



BCRC

be connected

30
MARCH

EXPERIENCE
SHARING
EVENT



CYBER SECURITY
COALITION.be



Solvay Lifelong Learning
BRUSSELS SCHOOL, ECONOMICS, MANAGEMENT



ISACA
Belgium Chapter





Skills and roles for cybersecurity

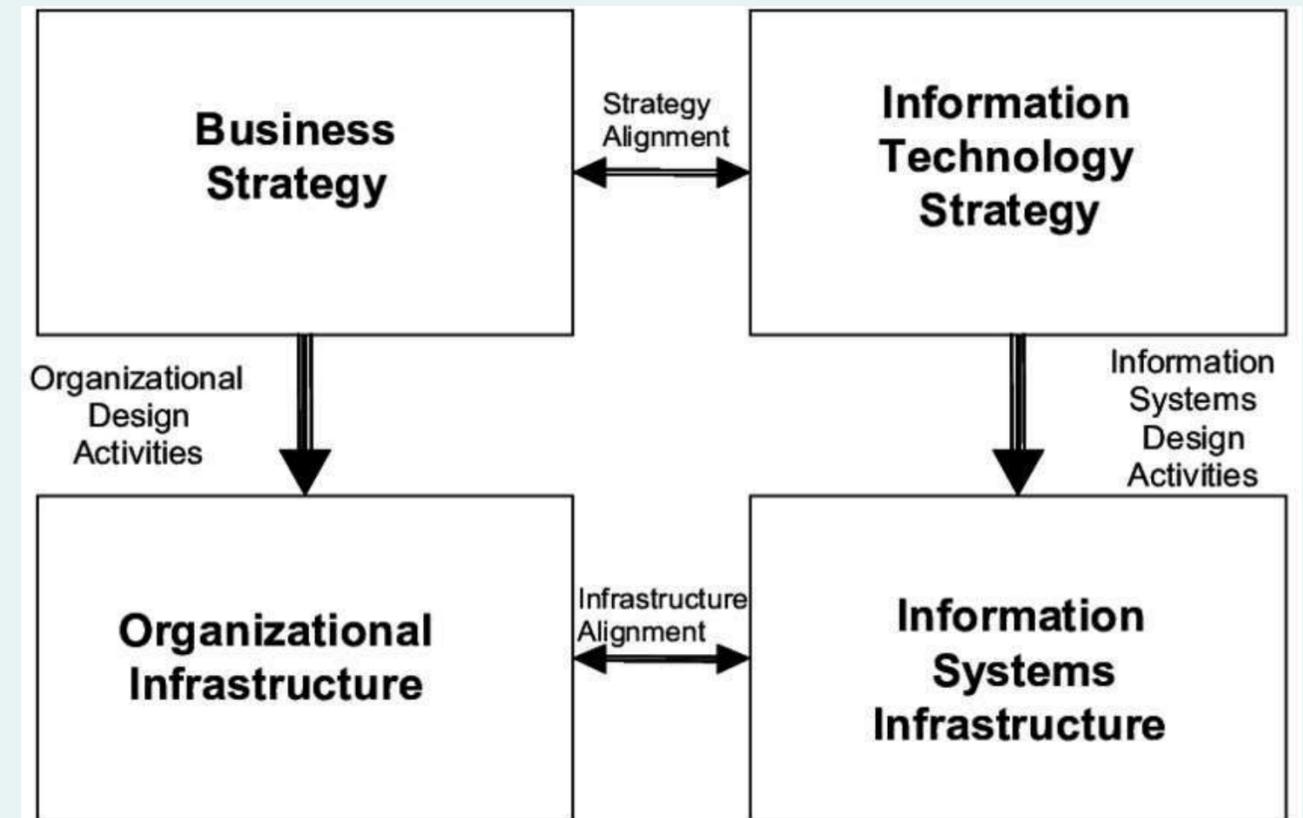
Georges Ataya
30 March 2023



DIGITAL GOVERNANCE

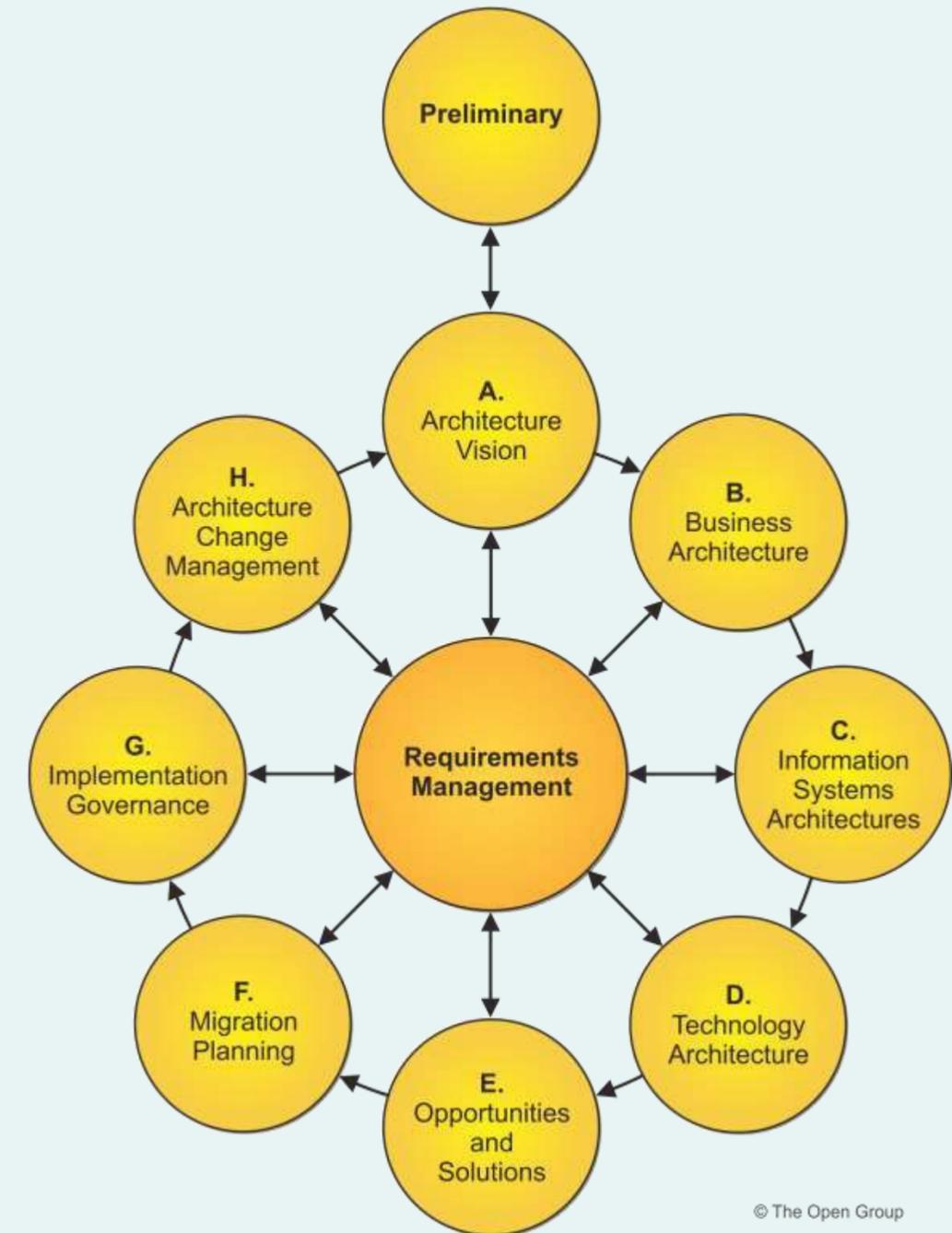
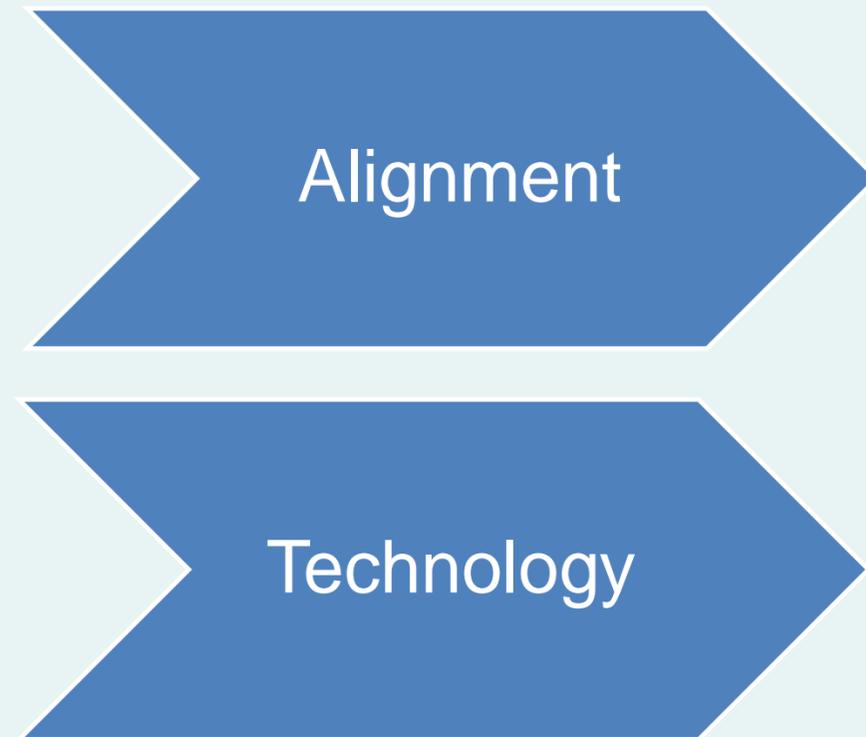


DIGITAL GOVERNANCE



Henderson and Venkatraman (1993)

