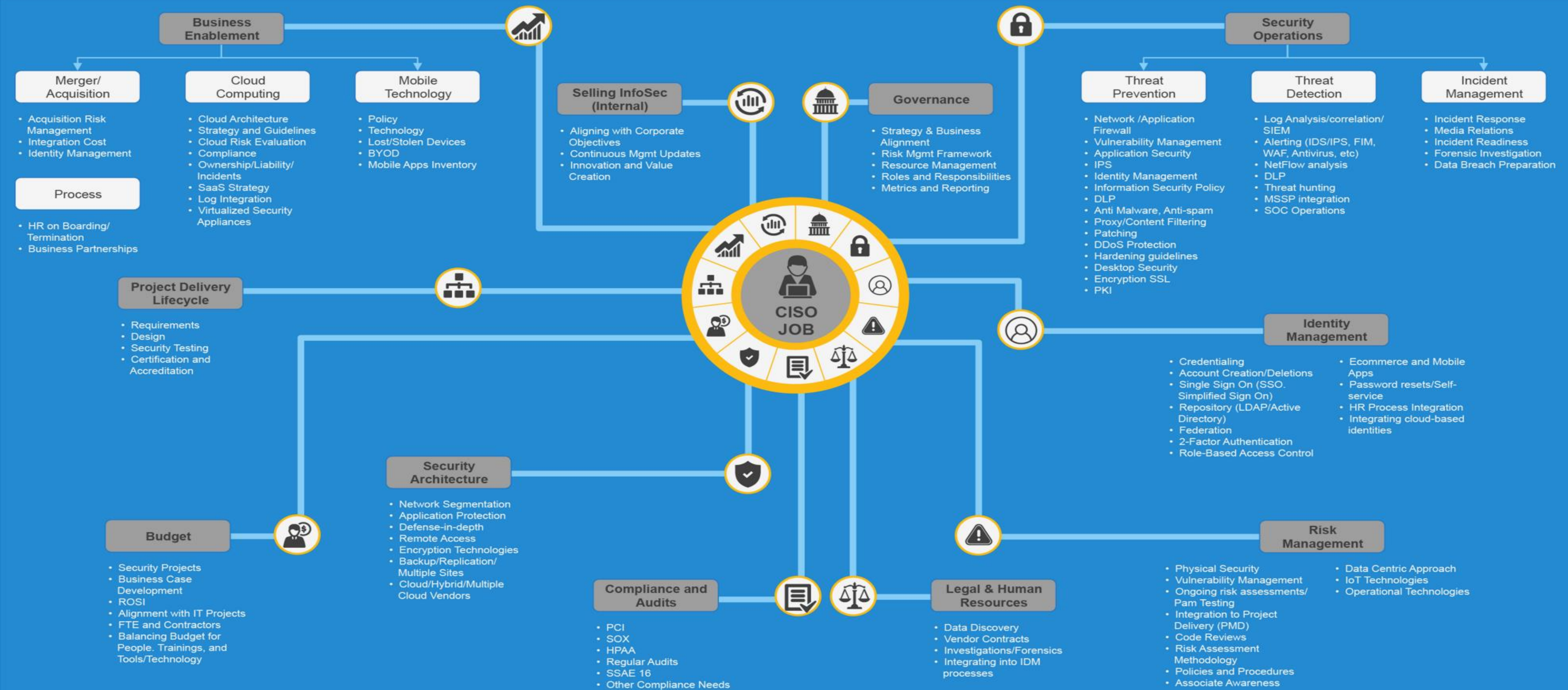


How to become a CISO

5. Keep current



CISO Mind Map: An Overview of The Responsibilities and Ever Expanding Role of The CISO



Chief Information Security Officer

Success formula:

4C x **3I** x **2S** x **0**

4C = Complexity + Culture + Communication + Collaboration


3I = Information + Interconnectiveness + Initiative

2S = Strategy + Security

0 = Optimization



Stephane Nappo, VP & Global CISO, Groupe SEB



If I do a job in **30 minutes**,
it's because I spend **10 years**
learning how to do that in 30
minutes. You owe me for the
years **not the minutes.**

Contact details

Mr. Marc Vael, CISM, CISSP, CRISC, CGEIT, ITIL SM, Guberna Certified Director

CISO

Esko

President

SAI

 **marc.vael@sai.be**

 **<http://www.linkedin.com/in/marcvael>**

 **[@marcvael](https://twitter.com/marcvael)**

A middle-aged man with glasses and a light blue short-sleeved button-down shirt is pushing a metal wire cart in a hospital hallway. He is wearing a dark lanyard with a white ID badge around his neck and a dark watch on his left wrist. The hallway has white walls, a whiteboard on a stand in the background, and a black wheelchair to the right. The lighting is bright and clinical.

Taco Mulder
CISO CHU-UVC
Brugmann & HUDERF

Practical implemental of security in critical infrastructures (hospitals)

- WHY?

Business Risk!

Who are at risk:

- Patients
- Employees
- Hospitals



Impact

Attacks on hospitals

18/01/21 Centre Hospitalier Wallonie Picarde (CHWAPI)

