GRC

be connected

30
MARCH

EXPERIENCE
SHARING
EVENT

CYBER SECURITY
COALITION.be

Solvay Lifelong Learning
BRUSSELS SCHOOL. ECONOMICS. MANAGEMENT

ISACA.
Belgium Chapter

CGEIT. CISA. CISM. CRISC. CSX-P

Skills and roles for cybersecurity

Georges Ataya
30 March 2023

DIGITAL GOVERNANCE

“CISO”

85% of enterprises have a CISO

“CIO”

Emerged as a job title in the 1980's

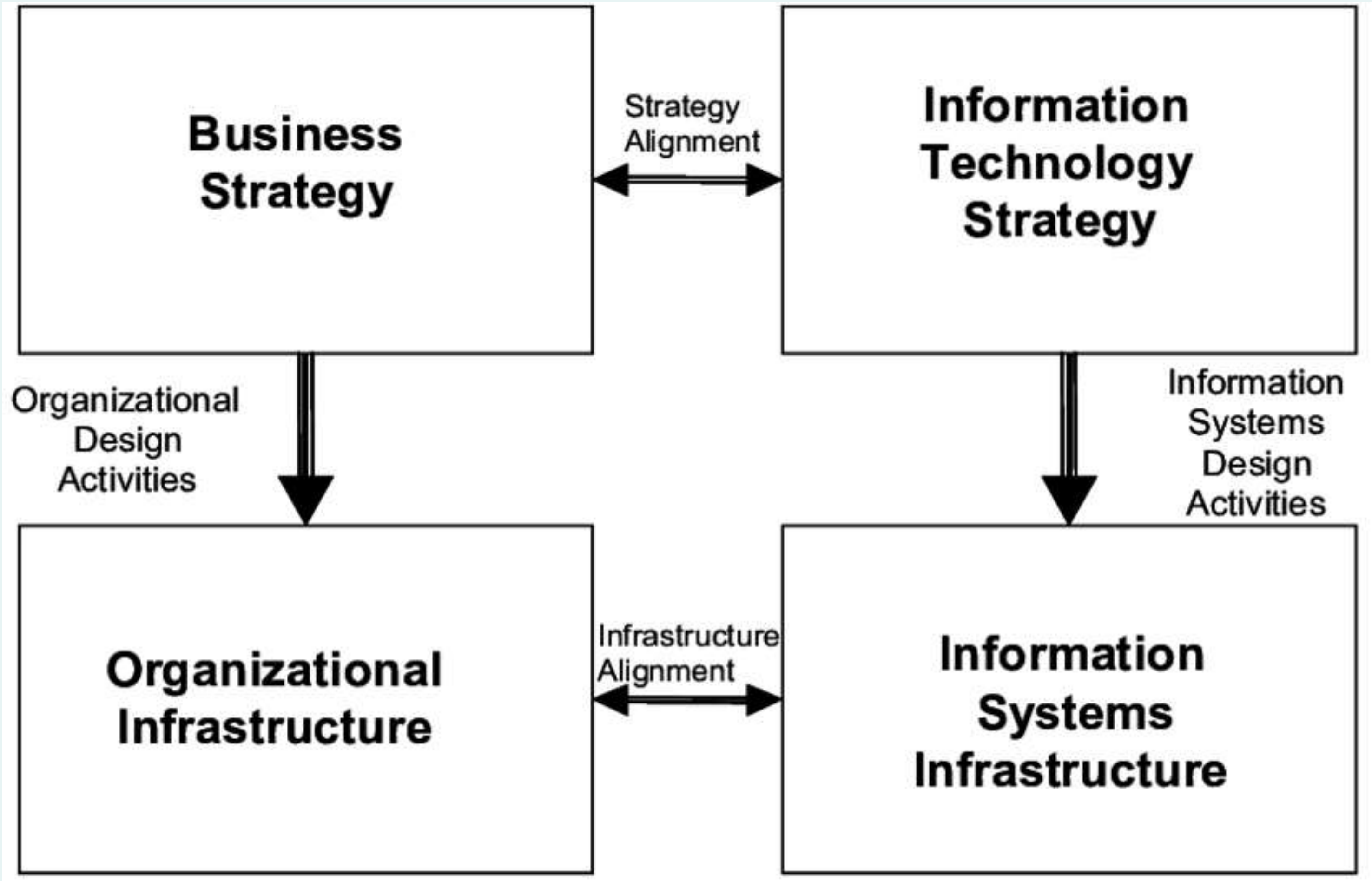
“CDO”

“CRO”

DIGITAL GOVERNANCE

“CISO”
85% of enterprises have a CISO

Alignment

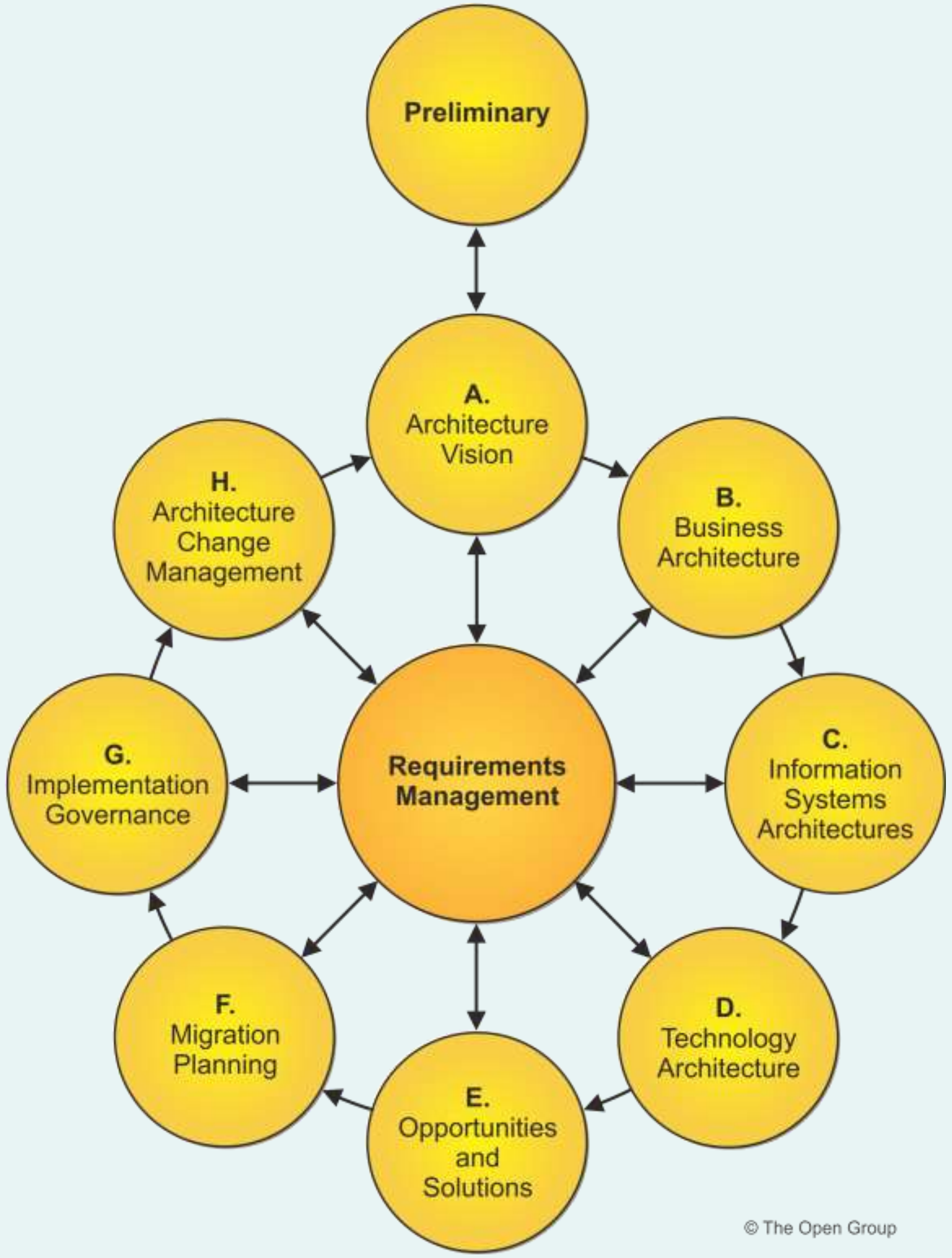

Business Strategy
Strategy Alignment
Information Technology Strategy
Organizational Design Activities
Information Systems Design Activities
Organizational Infrastructure
Infrastructure Alignment
Information Systems Infrastructure