DIGITAL GOVERNANCE



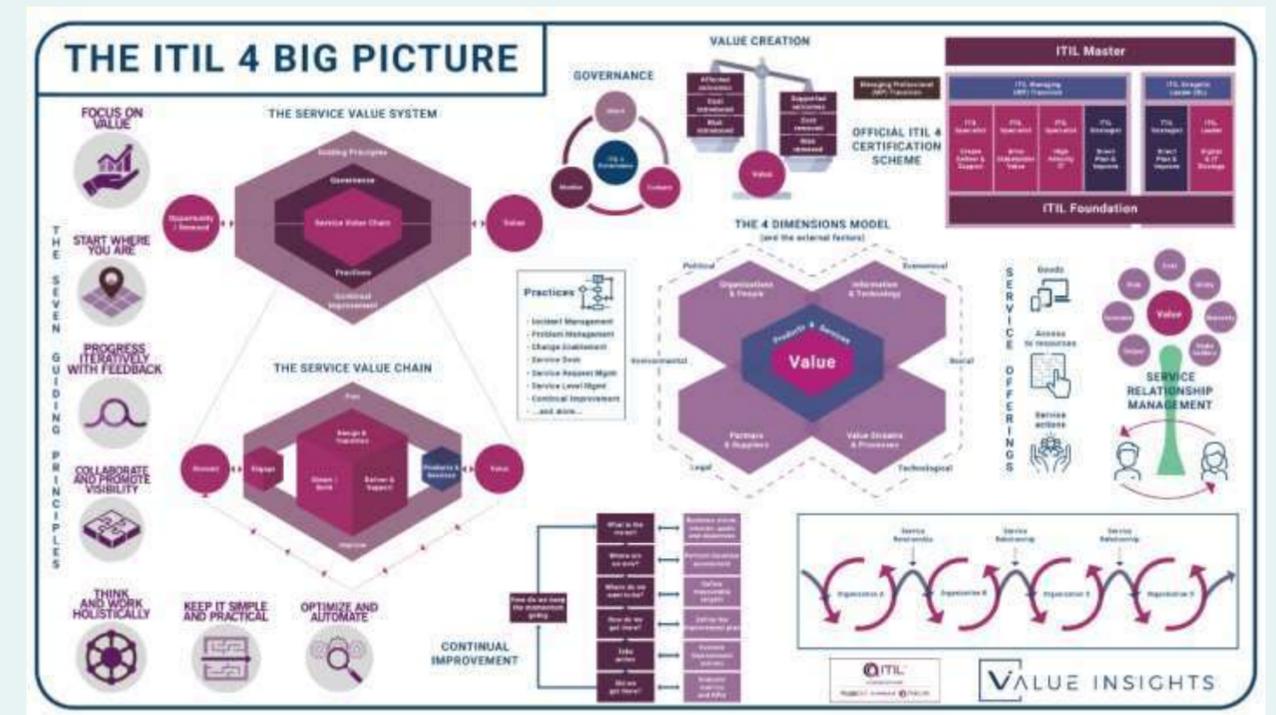
TOGAF

DIGITAL GOVERNANCE

Alignment

Technology

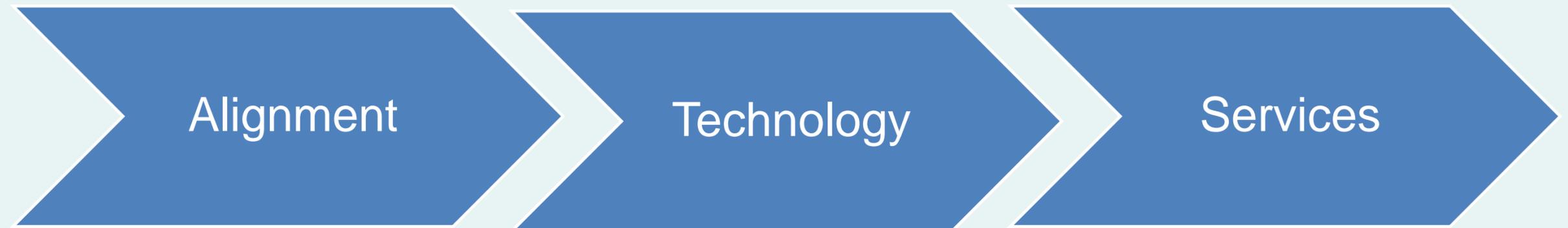
Services



Source: Value insights

ITIL Service Management

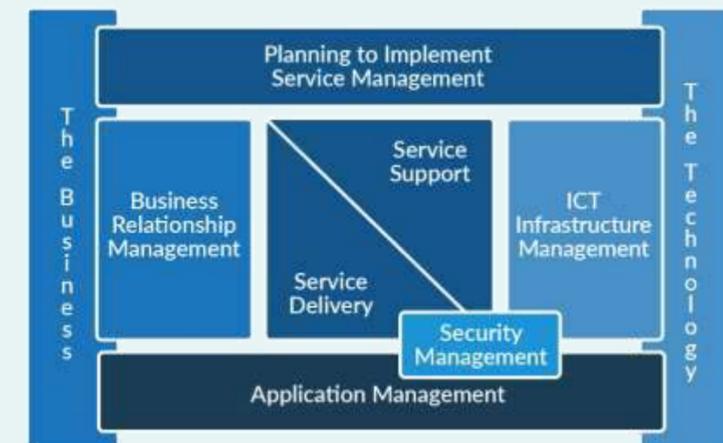
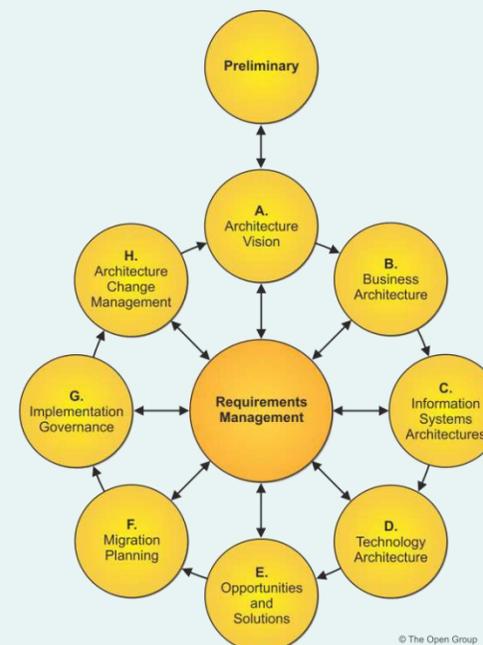
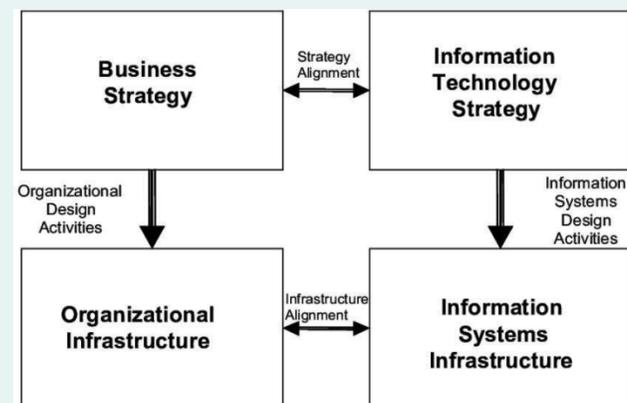
DIGITAL GOVERNANCE