02/02/21 Heilig Hartziekenhuis in Mol

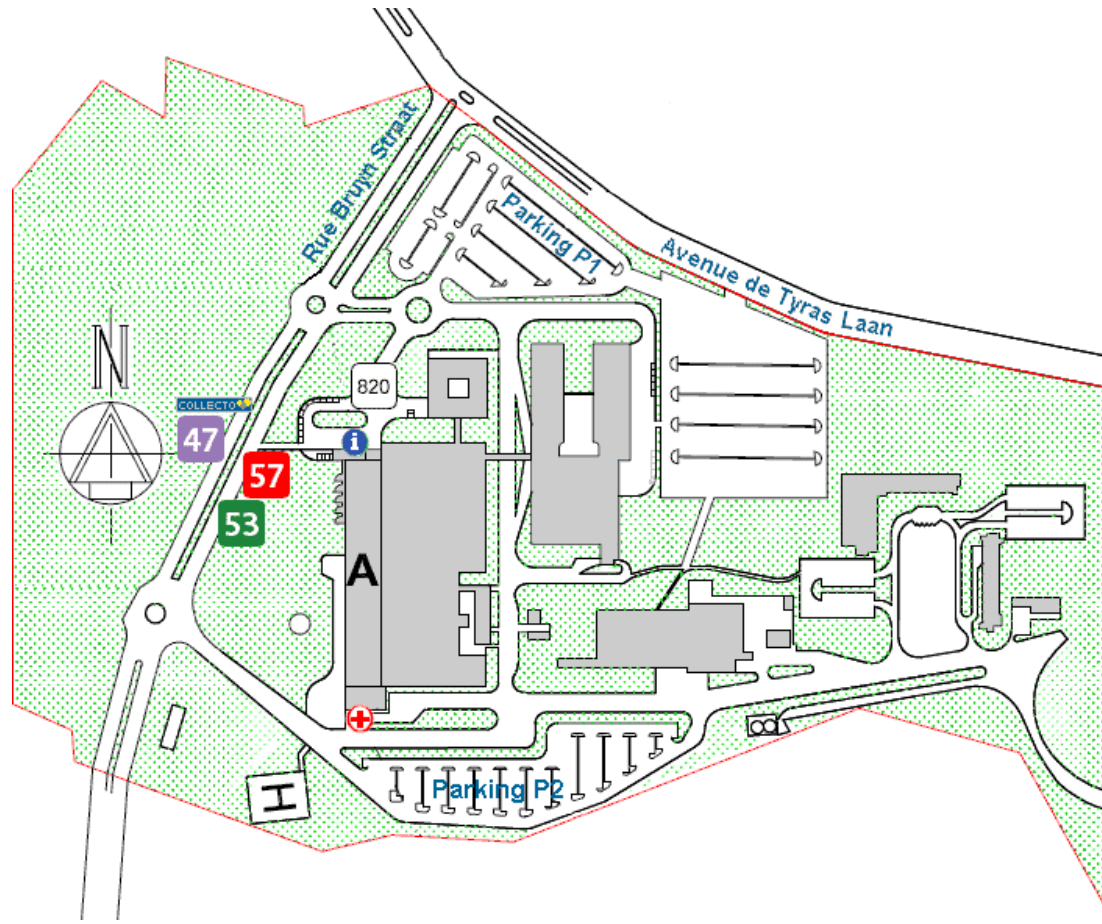
- Cyber threats on the healthcare system are increasing and need to be addressed with priority from our governments as the lives of the patients are on the line.



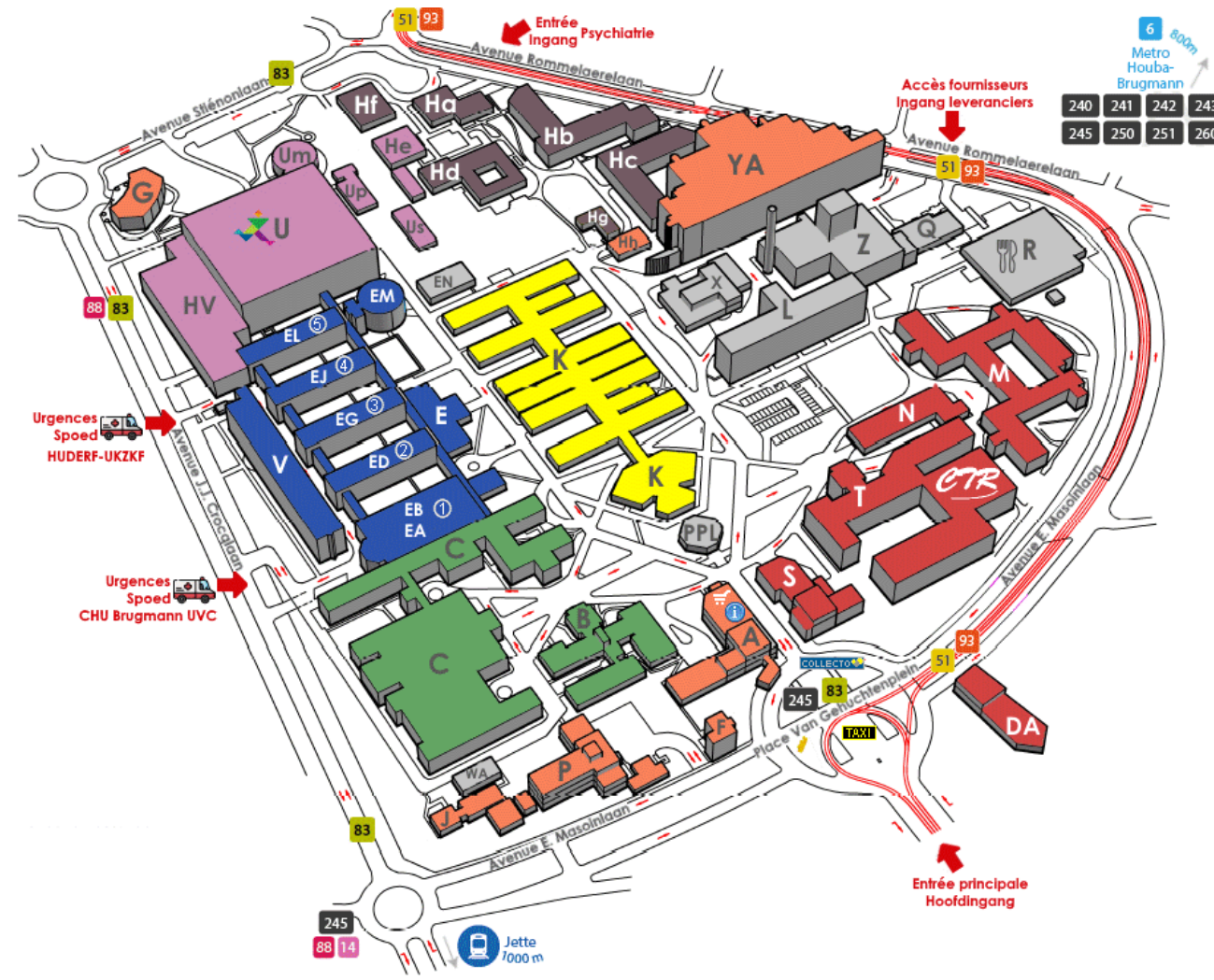
- Healthcare organizations collect and store vast amounts of personal information, making them a major target for cyber-criminals. This valuable data can be used for identity theft