Henderson and Venkatraman (1993)

DIGITAL GOVERNANCE

Alignment

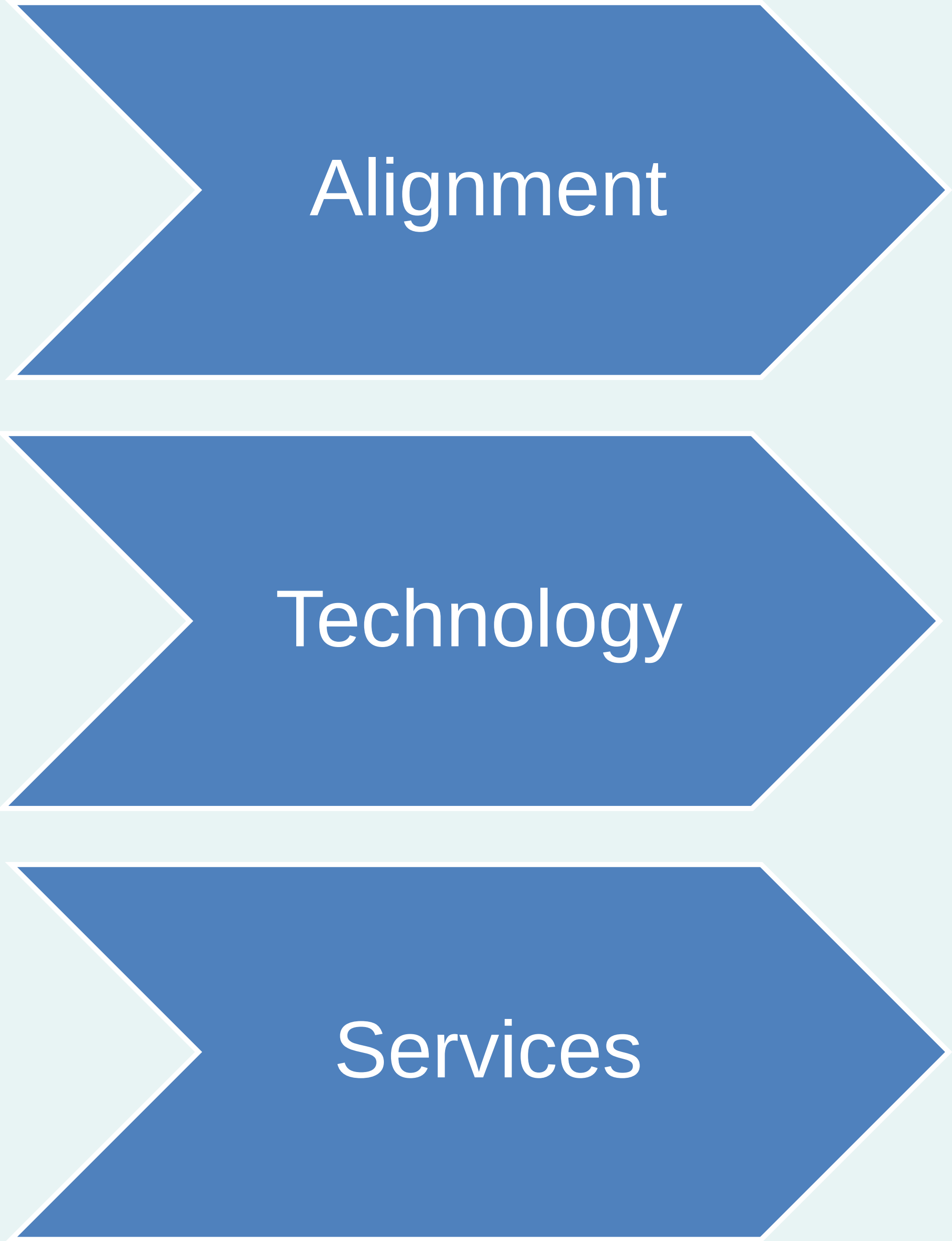
Technology


Preliminary
A. Architecture Vision
B. Business Architecture
C. Information Systems Architectures
D. Technology Architecture
E. Opportunities and Solutions
F. Migration Planning
G. Implementation Governance
H. Architecture Change Management
Requirements Management