Plan

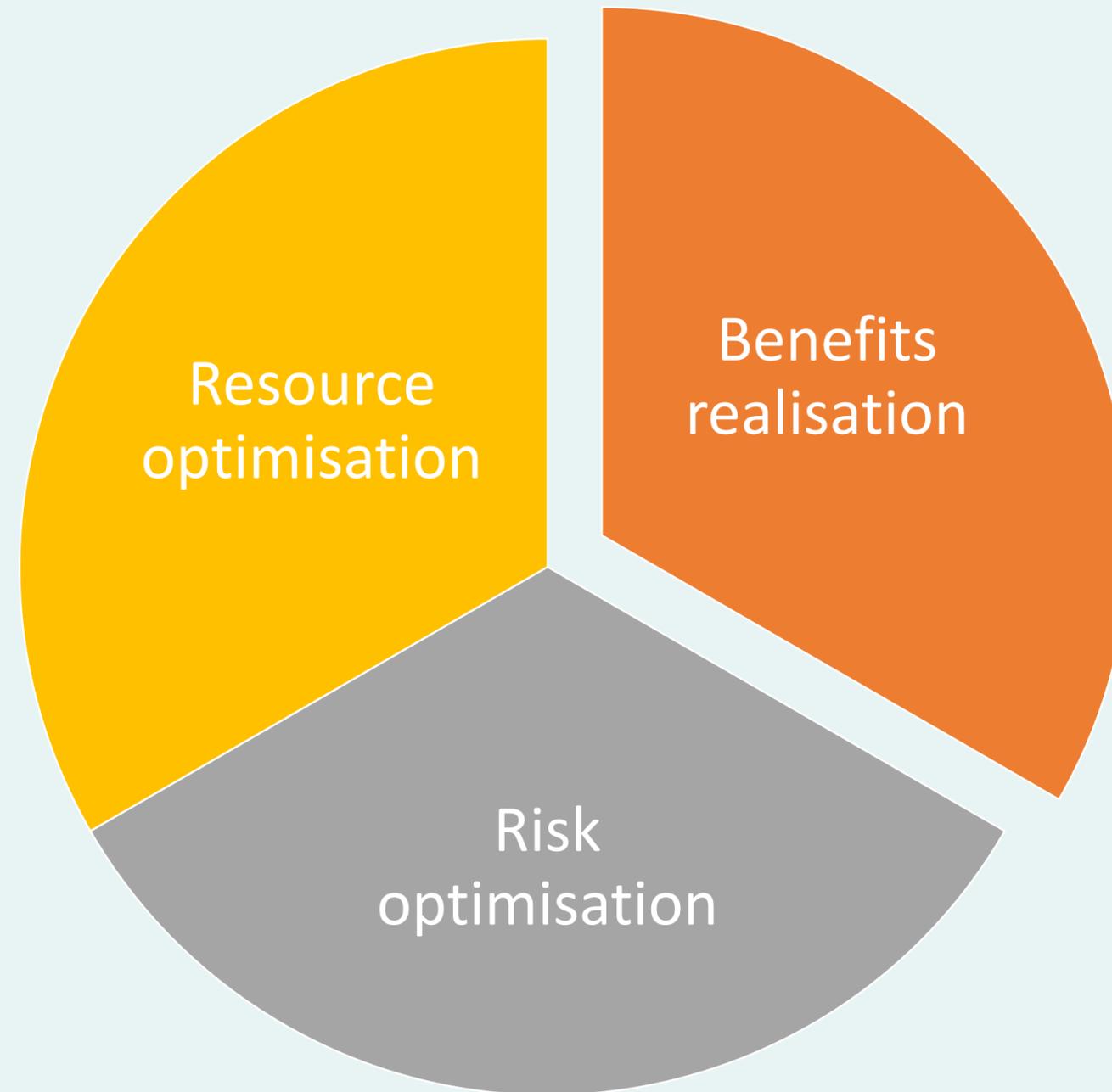
Build

Run

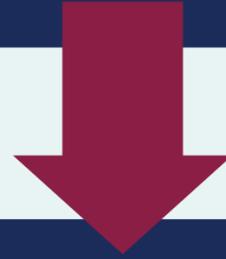


ENTERPRISE GOVERNANCE

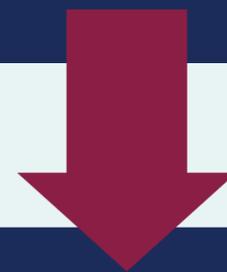
of DIGITAL ACTIVITIES



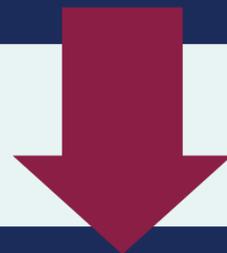
Stakeholder Drivers and Needs



Enterprise Goals



Alignment Goals

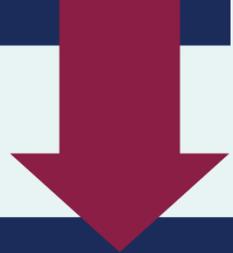


Governance and Management Objectives

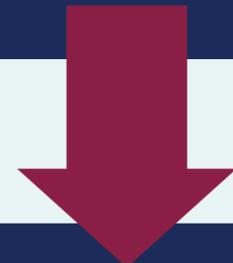


*Key objective:
Become an enabler of
the organisation's
strategy*

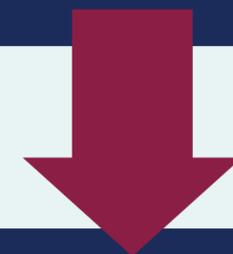
Stakeholder Drivers and Needs



Enterprise Goals



Alignment Goals



Governance and Management Objectives



COBIT Focus Area: Information Security



COBIT Focus Area: Information and Technology Risk

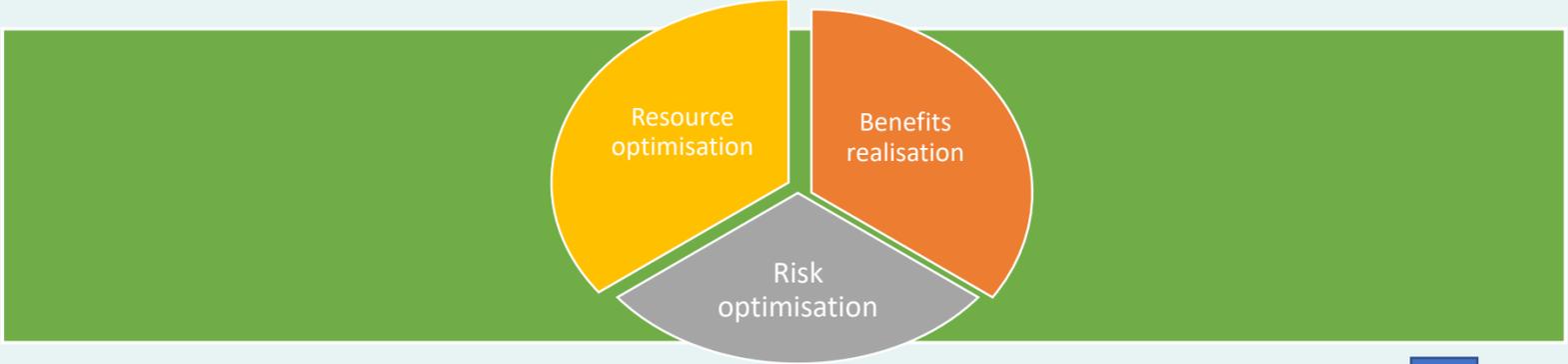


COBIT Focus Area: DevOps