“my” hospitals

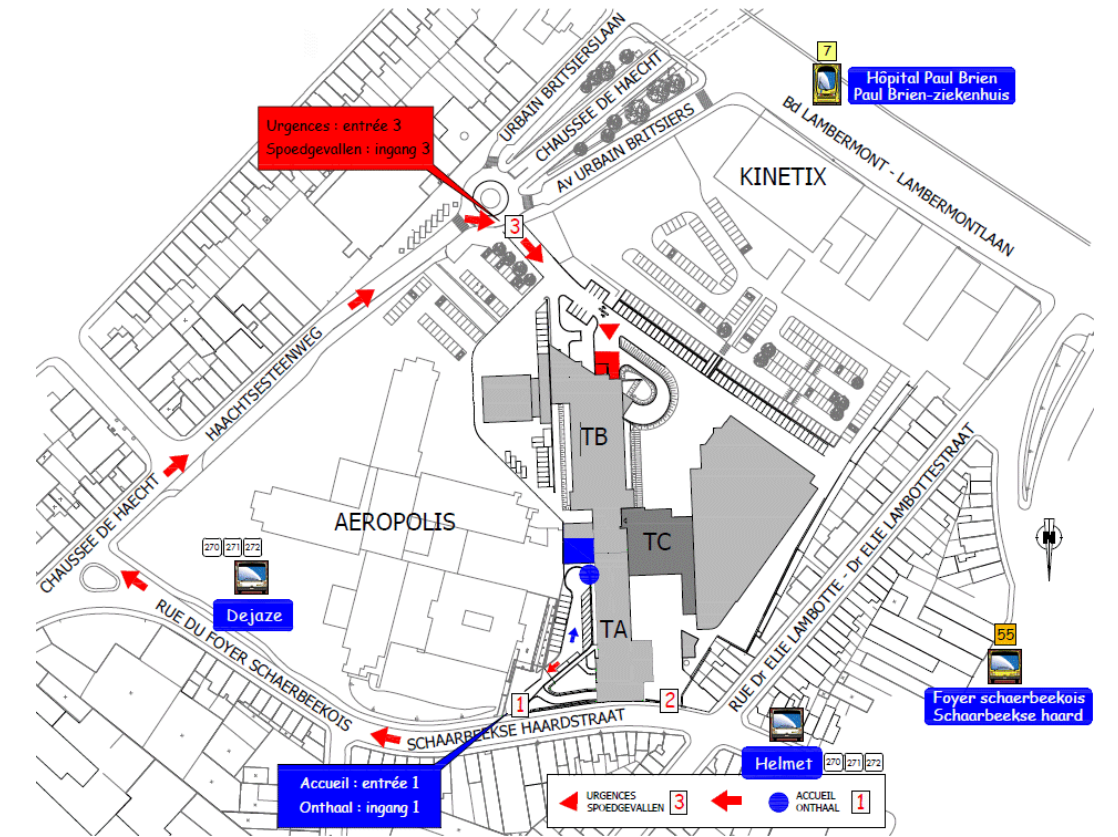
3 sites



Queen Astrid Military Hospital
Neder-Over-Heembeek



HORTA:
- CHU/UVC Brugmann
- HUDERF/UKZKF
Laken



Paul Brien Hospital
Schaerbeek

Information Security Governance

COBIT 2019 Design Factors