© The Open Group

TOGAF

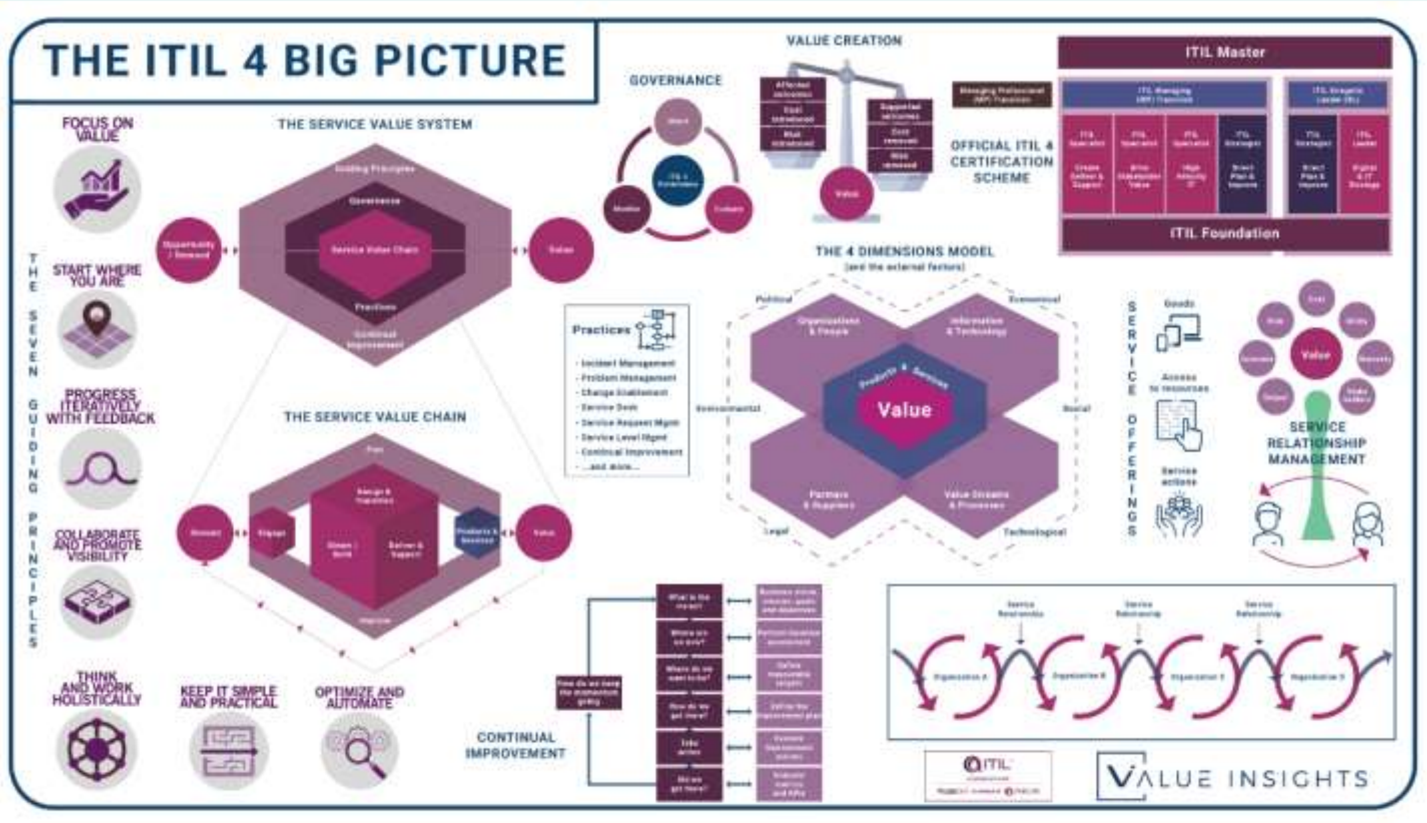
DIGITAL GOVERNANCE



Alignment

Technology

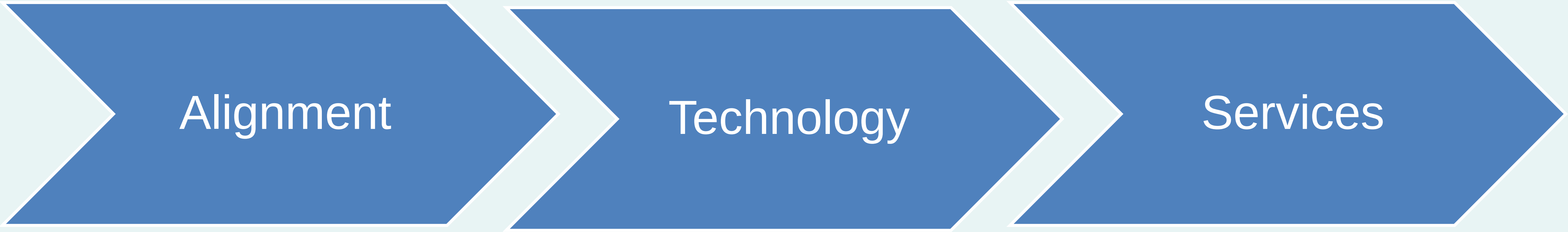
Services



Source: Value insights

ITIL Service Management

DIGITAL GOVERNANCE


Alignment

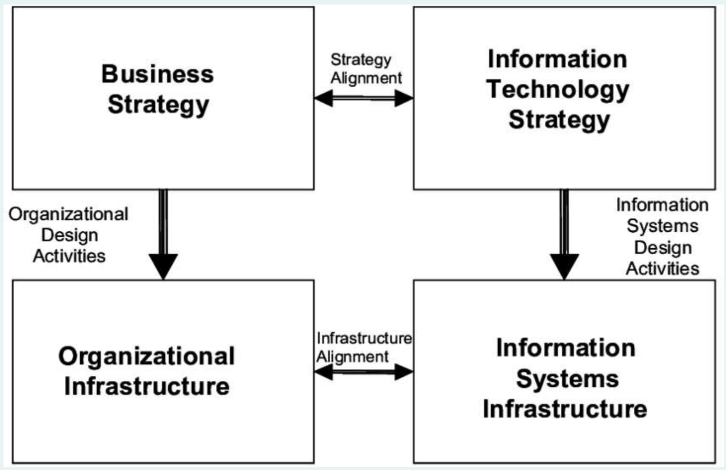
Technology

Services

Plan

Build

Run


Business Strategy

Strategy Alignment

Information Technology Strategy

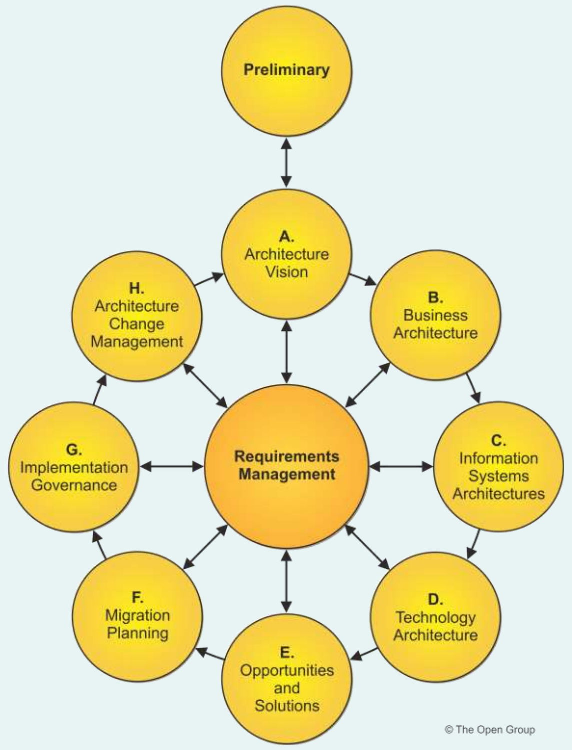
Organizational Design Activities

Information Systems Design Activities

Organizational Infrastructure

Infrastructure Alignment

Information Systems Infrastructure


Preliminary

A. Architecture Vision

B. Business Architecture

C. Information Systems Architectures

D. Technology Architecture