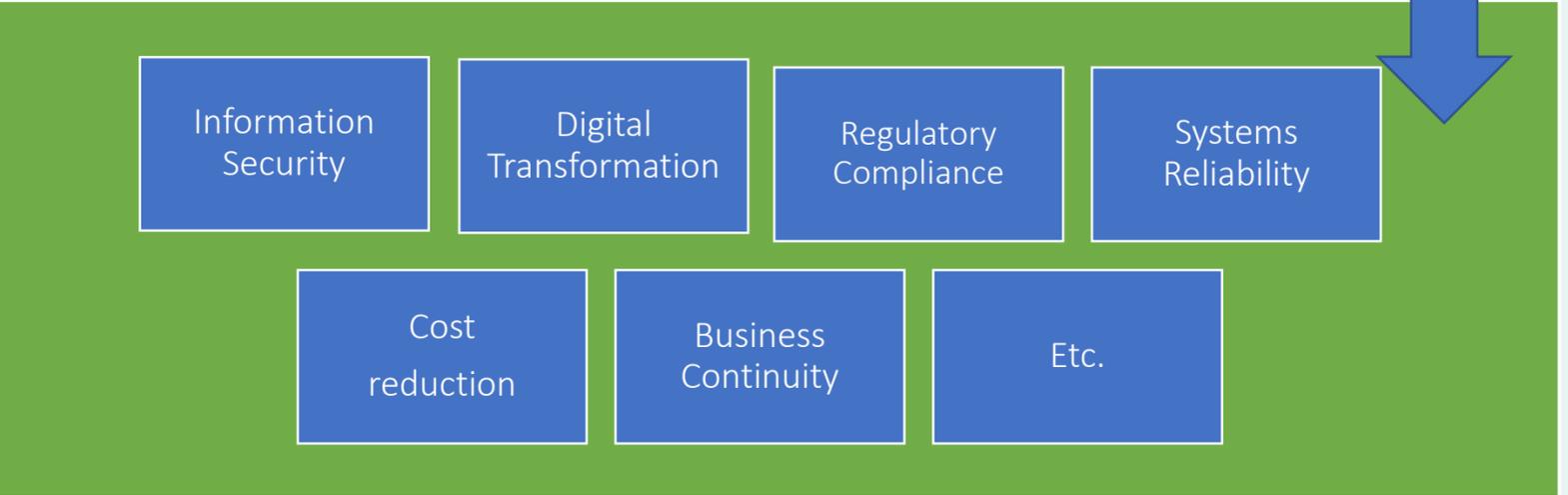


COBIT for Small and Medium Enterprises

Stakeholder Drivers and Needs



Enterprise Goals

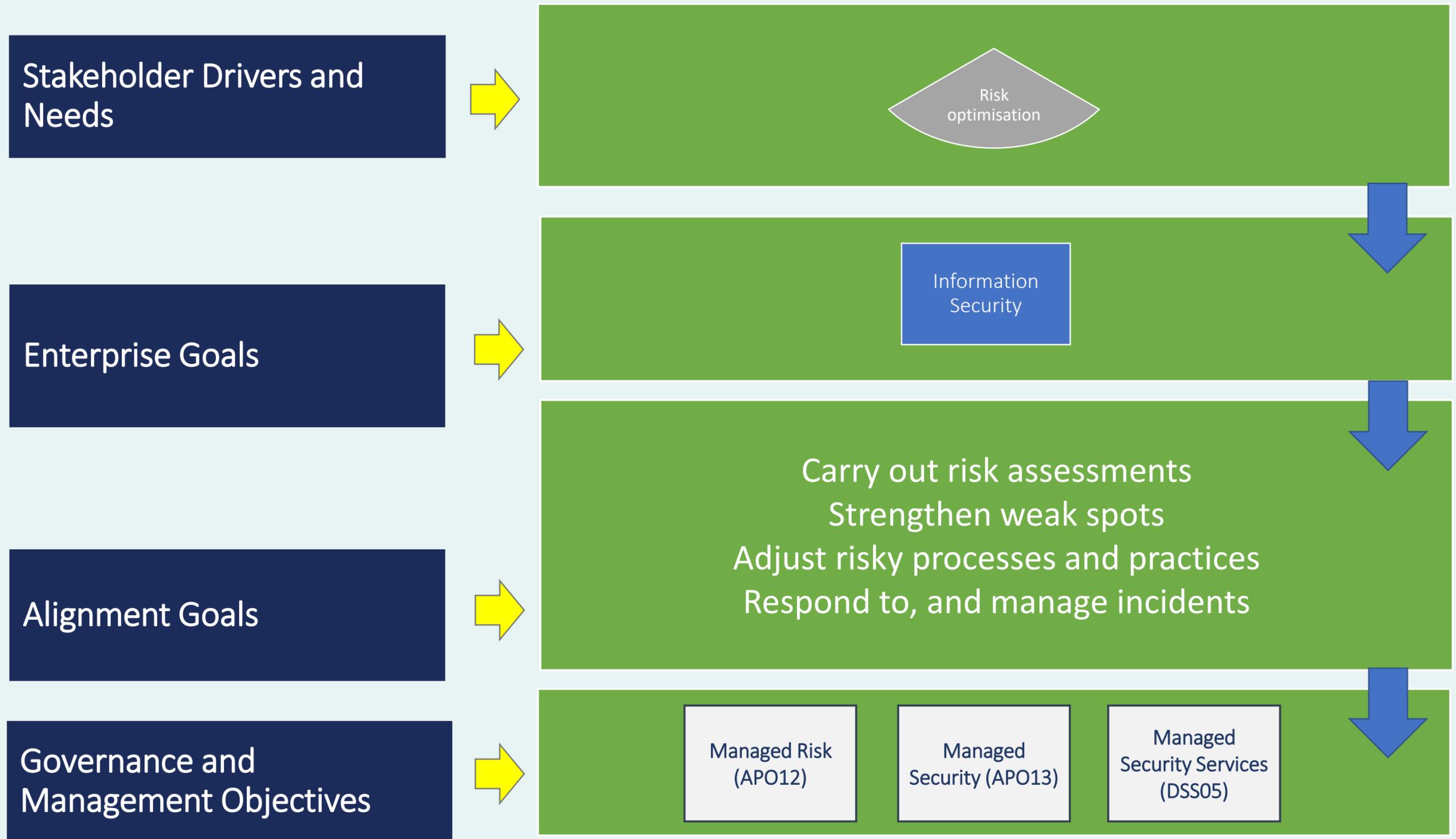


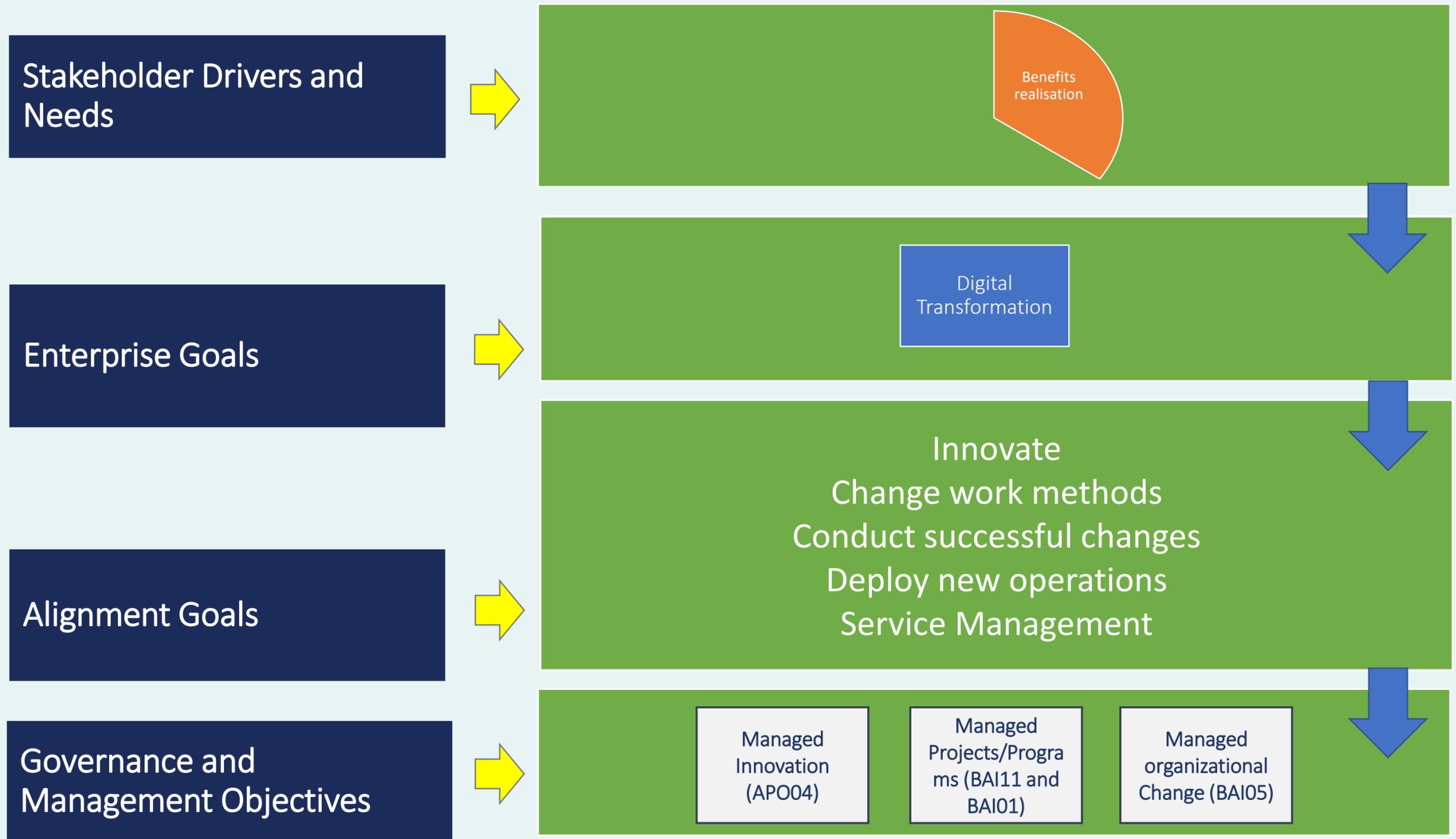
Alignment Goals

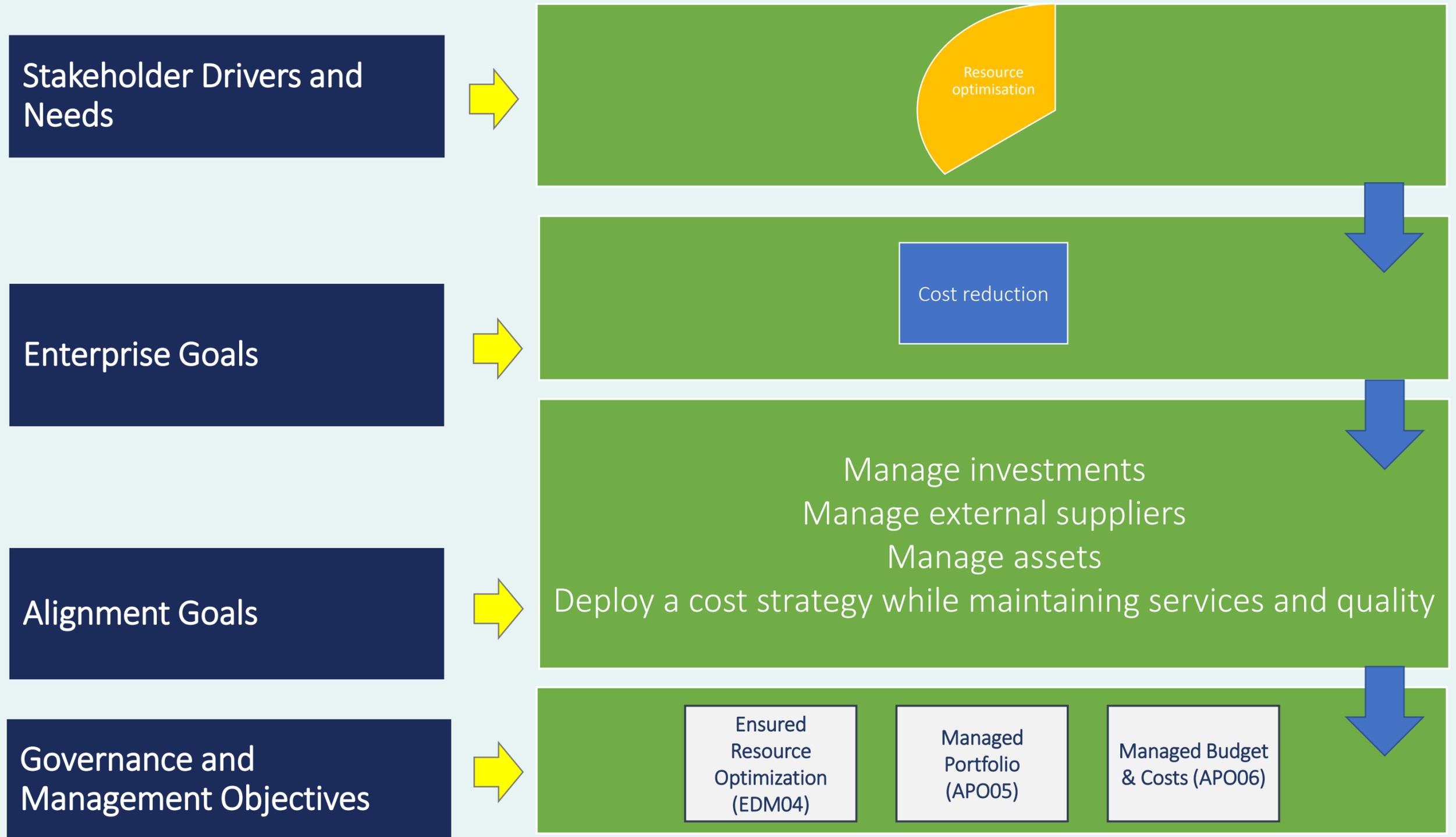


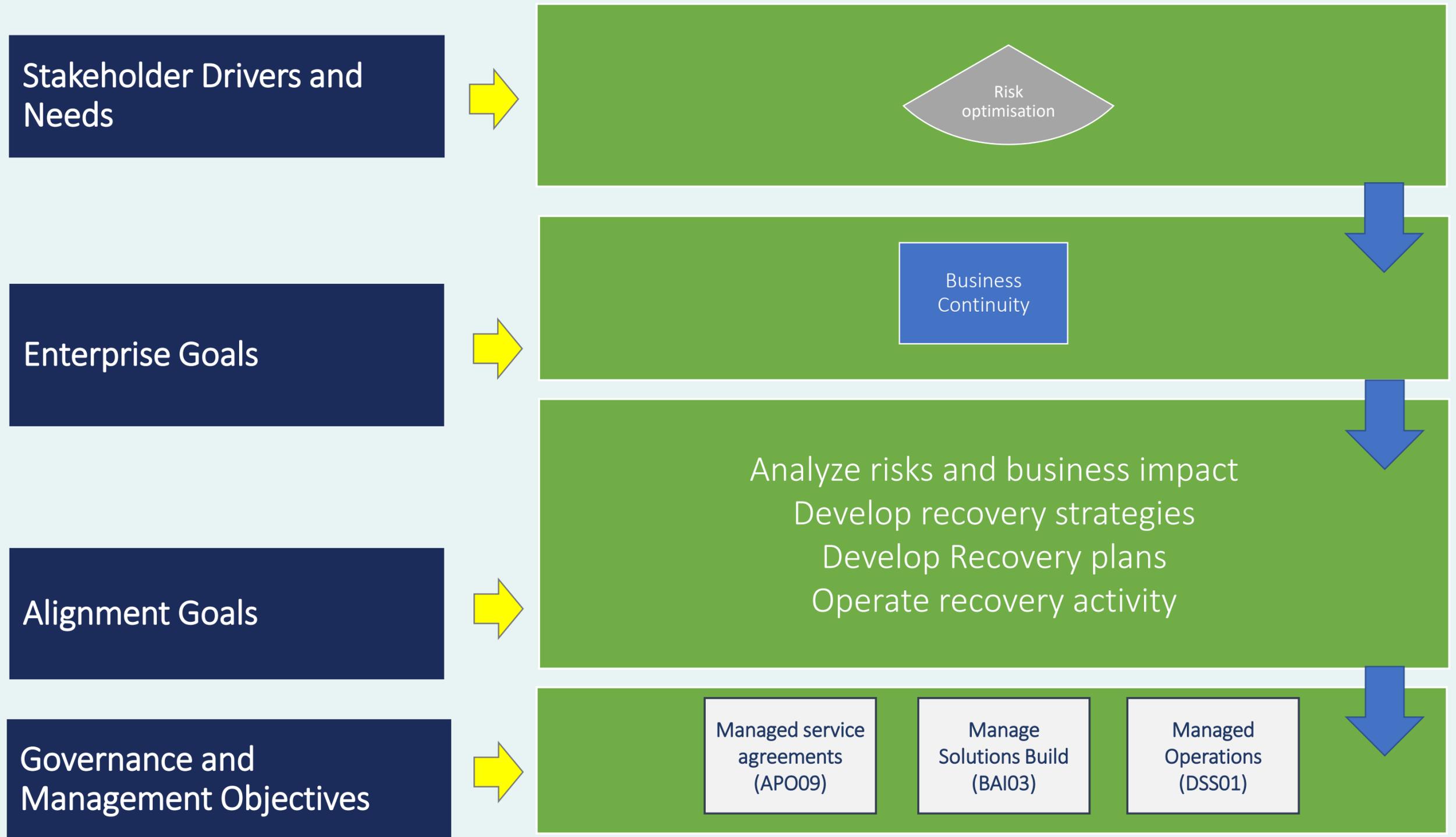
Governance and Management Objectives

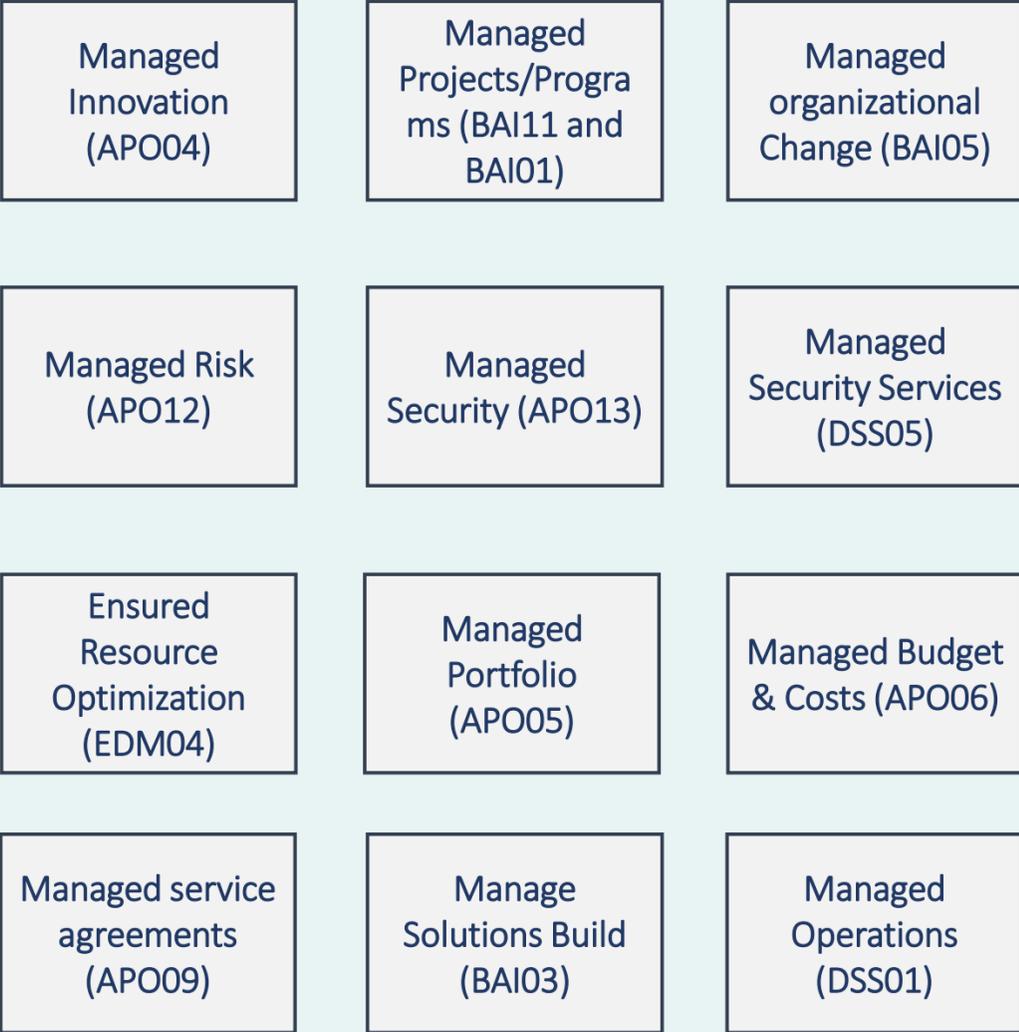












Govern

Ensured
Resource
Optimization
(EDM04)

Managed
Innovation
(APO04)

Managed
Portfolio (APO05)

Managed Budget
& Costs (APO06)

Managed service
agreements
(APO09)

Managed Risk
(APO12)

Managed
Security (APO13)

Plan

Managed
Projects/Program
s (BAI11 and
BAI01)

Manage
Solutions Build
(BAI03)

Managed
organizational
Change (BAI05)

Build

Managed
Operations
(DSS01)

Managed
Security Services
(DSS05)