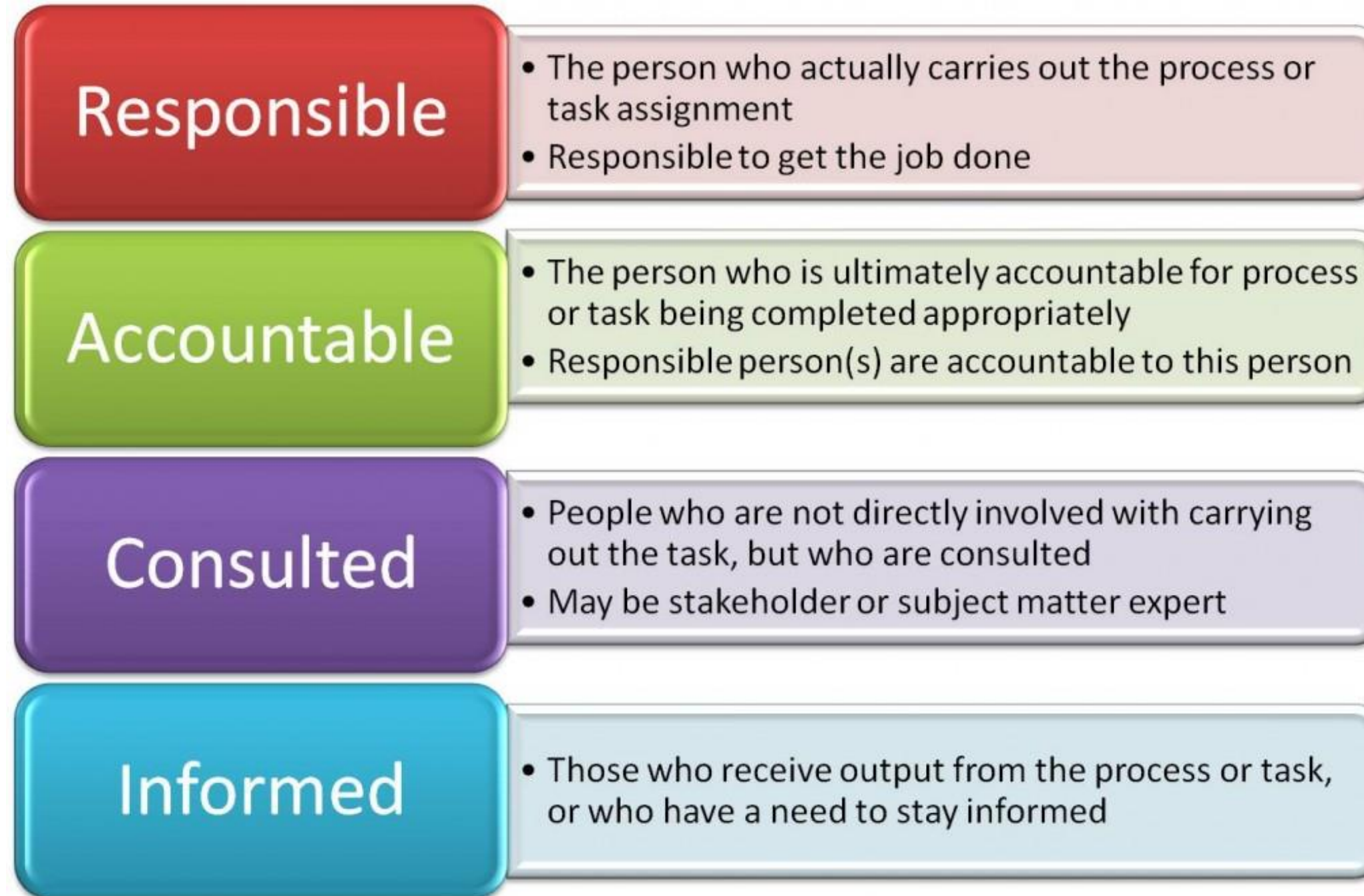


Information Security Governance

NIST Cybersecurity Framework Overview



Information Security Governance

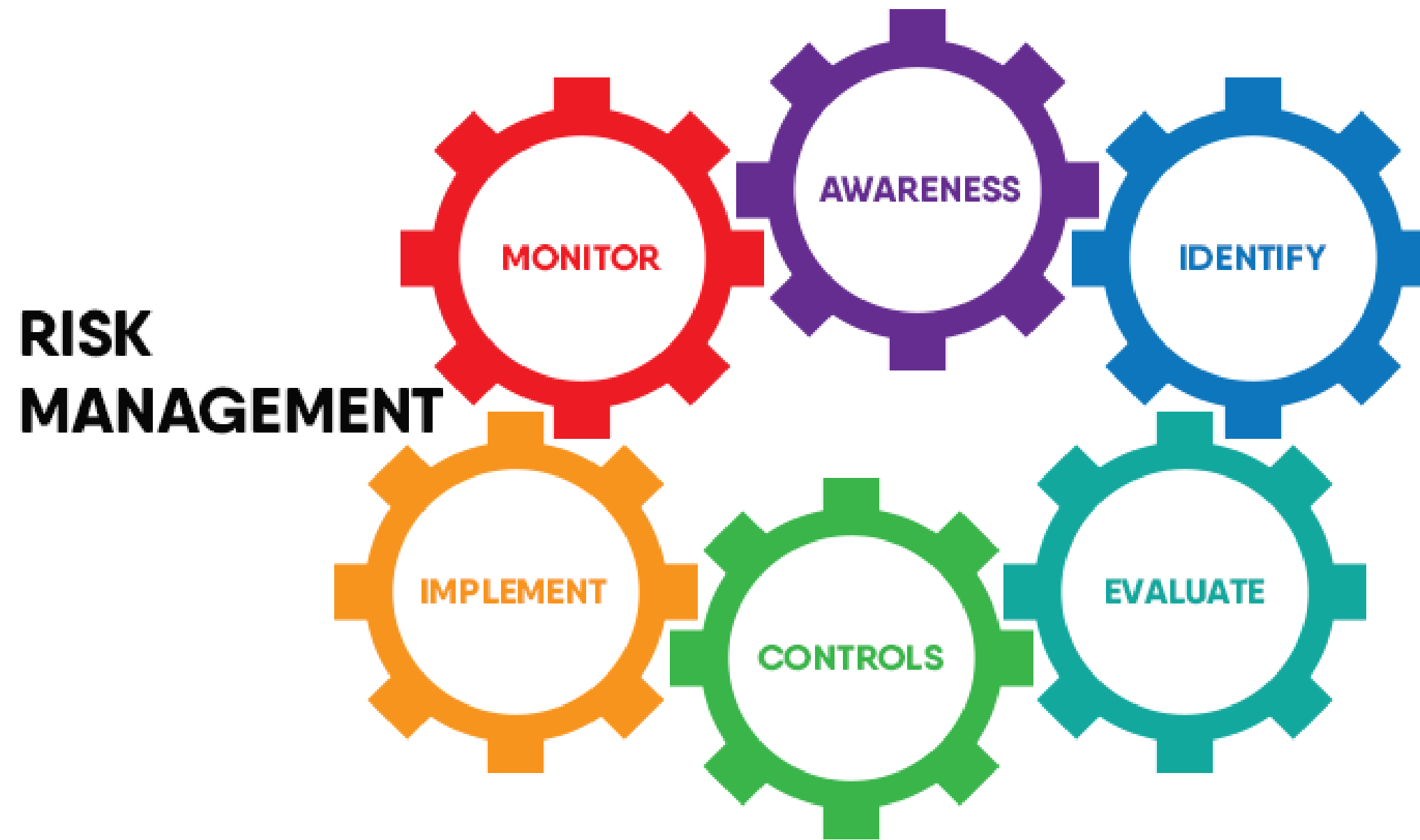


Information Security Governance

- Any policy should be endorsed, visibly, by the responsible people.