E. Opportunities and Solutions

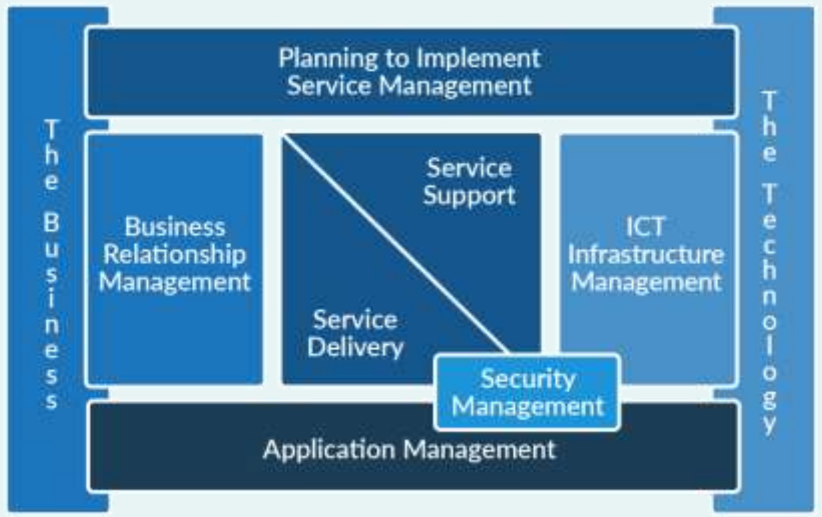
F. Migration Planning

G. Implementation Governance

H. Architecture Change Management

Requirements Management

© The Open Group


The Business

Planning to Implement Service Management

Business Relationship Management

Service Support

Service Delivery

ICT Infrastructure Management

Security Management

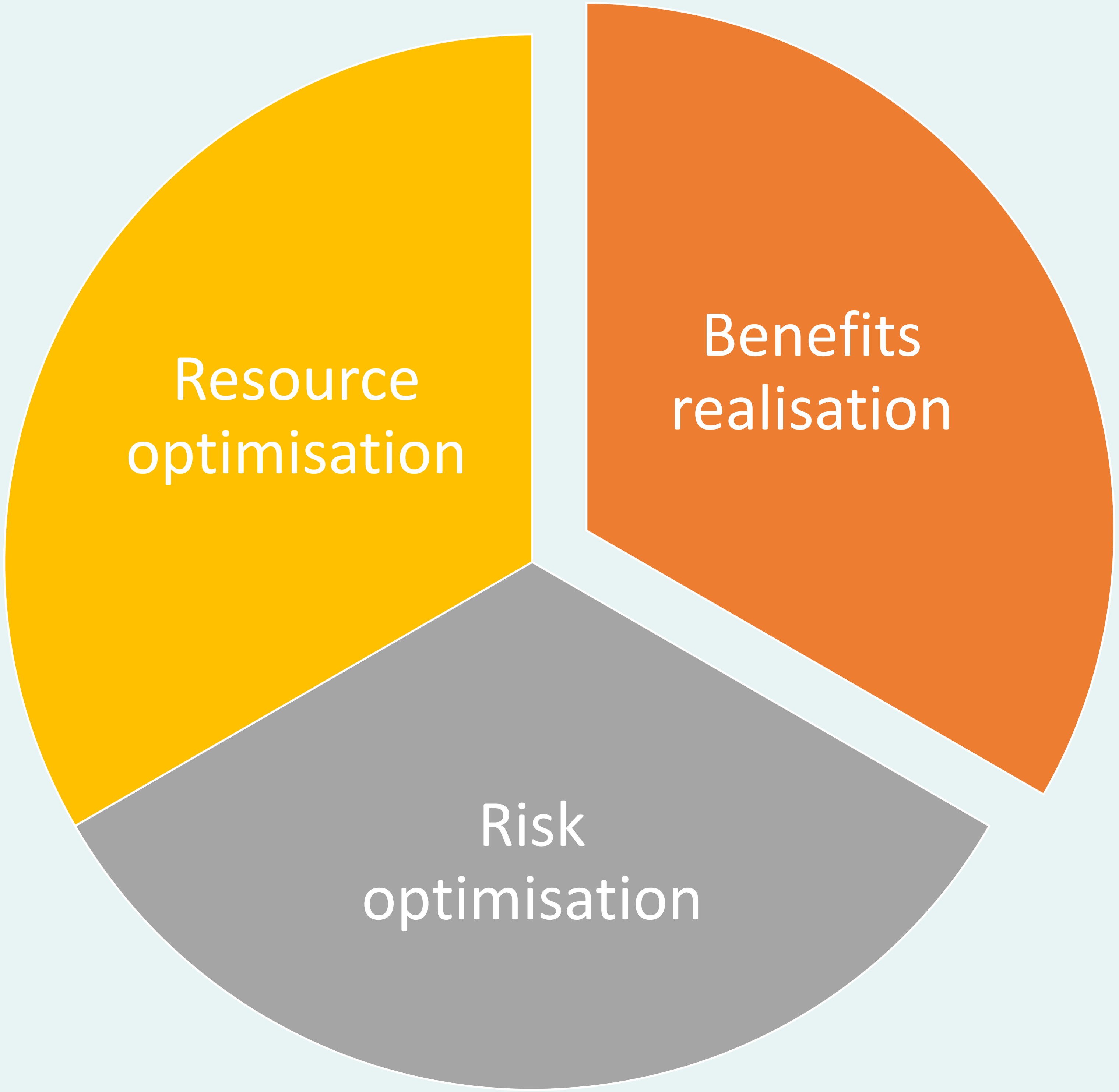
Application Management

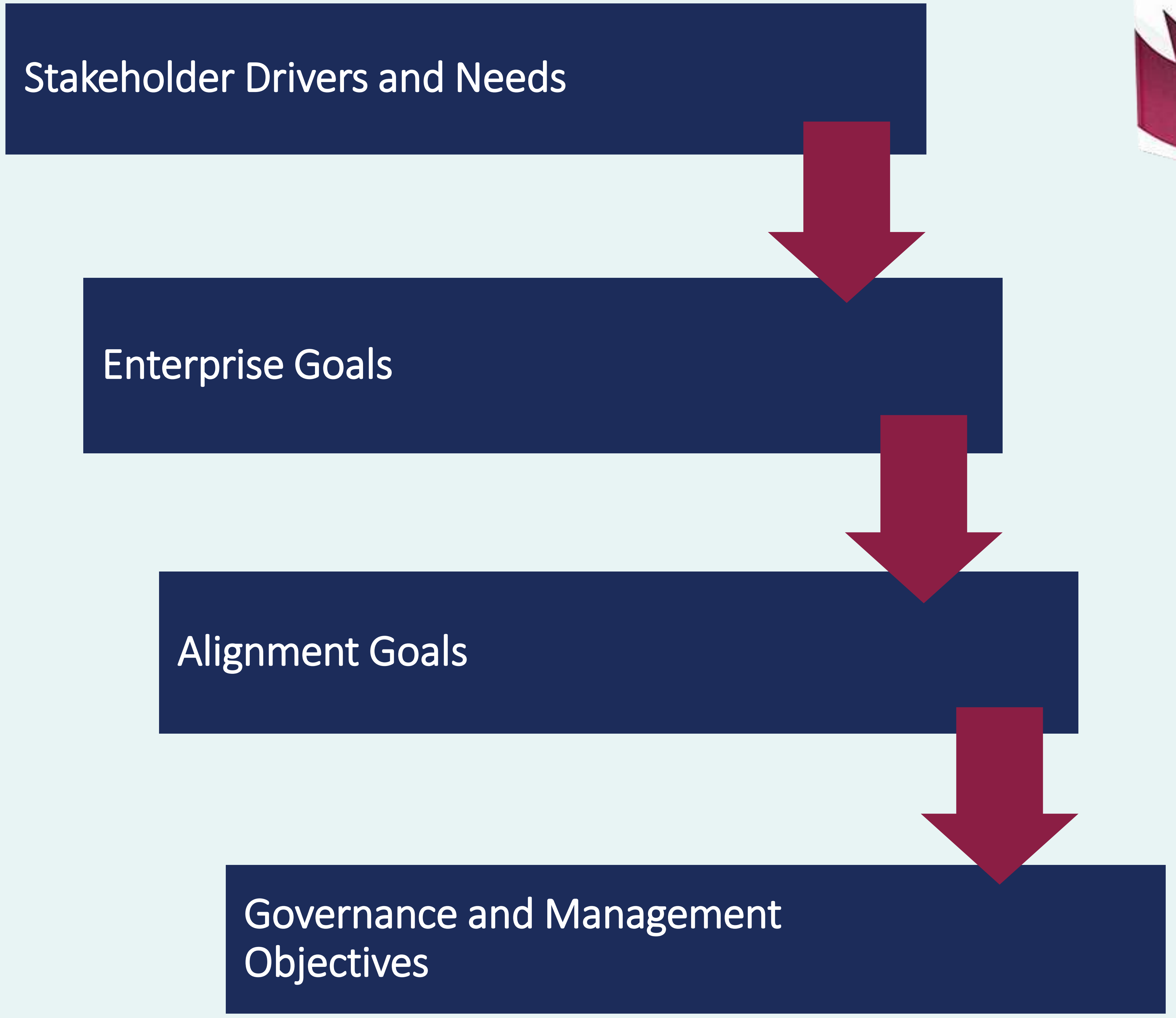
The Technology

© 2023 Copyright Georges Ataya & Solvay.edu

ENTERPRISE GOVERNANCE

of DIGITAL ACTIVITIES





Stakeholder Drivers and Needs

Enterprise Goals

Alignment Goals

Governance and Management Objectives

COBIT 2019