Run

Monitor

EDM01—Ensured
Governance
Framework Setting
and Maintenance

EDM02—Ensured
Benefits Delivery

Govern

EDM03—Ensured
Resource
Optimization

EDM05—Ensured
Stakeholder
Engagement

AP001—Managed
I&T Management
Framework

AP002—Managed
Strategy

AP003—Managed
Enterprise
Architecture

AP004—Managed
Information

AP005—Managed
Portfolio

AP006—Managed
Budget and Costs

AP007—Managed
Human Resources

Plan

AP008—Managed
Relationships

AP009—Managed
Service
Agreements

AP010—Managed
Vendors

AP011—Managed
Quality

AP012—Managed
Risk

AP013—Managed
Security

AP014—Managed
Data

BAI01—Managed
Programs

BAI02—Managed
Requirements
Definition

BAI03—Managed
Solutions
Identification
and Build

BAI04—Managed
Availability
Capacity

BAI05—Managed
Organizational
Change

BAI06—Managed
IT Changes

BAI07—Managed
IT Change
Acceptance and
Transitioning

Build

BAI08—Managed
Knowledge

BAI09—Managed
Assets

BAI10—Managed
Configuration

BAI11—Managed
Projects

DSS01—Managed
Operations

DSS02—Managed
Service Requests
and Incidents

DSS03—Managed
Problems

DSS04—Managed
Incidents

DSS05—Managed
Security
Services

DSS06—Managed
Business
Process Controls

Run

MEA01—Managed
Performance and
Conformance
Monitoring

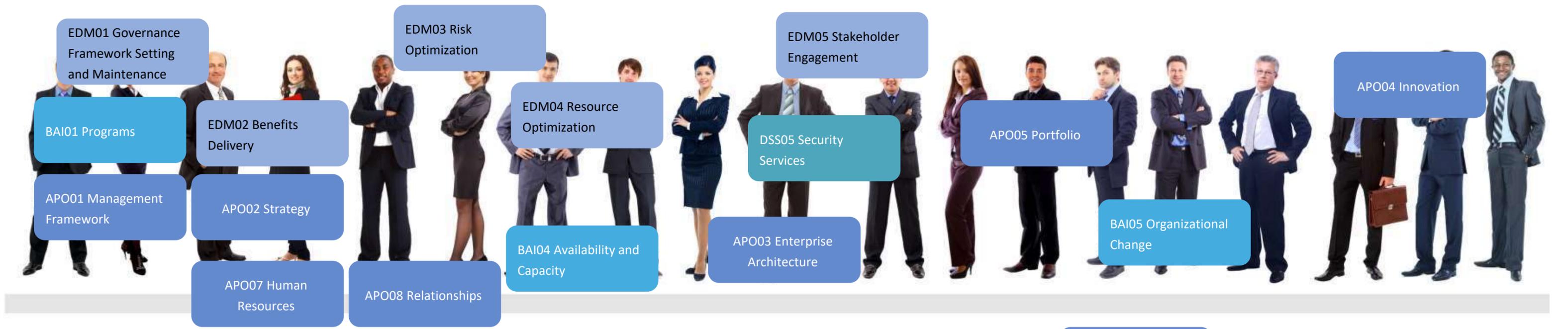
MEA02—Managed
System Internal
Control

MEA03—Managed
Compliance With
External
Requirements

MEA04—Managed
Assurance

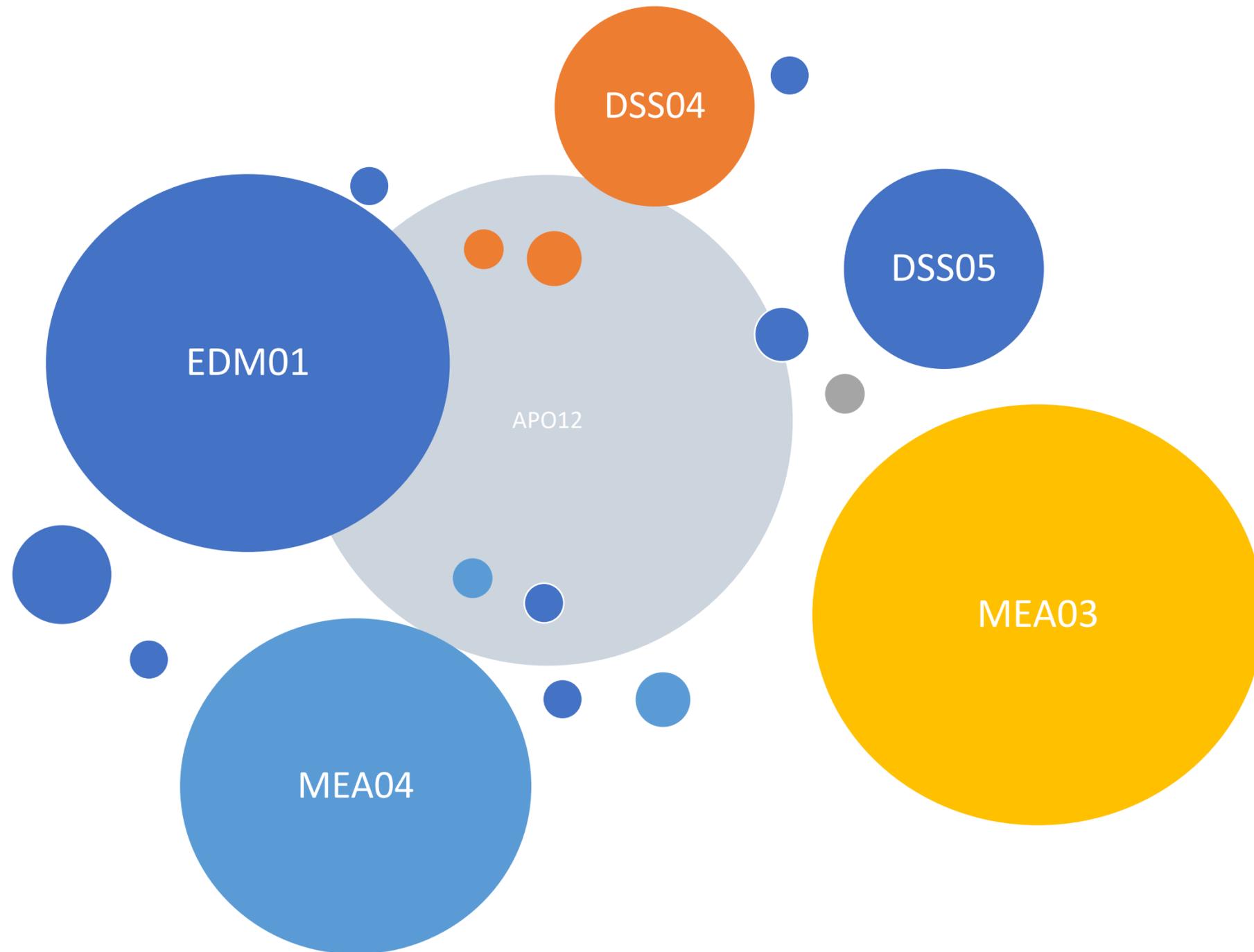
Monitor





Mapping Compliance Requirements

to Governance and Management Objectives (source COBIT annexes)



Plan

Build

Run

Monitor

Sample organisation 1

Plan

Build

Run

Monitor

Sample organisation 2

Plan

Build

Run

Monitor



1 . Information Security Leadership

March to April 2023

The management activities of Cybersecurity leaders includes the governance process, the business risk management process, the implementation process, and the incident management process. This module shall...

[> Learn more](#)

2 . Security Controls

May to June 2023

A review of enterprises landscape including business objectives and requirements collection for security controls. A thorough understanding of security controls in various domains and including...

[> Learn more](#)

3 . Security Architecture

September to October 2023

The architectural landscape is demystified, and components are identified to ensure adequate protections. Various architectural models shall be acquired by participants. The creation and implementation...

[> Learn more](#)

4 . Security Operations

November to December 2023

Business operations and information availability and integrity require the involvement of the whole organisation. Activities leading to building an adequate continuity are...

[> Learn more](#)

5 . Cybersecurity Battleground

January to February 2024

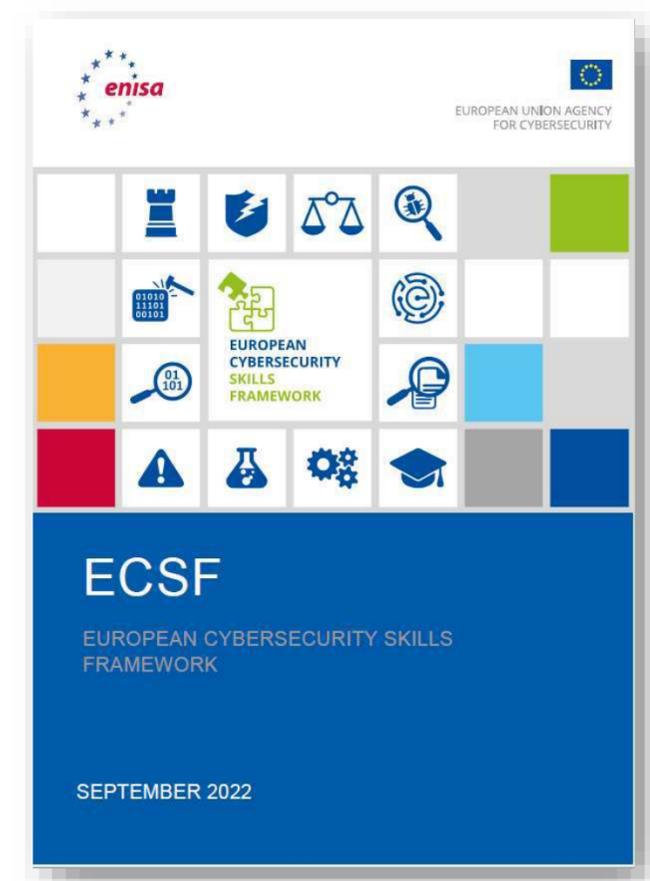
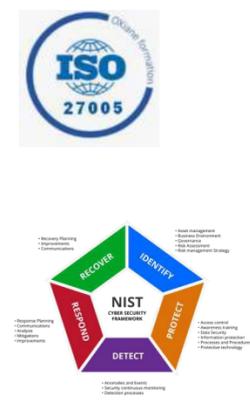
Cybersecurity management practices require the knowledge of own business, its functional and technical vulnerabilities and the threat landscape that needs to be addressed. The capabilities that...

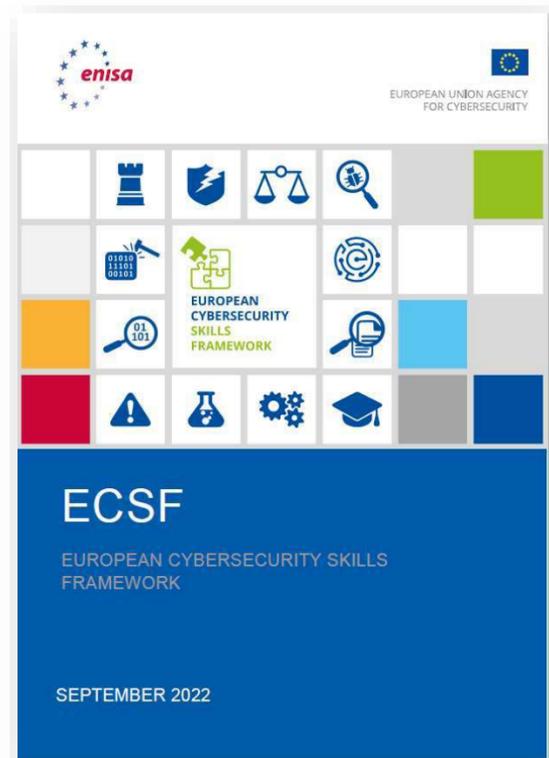
[> Learn more](#)