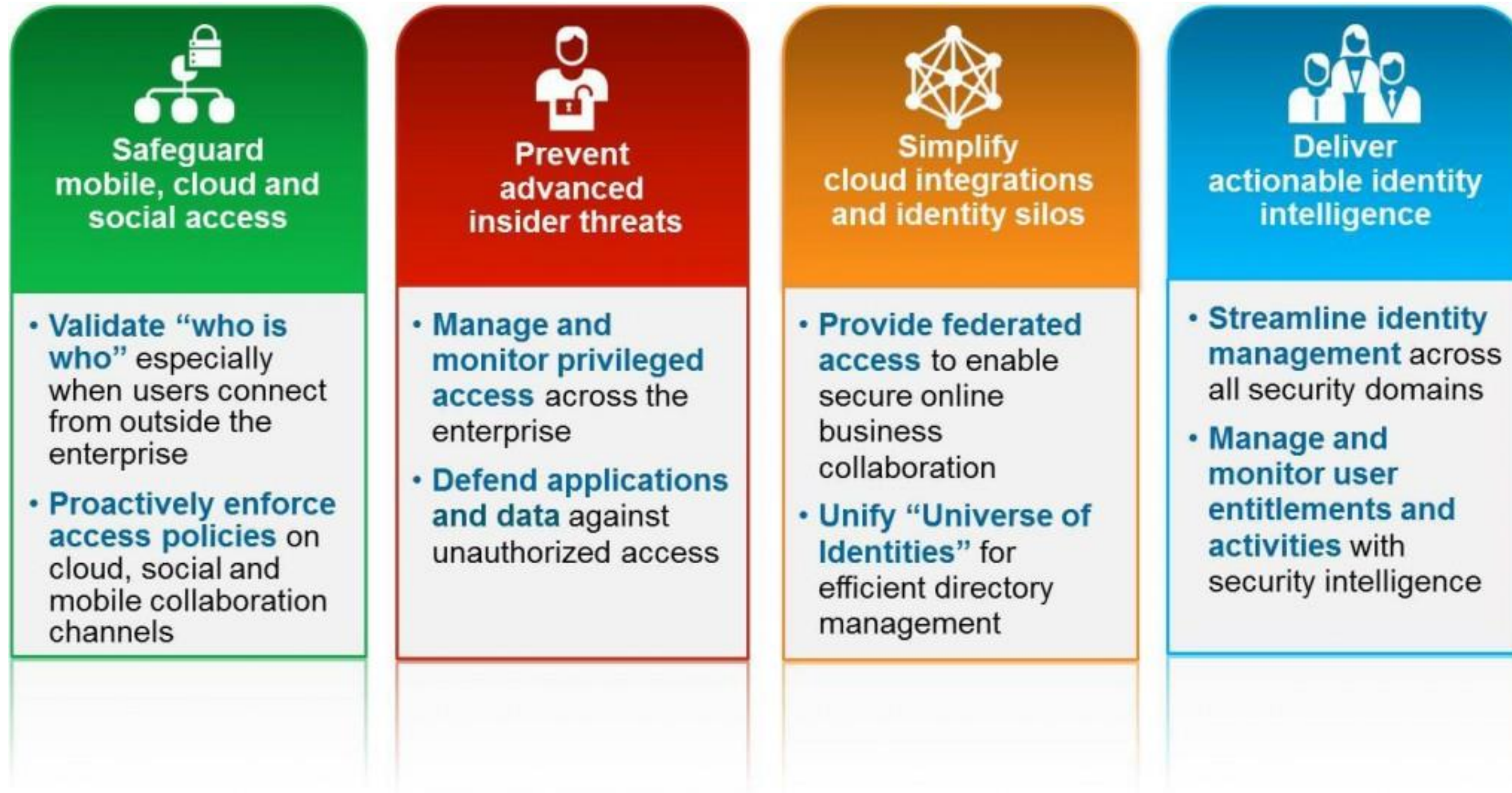
Information Risk Management



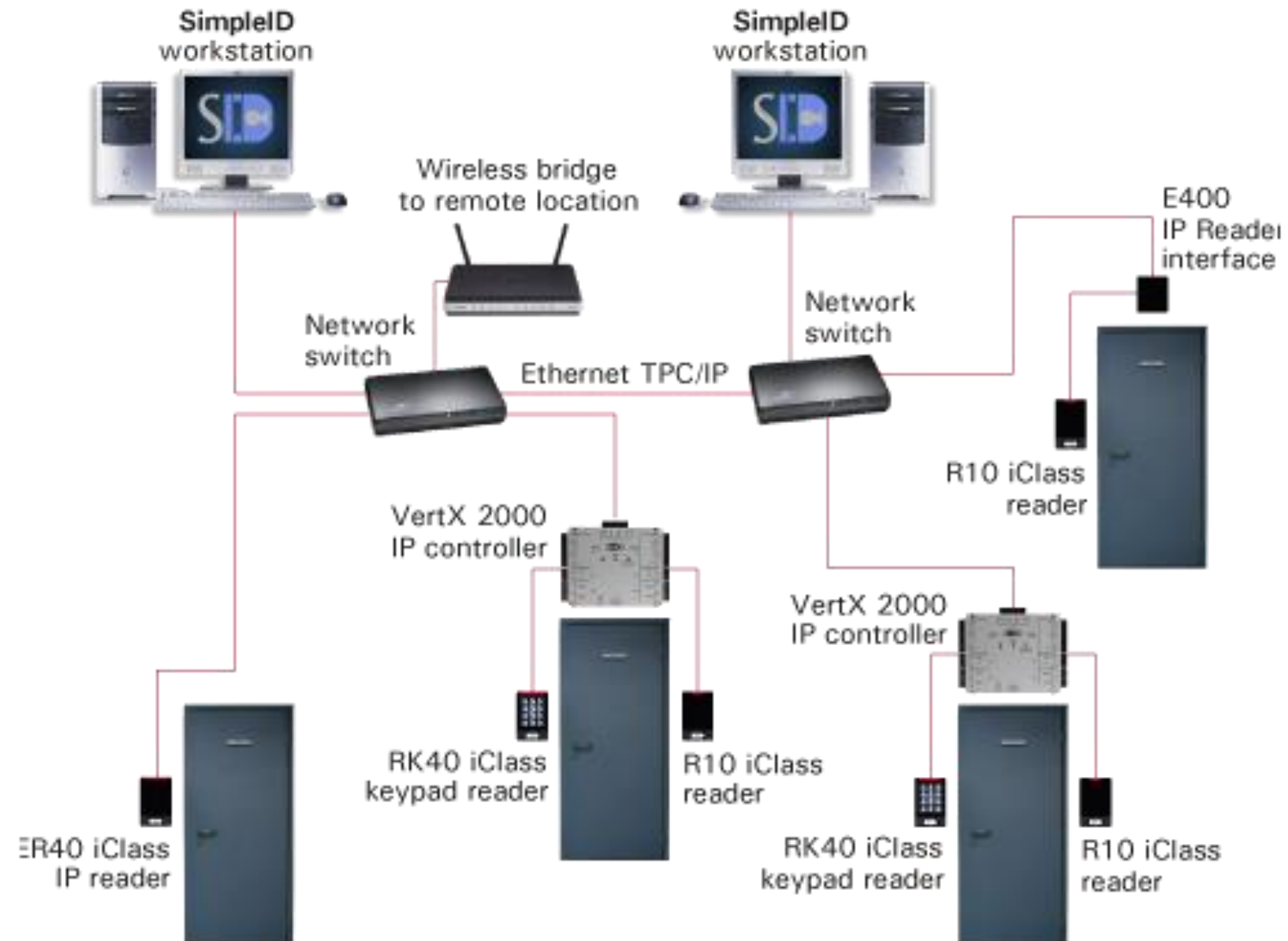
Information Risk Management

Risk Assessment Matrix				
Impact of Risk (Consequence)	Major	Medium	High	Extreme
	Moderate	Medium	Medium	High
	Minor	Low	Medium	Medium
Seriousness of Risk = Probability x Impact		Unlikely (0-33%)	Moderately Likely (33%-66%)	Highly Likely (66%-100%)
		Probability of Risk (Likelihood)		

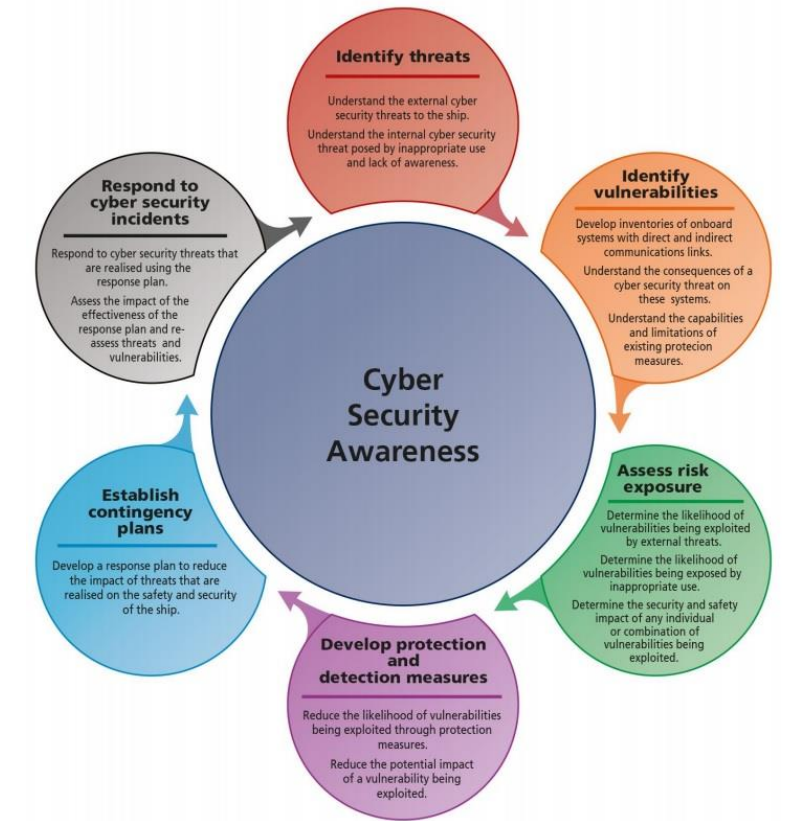
Information Security Program Development and Management