Designing an Information and Technology Governance Solution

COBIT 2019

Governance and Management Objectives

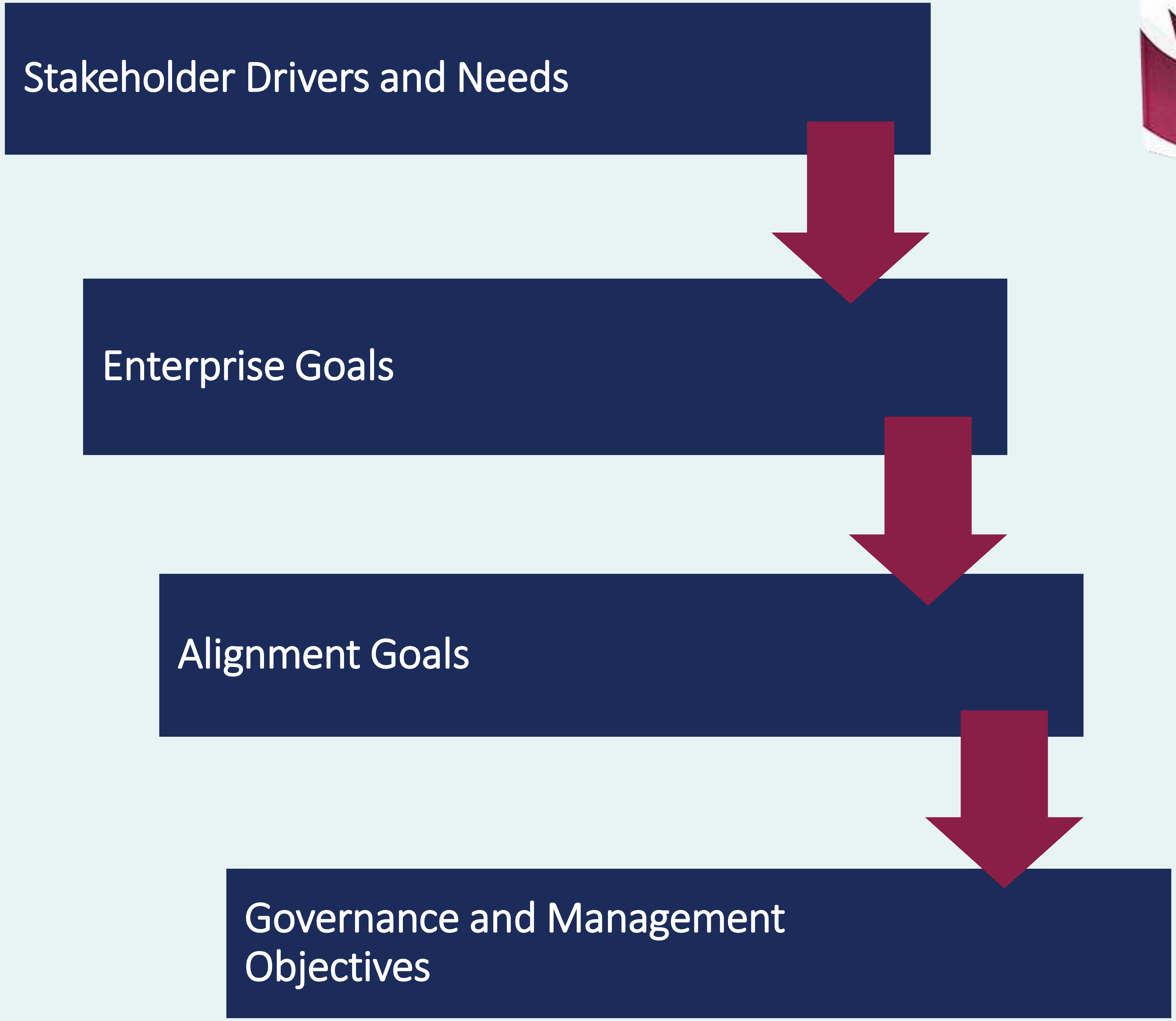
COBIT 2019

Governance and Management Objectives

COBIT 2019

Implementing and Optimizing an Information and Technology Governance Solution

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



Stakeholder Drivers and Needs

Enterprise Goals

Alignment Goals

Governance and Management Objectives

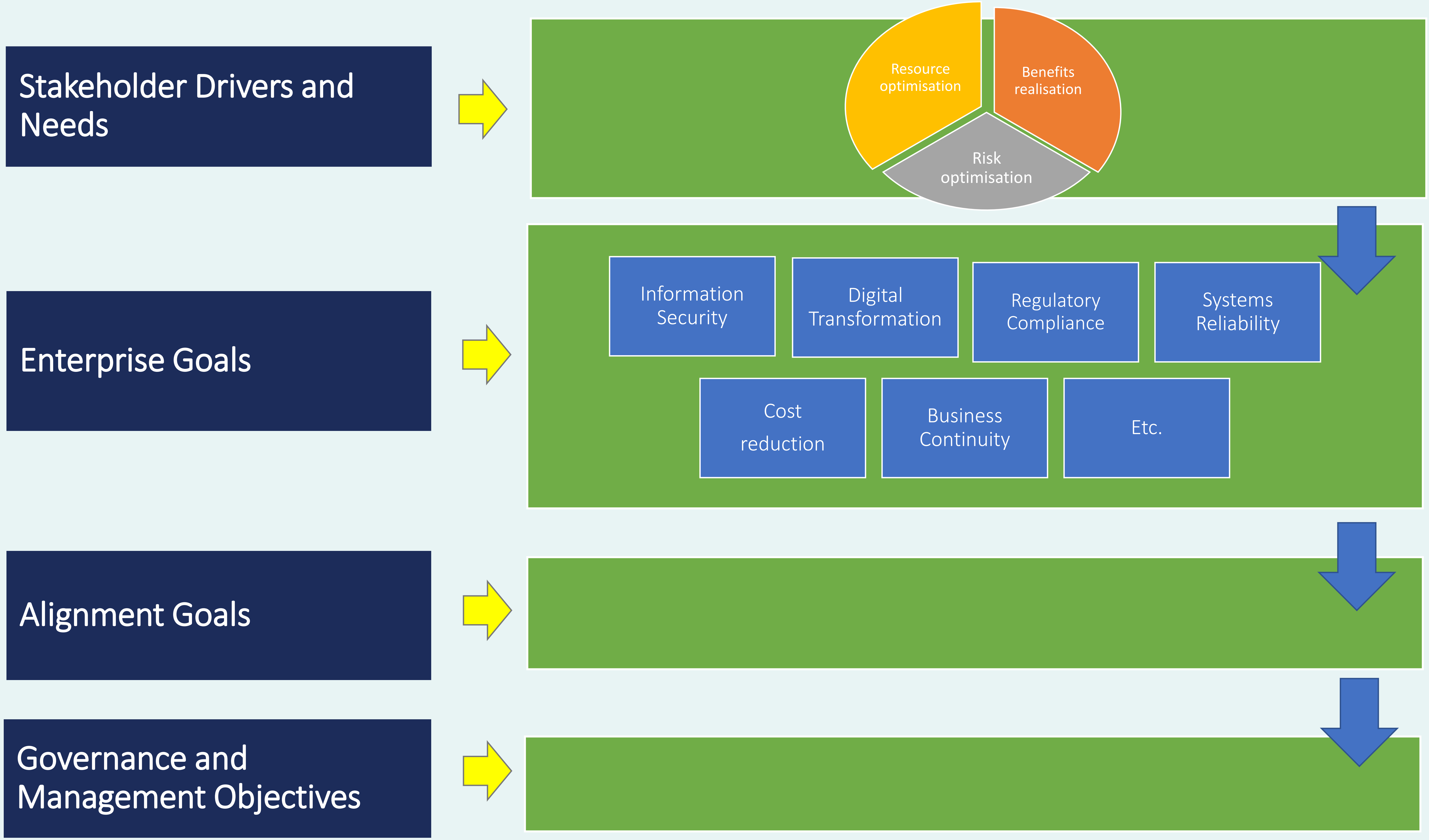
COBIT 2019
Designing an Information and Technology Governance Solution
COBIT 2019
Governance and Management Objectives
COBIT 2019
Governance and Management Objectives
COBIT 2019
Implementing and Optimizing an Information and Technology Governance Solution