ALIGN WITH MAJOR BODIES OF KNOWLEDGE AND FRAMEWORKS



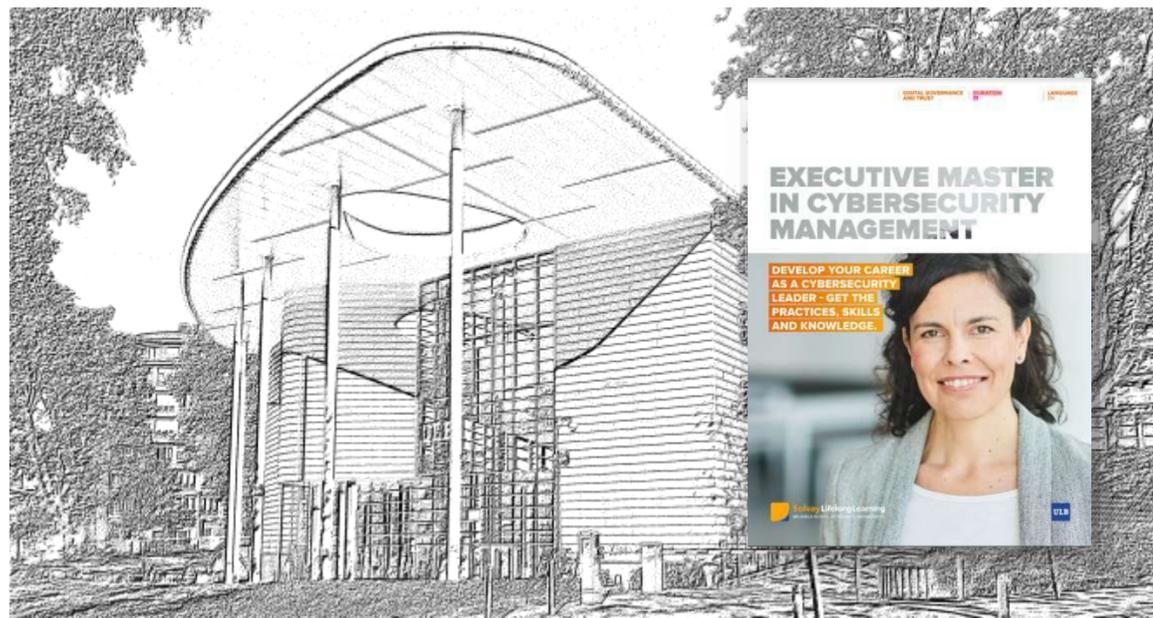
CyBOK

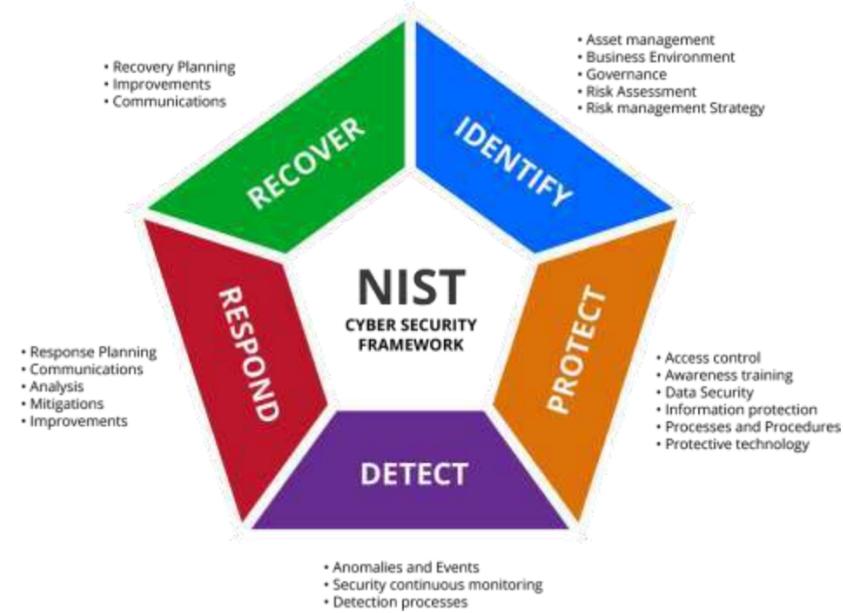




Alignment mapping

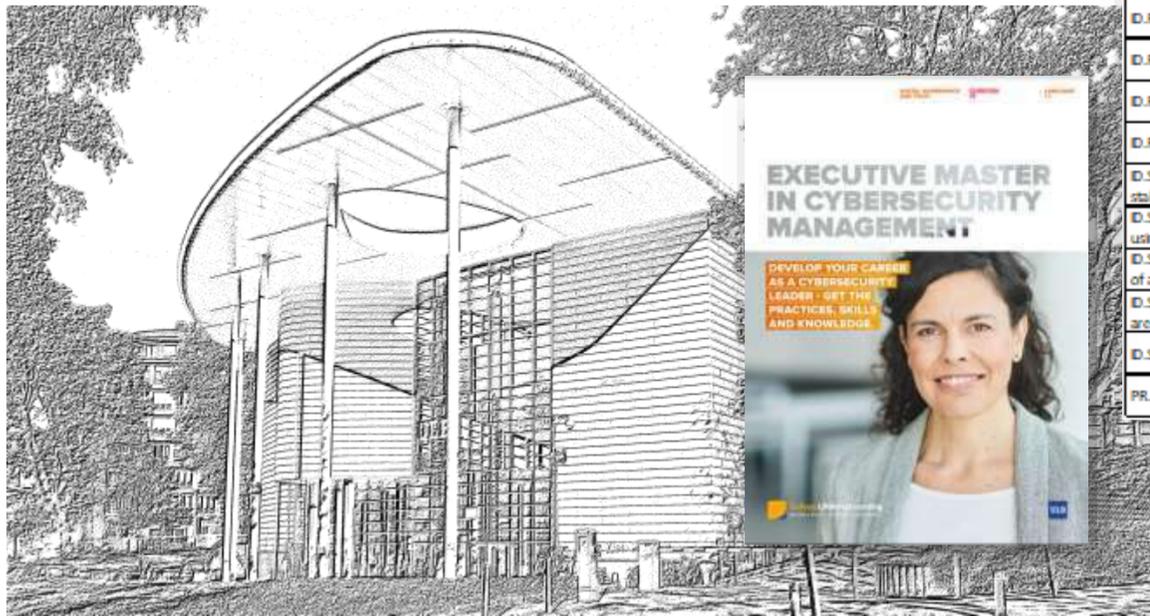
	PRIMARY or SECONDARY knowledge for Cybersecurity roles	Information Security Leadership	Security Controls	Security Architecture	Security Operations	Cybersecurity Battleground	General Management for CISO
1	CHIEF INFORMATION SECURITY OFFICER (CISO)	■	■	■	■	■	■
2	CYBER INCIDENT RESPONDER	□	■	□	■	■	□
3	CYBER LEGAL, POLICY & COMPLIANCE OFFICER	■	■	□	□	■	□
4	CYBER THREAT INTELLIGENCE SPECIALIST	□	□	■	■	■	□
5	CYBERSECURITY ARCHITECT	□	■	■	□	■	□
6	CYBERSECURITY AUDITOR	■	■	□	■	■	□
7	CYBERSECURITY EDUCATOR	■	■	□	□	□	□
8	CYBERSECURITY IMPLEMENTER	■	■	■	■	■	□
9	CYBERSECURITY RESEARCHER	□	■	■	■	■	□
10	CYBERSECURITY RISK MANAGER	□	■	■	□	■	□
11	DIGITAL FORENSICS INVESTIGATOR	□	■	■	■	■	□
12	PENETRATION TESTER	□	■	■	■	■	□
		■	P - Primary				
		□	S - Secondary				





Alignment mapping

	Information Security Leadership	Security Controls	Security Architecture	Security Operations	Cybersecurity Battleground	General Management for CISO
ID.AM 1: Physical devices and systems within the organization are inventoried				X		
ID.AM 2: Software platforms and applications within the organization are inventoried				X		
ID.AM 3: Organizational communication and data flows are mapped		X				
ID.AM 4: External information systems are catalogued				X		
ID.AM 5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value				X		
ID.AM 6: Cybersecurity roles and responsibilities for the entire workforce and third party stakeholders (e.g., suppliers, customers, partners) are established	X					
ID.BE 1: The organization's role in the supply chain is identified and communicated	X					
ID.BE 2: The organization's place in critical infrastructure and its industry sector is identified and communicated	X					
ID.BE 3: Priorities for organizational mission, objectives, and activities are established and communicated	X					
ID.BE 4: Dependencies and critical functions for delivery of critical services are established			X			
ID.BE 5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)				X		
ID.GV 1: Organizational cybersecurity policy is established and communicated					X	
ID.GV 2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners		X				
ID.GV 3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed		X				
ID.GV 4: Governance and risk management processes address cybersecurity risks		X				
ID.RA 1: Asset vulnerabilities are identified and documented		X				
ID.RA 2: Cyber threat intelligence is received from information sharing forums and sources					X	
ID.RA 3: Threats, both internal and external, are identified and documented					X	
ID.RA 4: Potential business impacts and likelihoods are identified		X				
ID.RA 5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk					X	
ID.RA 6: Risk responses are identified and prioritized					X	
ID.RM 1: Risk management processes are established, managed, and agreed to by organizational stakeholders		X				
ID.RM 2: Organizational risk tolerance is determined and clearly expressed	X					
ID.RM 3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	X					
ID.SC 1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders		X				
ID.SC 2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process					X	
ID.SC 3: Contracts with suppliers and third party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.		X				
ID.SC 4: Suppliers and third party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.		X				
ID.SC 5: Response and recovery planning and testing are conducted with suppliers and third party providers				X	X	
PR.AC 1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes			X	X		



5 Functions

23 Categories

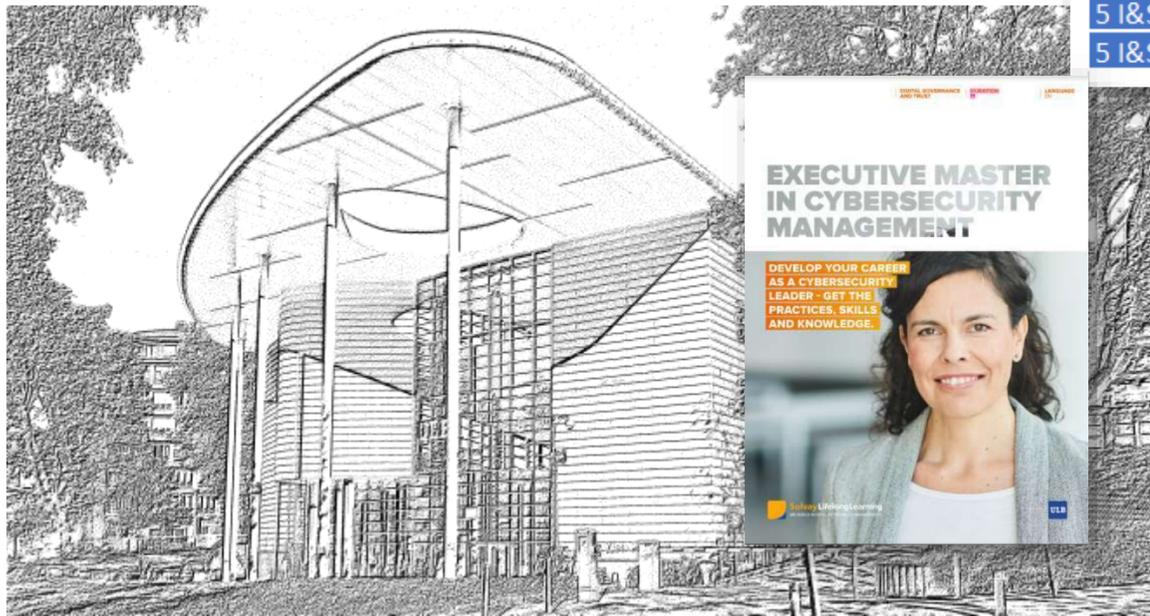
108 Subcategories

CyBOK

Alignment mapping

	Information Security Leadership	Security Controls	Security Architecture	Security Operations	Cybersecurity Battleground	General Management for CISO
0 - - - Introduction						
1 HOR - Human Factors	X					
1 HOR - Law Regulation	X					
1 HOR - Privacy Online Rights		X				
1 HOR - Risk Management Governance		X				
2 A&D - Adversarial Behaviours					X	
2 A&D - Forensics					X	
2 A&D - Malware Attack Technologies					X	
2 A&D - Security Operations Incident Management				X		
3 S&S - Authentication Authorisation Accountability			X			
3 S&S - Cryptography			X			
3 S&S - Distributed Systems Security			X			
3 S&S - Formal Methods for Security			X			
3 S&S - Operating Systems Virtualisation Security			X			
4 SPS - Secure Software Lifecycle			X			
4 SPS - Software Security			X			
4 SPS - Web Mobile Security			X			
5 I&S - Applied Cryptography			X			
5 I&S - Cyber Physical Systems			X			
5 I&S - Hardware Security			X			
5 I&S - Network Security			X			
5 I&S - Physical Layer			X			