Information Security Program Development and Management



Information Security Program Development and Management



Information Security Incident Management

The Attack Chain



Information Security Incident Management



1. Identify the Incident Response Team – include roles, responsibilities and contact details; Internal and External (CERT.be, FCCU, RCCU)
2. Identify and prioritize the incident – rank the level of risk to the organization and detail the type of response required;
3. Review all possible outcomes of the attack and implement the predetermined risk responses;
4. Review the pre-determined legal and compliance reporting requirements that your company must meet;
5. Implement the Incident Response using the pre-determined scenarios in your risk register
 1. Containment procedures
 2. Eradication methods
 3. Recovery from the attack
6. Lessons learned

Taco Mulder

EMSc, CISM



Why and how implement an information security management system?

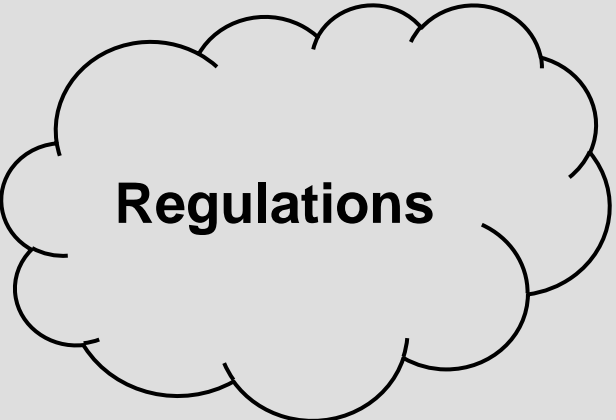
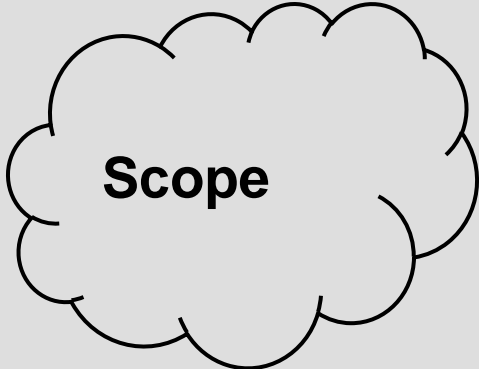
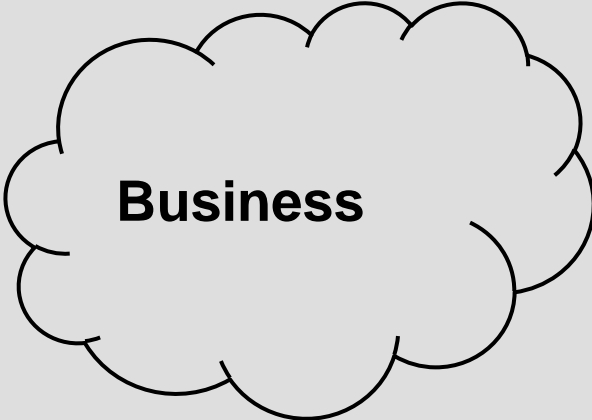
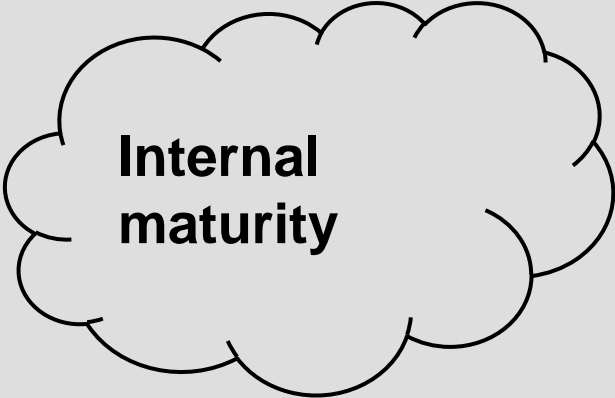