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

Resource optimisation

Benefits realisation

Risk optimisation

Enterprise Goals

Information Security

Digital Transformation

Regulatory Compliance

Systems Reliability

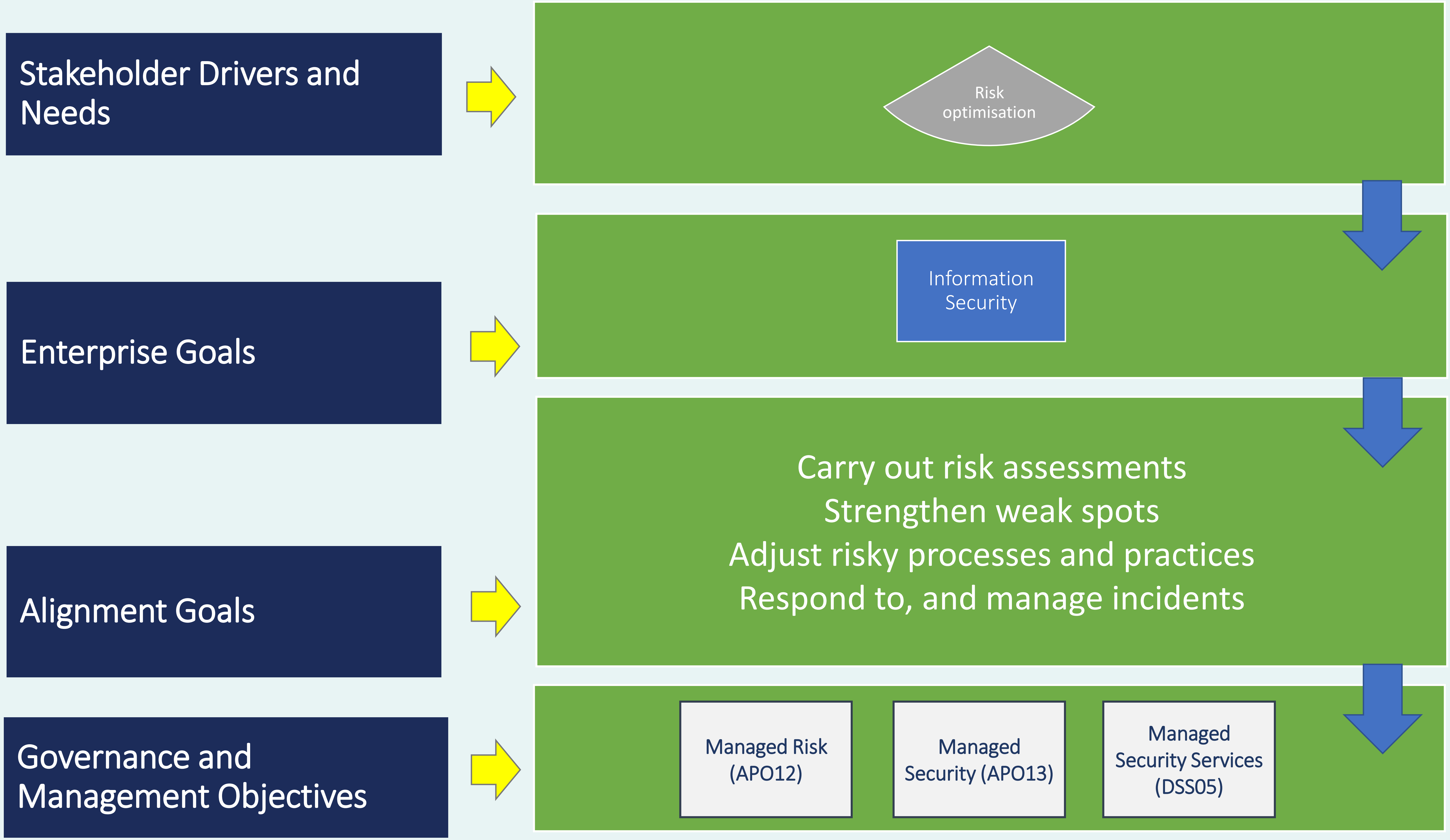
Cost reduction

Business Continuity

Etc.

Alignment Goals

Governance and Management Objectives



Stakeholder Drivers and Needs

Risk optimisation

Enterprise Goals

Information Security

Alignment Goals

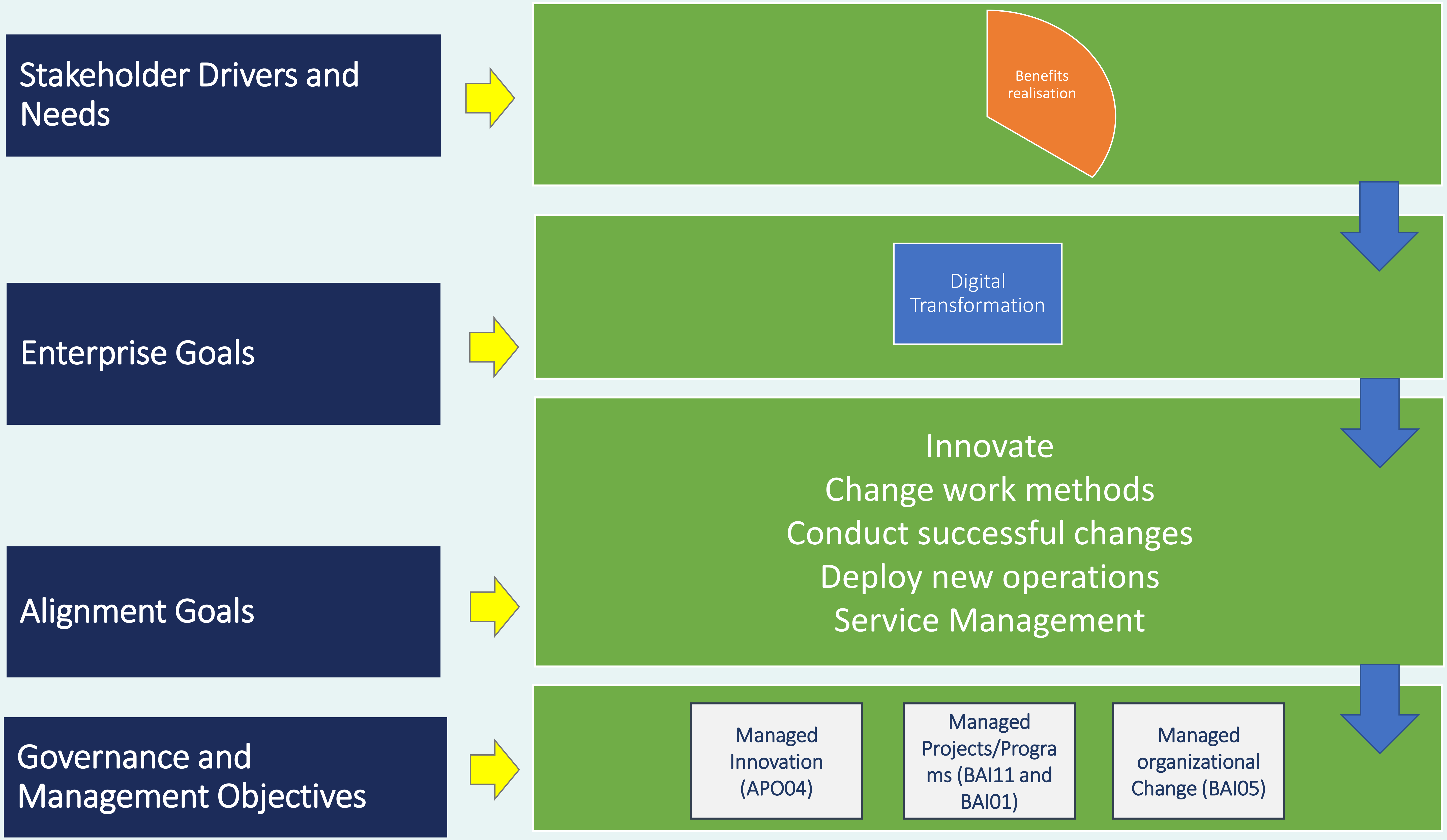
Carry out risk assessments
Strengthen weak spots
Adjust risky processes and practices
Respond to, and manage incidents