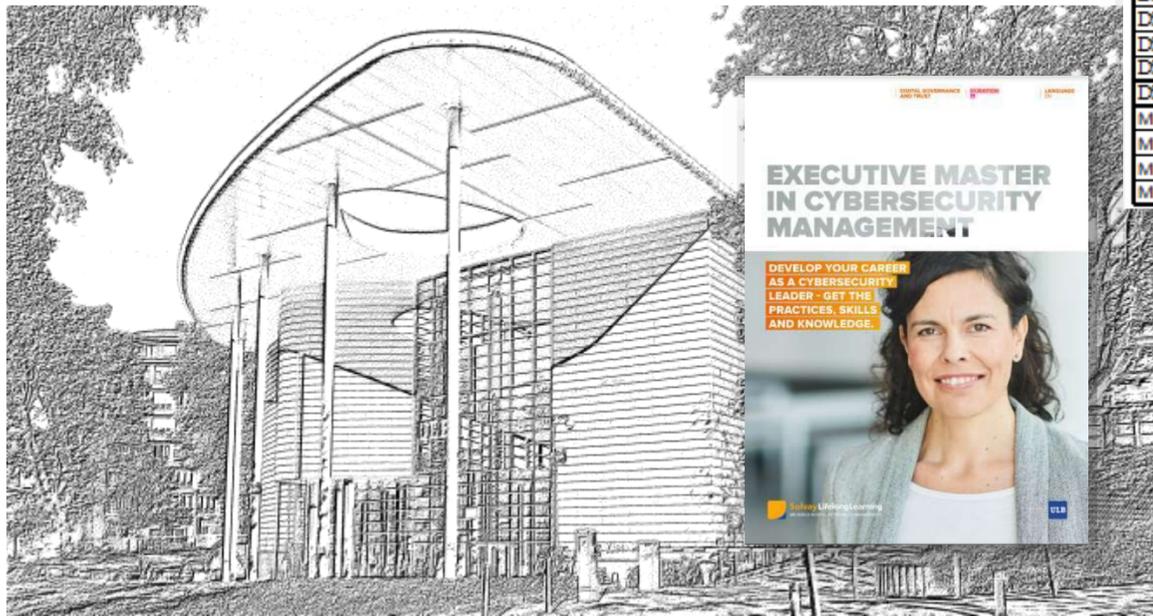
22 Sub-Domains





Alignment mapping

COBIT 2019 MANAGEMENT CONTROLS		Information Security Leadership	Security Controls	Security Architecture	Security Operations	Cybersecurity Battleground	General Management for CISO
EDM01	Ensured governance framework setting and maintenance	p					
EDM02	Ensured benefits delivery	p					
EDM03	Ensured risk optimization	p					
EDM04	Ensured resource optimization	p					
EDM05	Ensured stakeholder engagement	p					
APO01	Managed I&T management framework	p					
APO02	Managed strategy	p					
APO03	Managed enterprise architecture			p			
APO04	Managed innovation	p					
APO05	Managed portfolio	p					
APO06	Managed budget and costs	p					
APO07	Managed human resources	p					
APO08	Managed relationships	p					
APO09	Managed service agreements				p		
APO10	Managed vendors				p		
APO11	Managed quality		p				
APO12	Managed risk		p				
APO13	Managed security	p	p	p	p	p	p
APO14	Managed data				p		p
BAI01	Managed programs			p			
BAI02	Managed requirements definition		p	p			
BAI03	Managed solutions identification and build			p			
BAI04	Managed availability and capacity				p		
BAI05	Managed organizational change	p					
BAI06	Managed IT changes and transitioning			p			
BAI07	Managed IT change acceptance		p				
BAI08	Managed knowledge			p	p	p	
BAI09	Managed assets				p		
BAI10	Managed configuration			p			
BAI11	Managed projects			p			
DSS01	Managed operations				p		
DSS02	Managed service requests and incidents				p		
DSS03	Managed problems			p	p	p	
DSS04	Managed continuity				p		
DSS05	Managed security services controls				p		
DSS06	Managed business process				p		
MEA01	Managed performance and conformance monitoring	p	p				
MEA02	Managed system of internal control		p				
MEA03	Managed compliance with external requirements		p				
MEA04	Managed assurance		p				

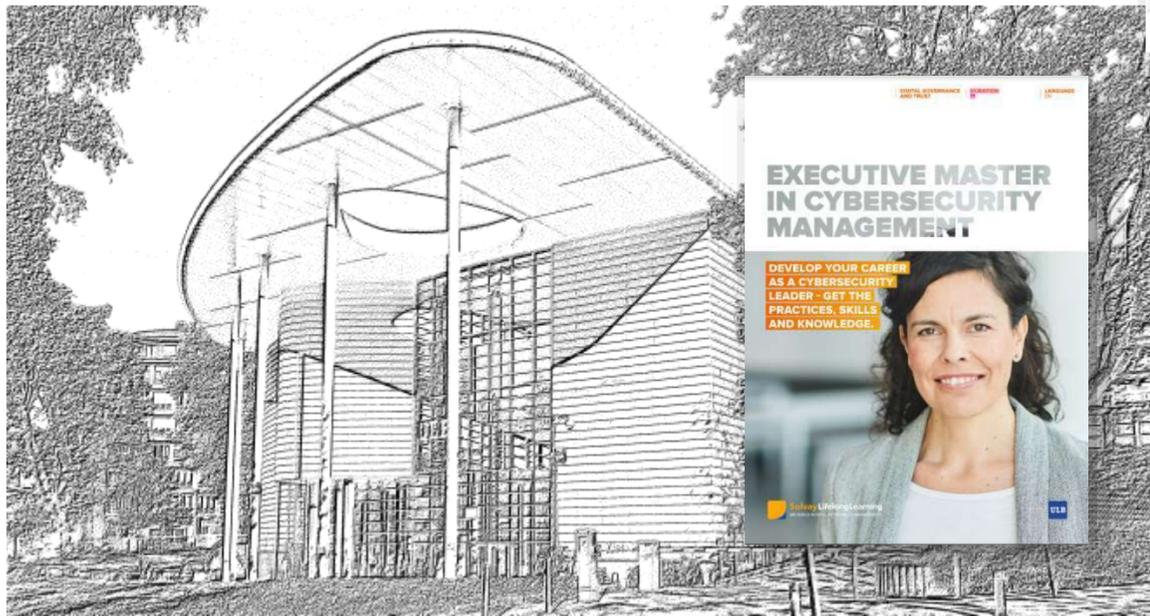


40 Management Objectives



Alignment mapping

skill_code	Title	Security Leadership	Security Controls	Security Architecture	Security Operations	Cybersecurity Battleground	General Management for CISO				
BPTS	Acceptance testing										
ADEV	Animation development										
ASUP	Application support			P							
ASMG	Asset management				P						
AUDT	Audit		P						S		
AVMT	Availability management				P				P		
BENM	Benefits management	P							P		
ADMN	Business administration	P							P		
BINT	Business intelligence						P				
BSMO	Business modelling		P								
BPRE	Business process improvement		P								
BUSA	Business situation analysis		P								
CPMG	Capacity management				P						
CSOP	Certification scheme operation		P								
CHMG	Change control			P							S
LEDA	Competency assessment	P									
CFMG	Configuration management				P				P		
CNSL	Consultancy					P					
INCA	Content authoring						P				
ICPM	Content publishing				P						
COPL	Continuity management				P						
ITCM	Contract management		P								
RFEN	Radio frequency engineering					S					
RESD	Real-time/embedded systems development					P					
RELM	Release and deployment						P				
REQM	Requirements definition and management				P						
THIN	Threat intelligence									P	
UNAN	User experience analysis										P
HCEV	User experience design										P



120 total skills

EXECUTIVE MASTER IN CYBERSECURITY MANAGEMENT

INTENDED AUDIENCE



© 2023 Copyright Georges Ataya, Solvay Learning and Design Hub

1

Intended Audience

CHIEF INFORMATION SECURITY MANAGER (CISO)



Decision making and relations with the General Management; Security Architecture and its impact on cybersecurity and business strategy; Cybersecurity operations and its impact on business activity; certification and accreditation in line with industry standards and regulatory requirements; the risk profiles in relation to budget priorities and protection targets.

© 2023 Copyright Georges Ataya, Solvay Learning and Design Hub

2

Intended Audience

CYBERSECURITY IMPLEMENTATION MANAGER



Cybersecurity project and program management; Security Architecture and its impact on targeted protections; impact of implementation projects and architecture on Cybersecurity operations; Capabilities and technology requirements for reaching intended industry standards and regulatory requirements; the residual risks in relation to program and project delivery as well as business risks related to delivered capabilities.

© 2023 Copyright Georges Ataya, Solvay Learning and Design Hub

3

Intended Audience

CYBERSECURITY MANAGEMENT ADVISOR



Capabilities to deliver CISO services, strategy, and architecture advisory and management counselling; Risk prioritisation and business impact analysis; Auditing; Risk assessment and maturity improvement projects; Review and assistance with external services, with the reliance on technology solutions, and with personnel maturity.

© 2023 Copyright Georges Ataya, Solvay Learning and Design Hub

4

Intended Audience

DIGITAL TRANSFORMATION PROFESSIONAL



Managing portfolio, programs or projects involve adequate knowledge of Cybersecurity issues related to business, technology and implementation constraints. Cybersecurity Architecture, Business needs, risk, and compliance issues drive today's transformation initiatives.

© 2023 Copyright Georges Ataya, Solvay Learning and Design Hub

5

Intended Audience

Chief Information officer (CIO)



Lead information and Cybersecurity activities vertically or liaise with horizontal cybersecurity activities in an enterprise; Understand the business capabilities; technical requirements and process implementation while leading the implementation of cybersecurity protections. Develop a technology savvy business management to support cybersecurity maturity in services and products and within technology and business personnel.

© 2023 Copyright Georges Ataya, Solvay Learning and Design Hub

6

Intended Audience

SECURITY OPERATIONS PROFESSIONAL



Understanding the business requirements and managing cybersecurity related operations; Build adequate capabilities to support incident and crisis situations; manage the organisation capabilities including architecture, configuration, operations, and services.

© 2023 Copyright Georges Ataya, Solvay Learning and Design Hub

7

Intended Audience

RISK MANAGER



Translate cybersecurity risks into business impact and formulate protection targets and priorities; understand the financial returns on cybersecurity investments and advice general managers in their decision making; assess risks of cybersecurity related projects and acquired external services.

© 2023 Copyright Georges Ataya, Solvay Learning and Design Hub

8

Intended Audience

COMPLIANCE PROFESSIONAL



Management of compliance activities in relation to cybersecurity laws, regulations, and industry requirements. Implementation of and project activities related to implementing selected controls. Support in the accreditation and the certification of operations and systems. Support in reaching relevant maturity levels to build control layers towards reaching intended cybersecurity protection.

© 2023 Copyright Georges Ataya, Solvay Learning and Design Hub

Intended Audience

HUMAN RESOURCES MANAGER



Understand cybersecurity skills and roles that are required to support recruiting, upskilling, reskilling and promoting cybersecurity, IT and business personnel. Apply innovative methods to build cybersecurity maturity.

© 2023 Copyright Georges Ataya, Solvay Learning and Design Hub

Intended Audience

AUDIT PROFESSIONAL



Review of lines of defence related to Cybersecurity services, risk evaluation, compliance activities, maturity improvement projects, and cybersecurity governance and monitoring activities. Review of external services and evaluation of technology components and cybersecurity profile of business operations.

© 2023 Copyright Georges Ataya, Solvay Learning and Design Hub

Intended Audience

BUSINESS MANAGER



Use cybersecurity capabilities as a competitive advantage and integrate security protections in developed products and services; Actively use cybersecurity capabilities in FINTECH, technology start-ups, and innovative products and services.

© 2023 Copyright Georges Ataya, Solvay Learning and Design Hub

Intended Audience

SENIOR EXECUTIVE



Apply cybersecurity management methods while managing human resources, leading finance operations, directing operations and business processes, and selling products and services.

© 2023 Copyright Georges Ataya, Solvay Learning and Design Hub

Intended Audience

Cybersecurity technical experts



Manage Technical cybersecurity activities including Digital Forensics investigators, Penetration testers, and Cyber Threat Intelligence specialist. Apply management methods while determining relevant actions to face related risks. Manage technical teams accordingly.

© 2023 Copyright Georges Ataya, Solvay Learning and Design Hub

Intended Audience

Cybersecurity Architect



Use full knowledge of risks and mitigation actions in building layers of protection. Ensure that built architecture is capable of implementing targeted protection strategy. Align building blocks with cybersecurity operations and foreseen future needs.