Gaël Hachez

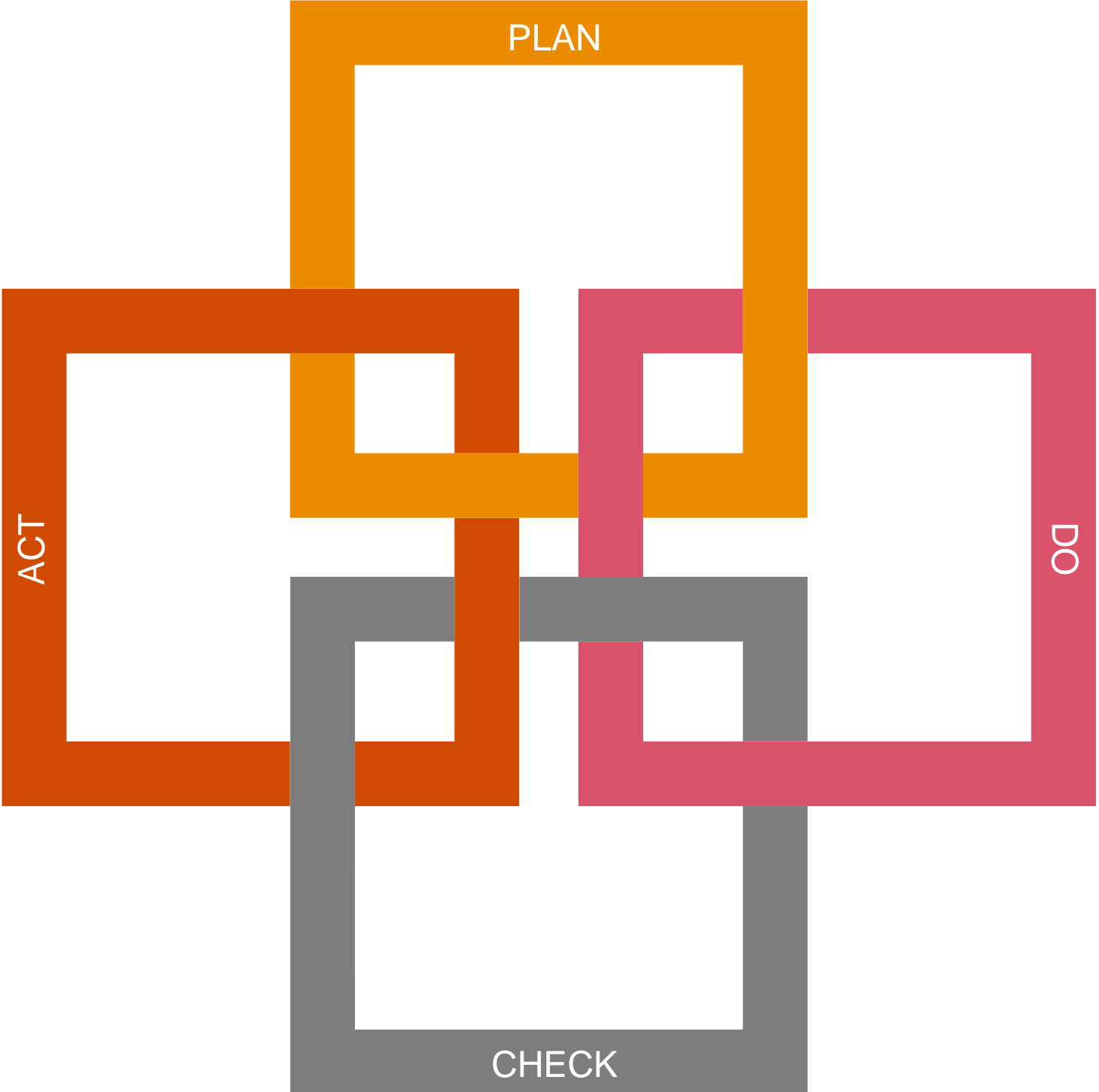
23 March 2021



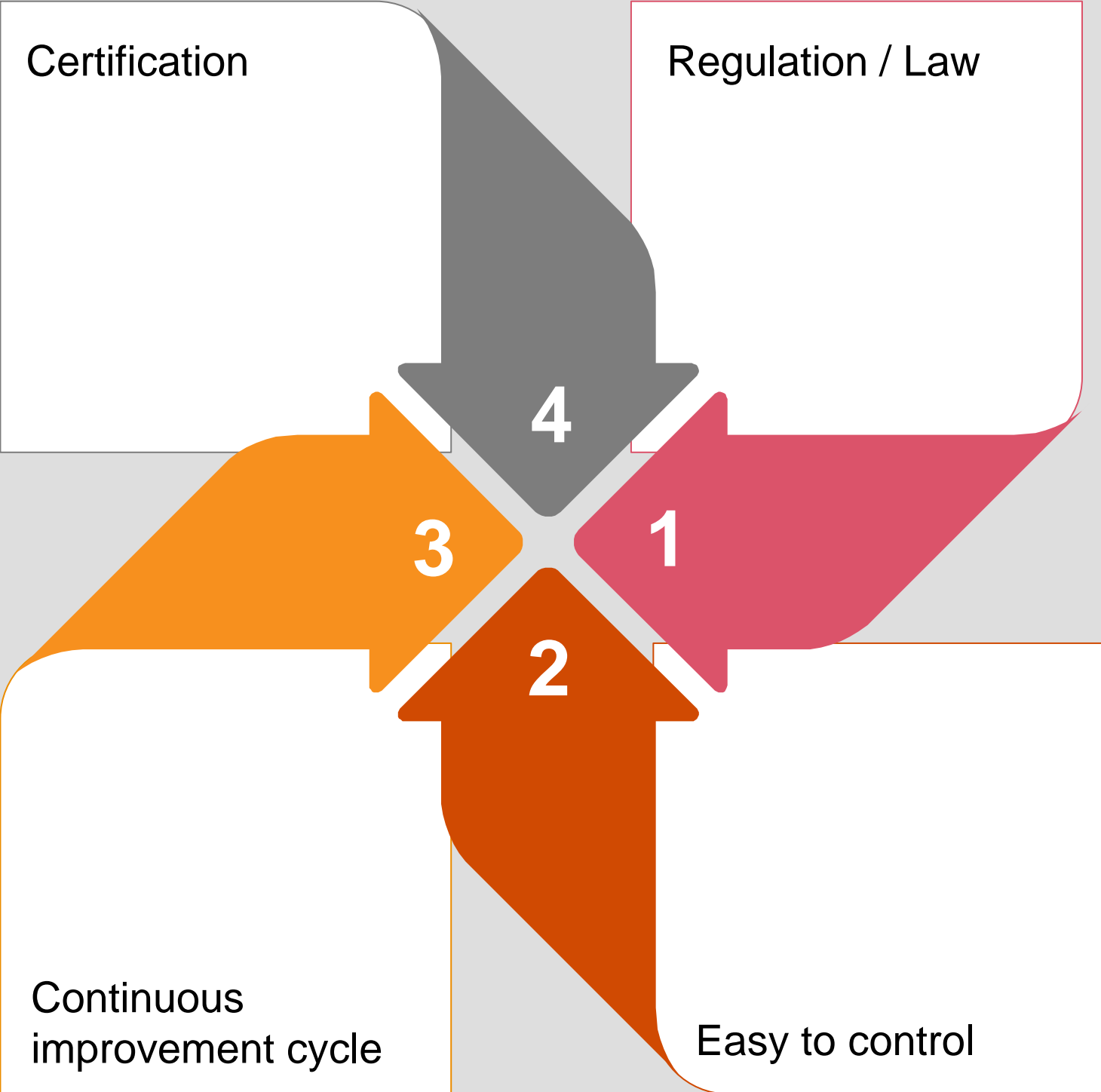
Information Security Management Standard? Do you need one? Which one?