Governance and Management Objectives

Managed Risk (APO12)

Managed Security (APO13)

Managed Security Services (DSS05)



Stakeholder Drivers and Needs

Benefits realisation

Enterprise Goals

Digital Transformation

Alignment Goals

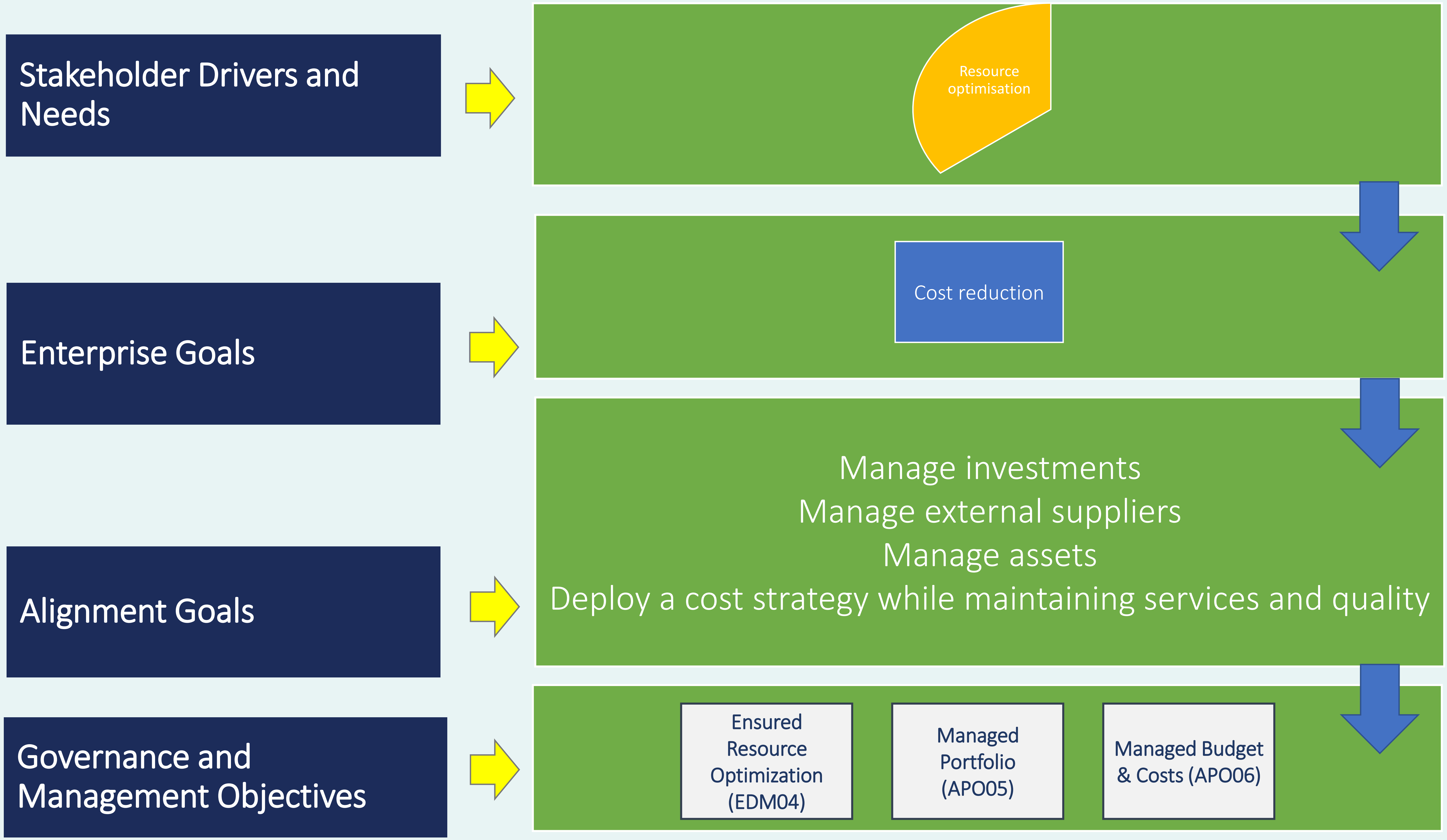
Innovate
Change work methods
Conduct successful changes
Deploy new operations
Service Management

Governance and Management Objectives

Managed Innovation (APO04)

Managed Projects/Programs (BAI11 and BAI01)

Managed organizational Change (BAI05)