© 2023 Copyright Georges Ataya, Solvay Learning and Design Hub

Intended Audience

Cybersecurity Academics



Get updated on most recent management practices, frameworks and standards in relation to cybersecurity. Re-use advanced education practices to promote awareness, management knowledge and

© 2023 Copyright Georges Ataya, Solvay Learning and Design Hub



Cyber Incident Responder



Chief Information Security Officer (CISO)



Cybersecurity Educator



Cybersecurity Auditor



Cybersecurity Implementer



Cybersecurity Architect



Cyber Legal, Policy and Compliance Officer



Cyber Threat Intelligence Specialist



Penetration Tester



Cybersecurity Researcher



Cybersecurity Risk Manager



Digital Forensics Investigator

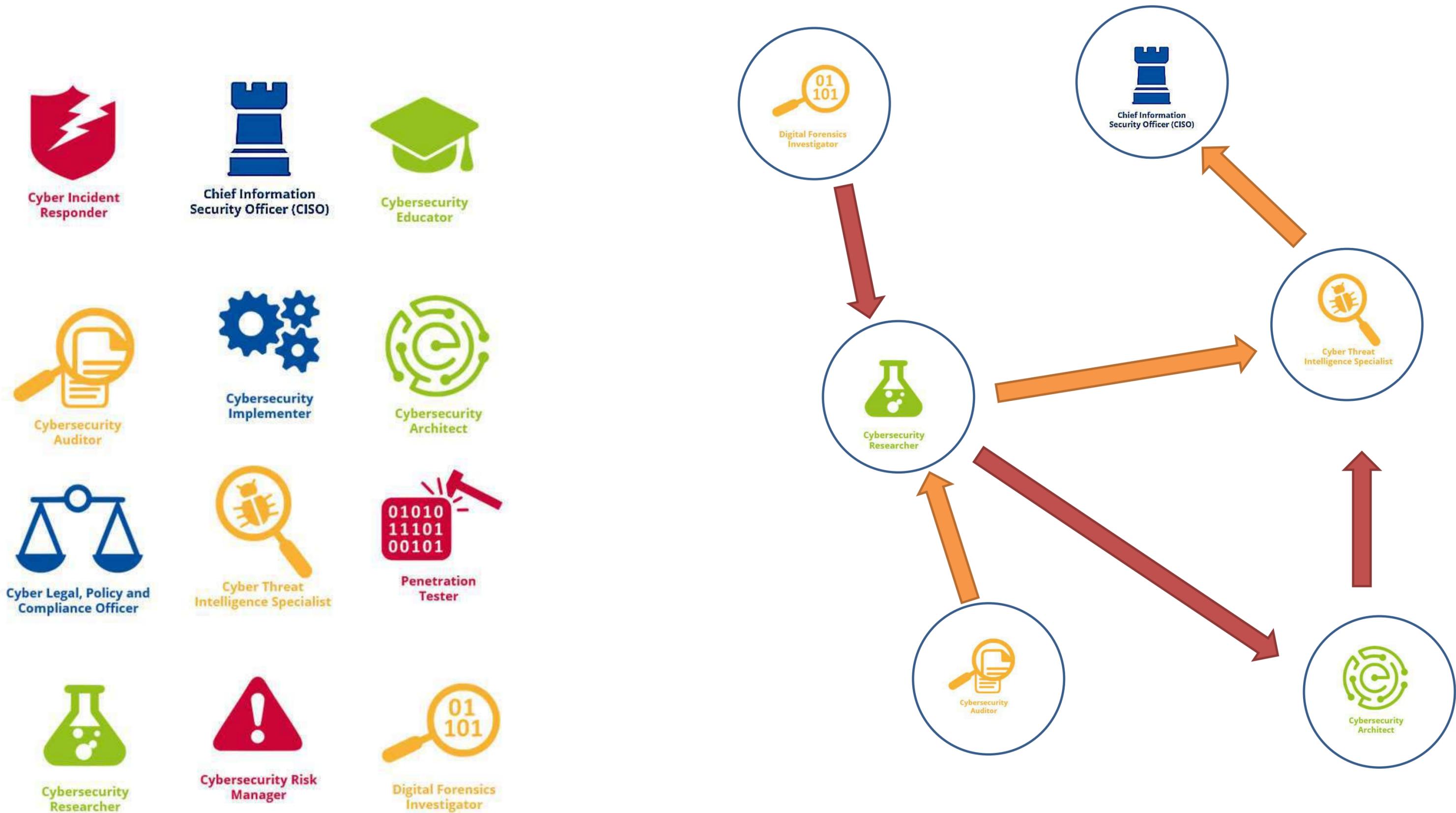
enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

ECSF
EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

SEPTEMBER 2022

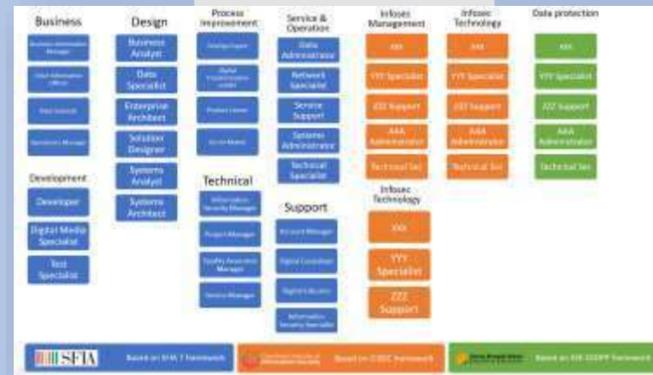


Cybersecurity Career Companion

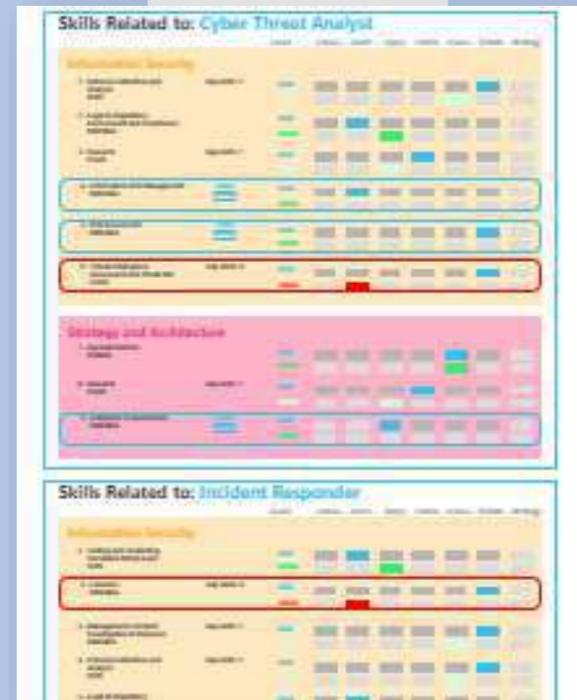
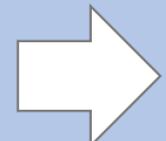
THROUGH

Life-Long learning





SELECT ROLE TO ASSESS



OBTAIN RESULTS AND IDENTIFY OTHER RELEVANT ROLES



ASSESS ALL SKILLS FOR THAT ROLE



Reference Strong skills



BUILD UPSKILLING PLAN

Identify skills mix fitness for the position

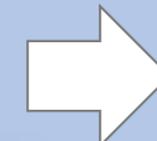
Link skills to my credentials

Link skills to my past experience



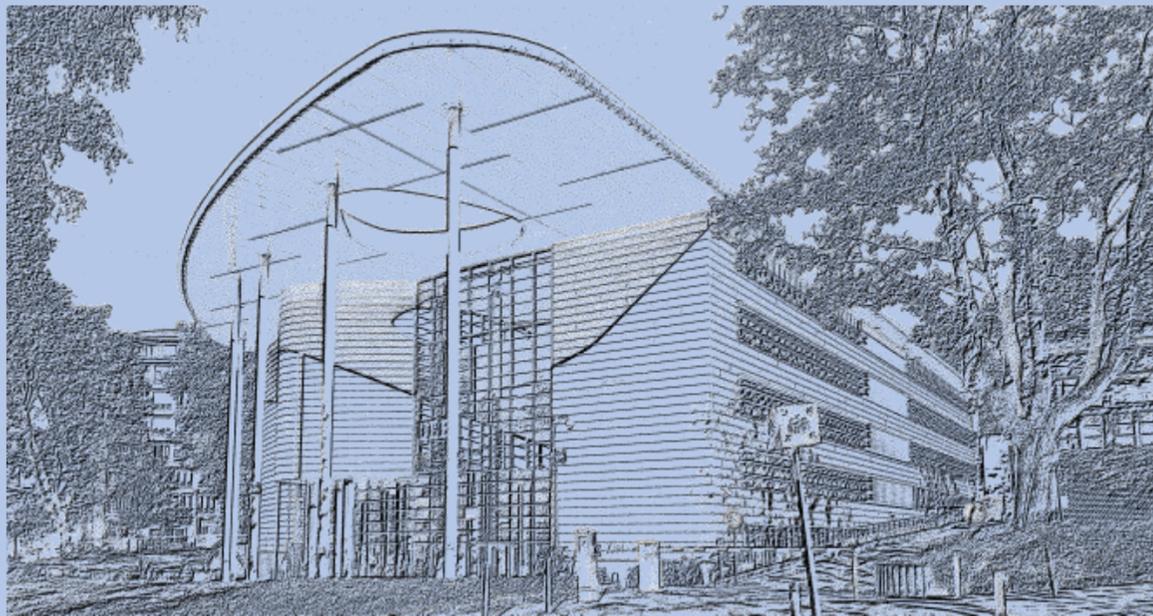
Identify skill gaps for the position

Develop my reskilling options and plan



OBTAIN THE ROLE QUALIFICATION AND UPSKILLING REPORTS

PERSONAL CURRICICULUM



IDENTIFY TARGET ROLES



Cybersecurity Implementer



Digital Forensics Investigator



Cyber Incident Responder

ASSESS SKILLS MIX AND GAPS

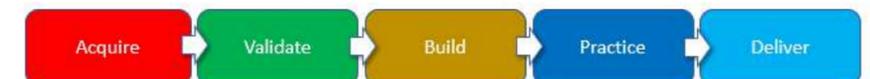


Role	Skills	Level	Score
Change and Transformation	BSM4	Senior Management	100
Change and Transformation	CPM	Change Management Planning and Management	100
Change and Transformation	TRM	Project Management	100
Information and Programmes	SLM	System Management	100
Strategy and Analysis	ESD	Enterprise System Development	100
Change and Transformation	PPM	Programme Management	100
Change and Transformation	TRM	Business Programme and Project Support	100
Strategy and Analysis	BSM2	Business IT	100
Strategy and Analysis	BSM3	Business Value	100
Development and Implementation	CCM	Cloud Management	100
Development and Implementation	CCM	Cloud Development Management	100
Information Security	ISRM	Incident Response	100
Information Security	ISRM	Incident Response Management	100
Information Security	ISRM	Incident Response Strategy	100
Information Security	ISRM	ISRM: Incident Response Strategy and Management	100
Information Security	BSM1	Business	100
Information Security	ISRM	Business Continuity Management	100
Information Security	ISRM	Business and Security Audit	100
Information Security	ISRM	Policy and Standards	100
Change and Transformation	BSM3	Business Process	100
Change and Transformation	BSM3	Business Process	100
Development and Implementation	ESD	System Design and Design	100
Change and Transformation	ESD	System Design and Design	100
Strategy and Analysis	ESD	System Design and Design	100
Strategy and Analysis	ESD	System Design and Design	100

Skills DNA

DEVELOP OWN CURRICULUM

CYBERSECURITY EXECUTIVE EDUCATION



Professor, founder and Academic Director of Digital Governance and Trust at Solvay Lifelong Learning
Co-Founder of the Belgian Cybersecurity Coalition
Co-founder DPO Circle
Member of the Advisory Board: Agoria, BECI, CIONET, ISACA, Belgian Cybersecurity Coalition
Founder at Ataya & partners, advisory firm (atayapartners.com)
Past International Vice President at ISACA
Past Partner Ernst & Young
Past Deputy International CIO ITT World Directories
Contributor: COBIT, CISM, CGEIT, VALIT.



Georges Ataya

[Linkedin: ataya](#)
gataya@solvay.edu
+32475705709

Thank You



Solvay Lifelong Learning
BRUSSELS SCHOOL. ECONOMICS. MANAGEMENT