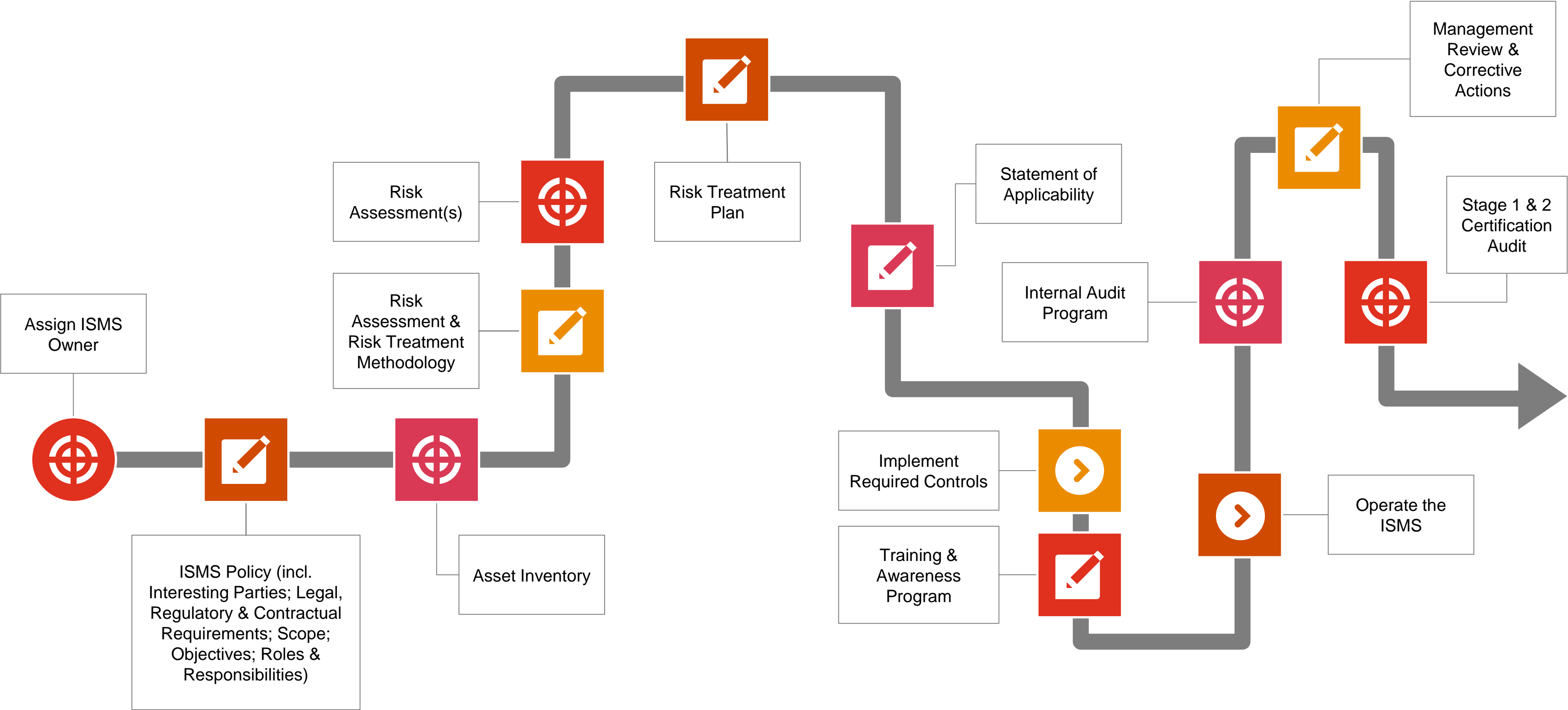
What is ISO 27001?



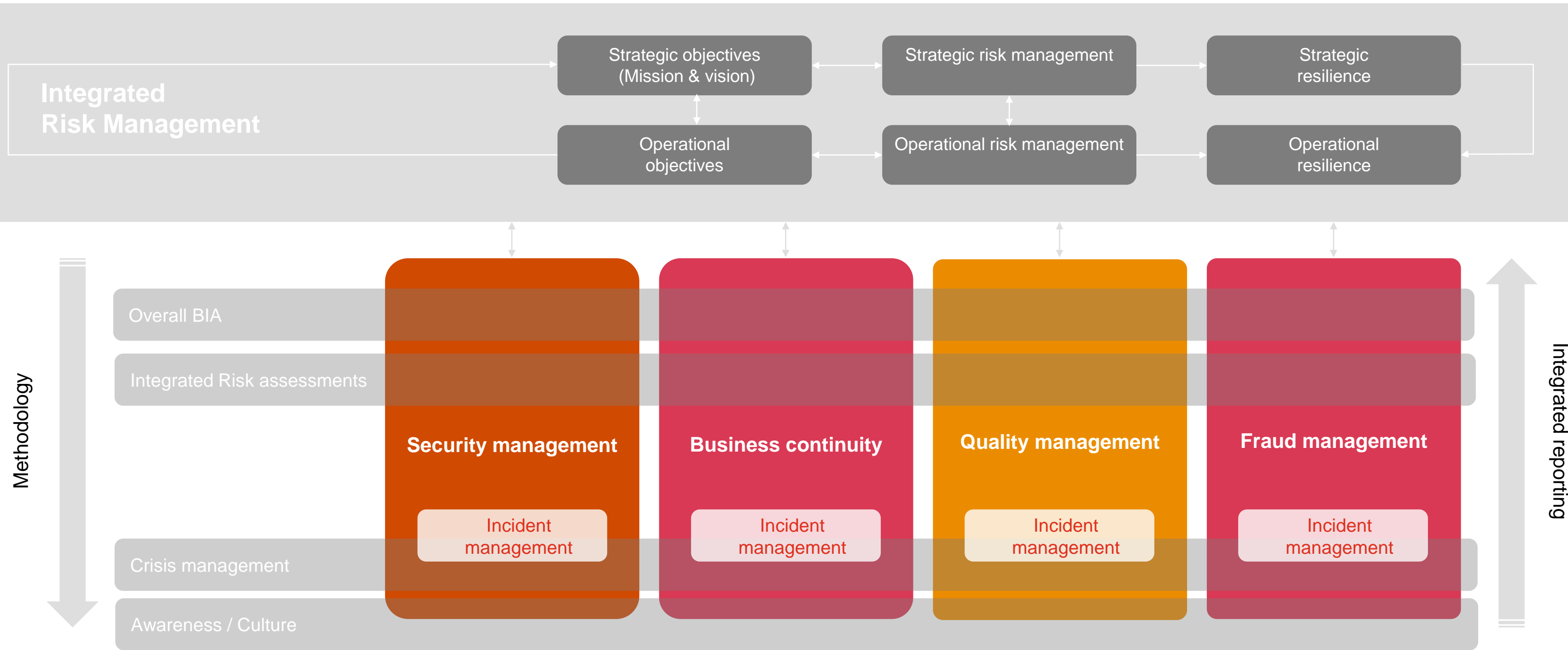
Why is it getting traction now?



ISO 27001 implementation - Overview of our practical approach



Integrated Management System



Thank you

www.pwc.be/en/services/consulting/technology-consulting/cybersecurity-cybercrime.html

© 2021 PwC. All rights reserved. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.