Stakeholder Drivers and Needs

Resource optimisation

Enterprise Goals

Cost reduction

Alignment Goals

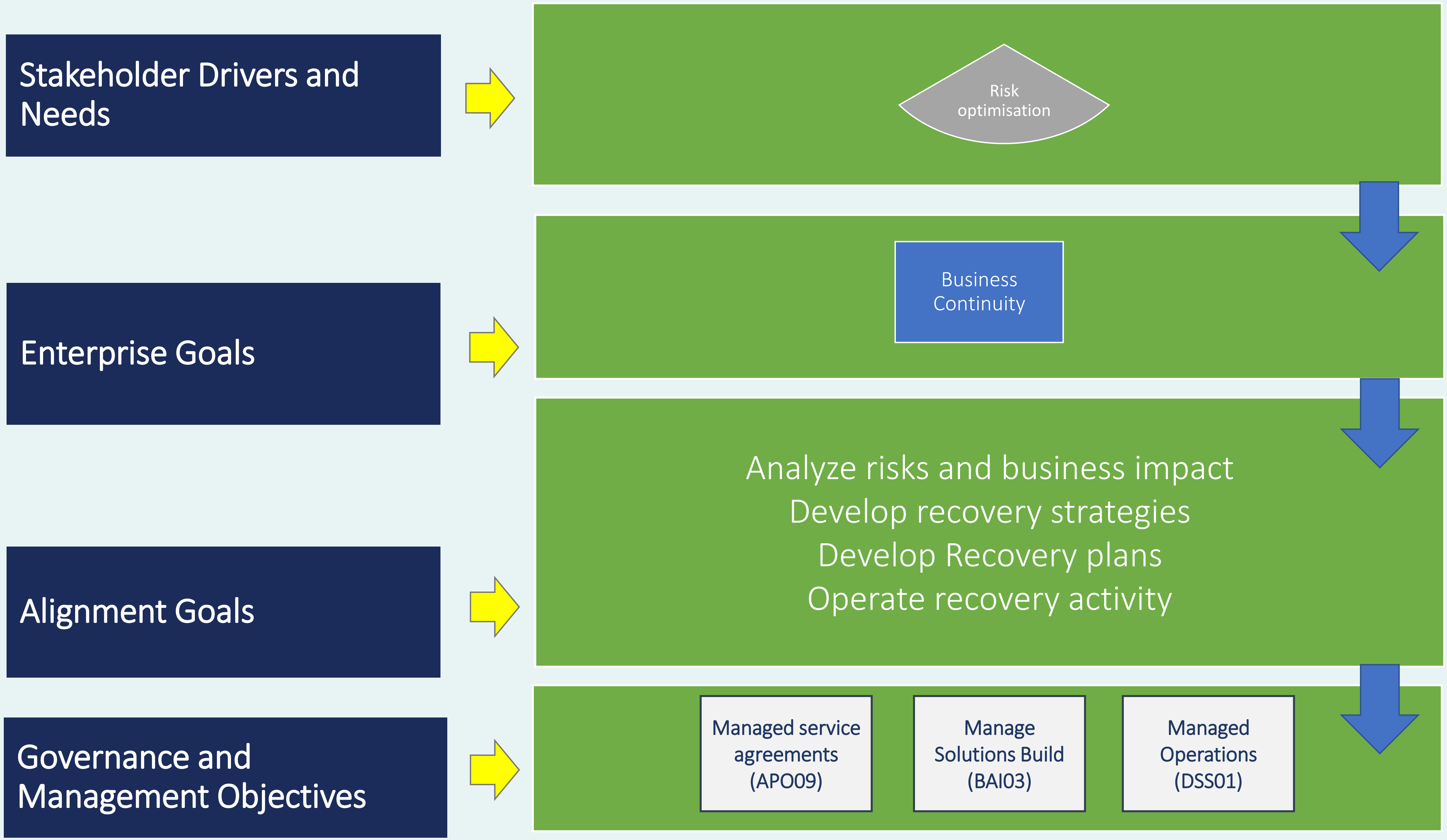
Manage investments
Manage external suppliers
Manage assets
Deploy a cost strategy while maintaining services and quality

Governance and Management Objectives

Ensured Resource Optimization (EDM04)

Managed Portfolio (APO05)

Managed Budget & Costs (APO06)



Stakeholder Drivers and Needs

Risk optimisation

Enterprise Goals

Business Continuity

Alignment Goals

Analyze risks and business impact
Develop recovery strategies
Develop Recovery plans
Operate recovery activity

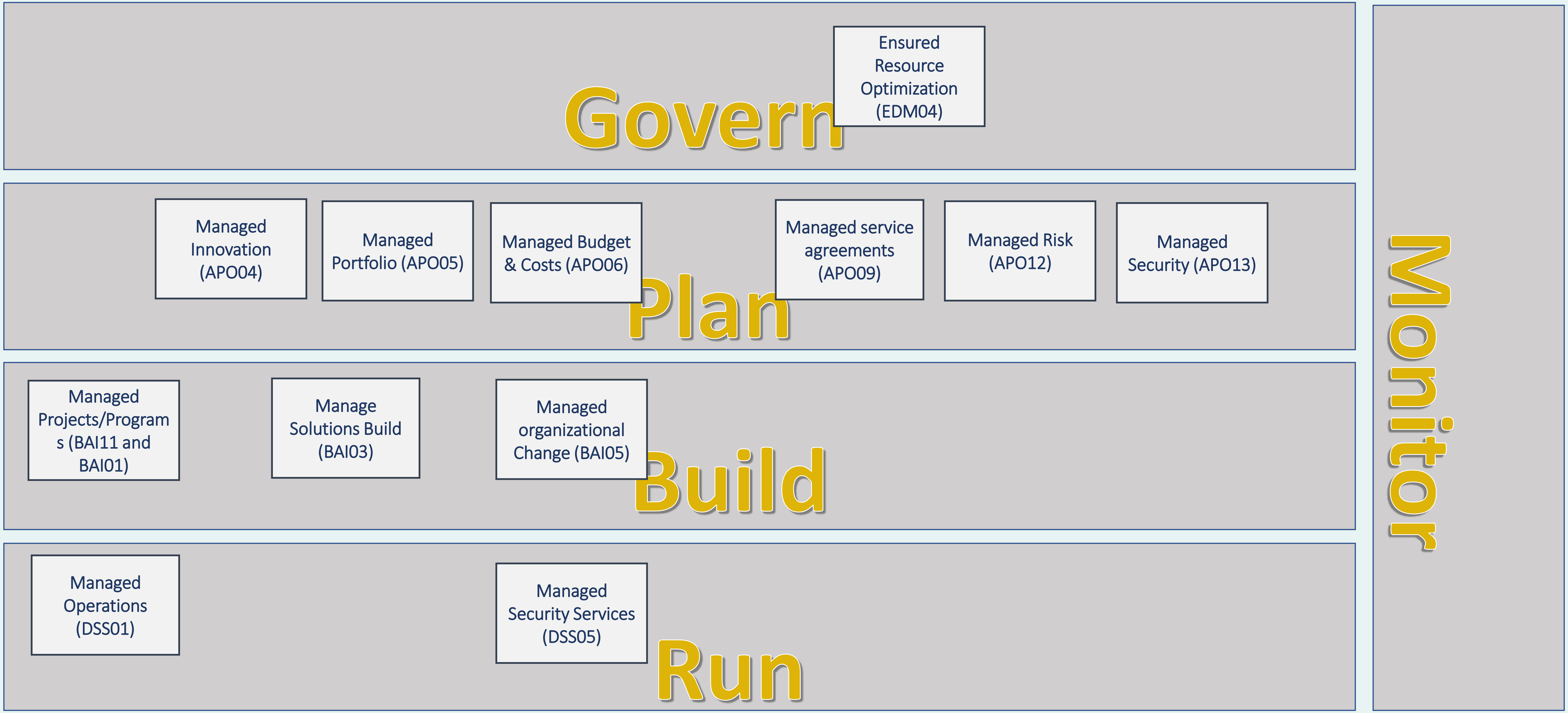
Governance and Management Objectives

Managed service agreements (APO09)

Manage Solutions Build (BAI03)

Managed Operations (DSS01)

Managed Innovation (APO04)	Managed Projects/Programs (BAI11 and BAI01)	Managed organizational Change (BAI05)
Managed Risk (APO12)	Managed Security (APO13)	Managed Security Services (DSS05)
Ensured Resource Optimization (EDM04)	Managed Portfolio (APO05)	Managed Budget & Costs (APO06)
Managed service agreements (APO09)	Manage Solutions Build (BAI03)	Managed Operations (DSS01)



Govern

Ensured Resource Optimization (EDM04)

Plan

Managed Innovation (APO04)

Managed Portfolio (APO05)

Managed Budget & Costs (APO06)

Managed service agreements (APO09)

Managed Risk (APO12)

Managed Security (APO13)

Build

Managed Projects/Programs (BAI11 and BAI01)

Manage Solutions Build (BAI03)

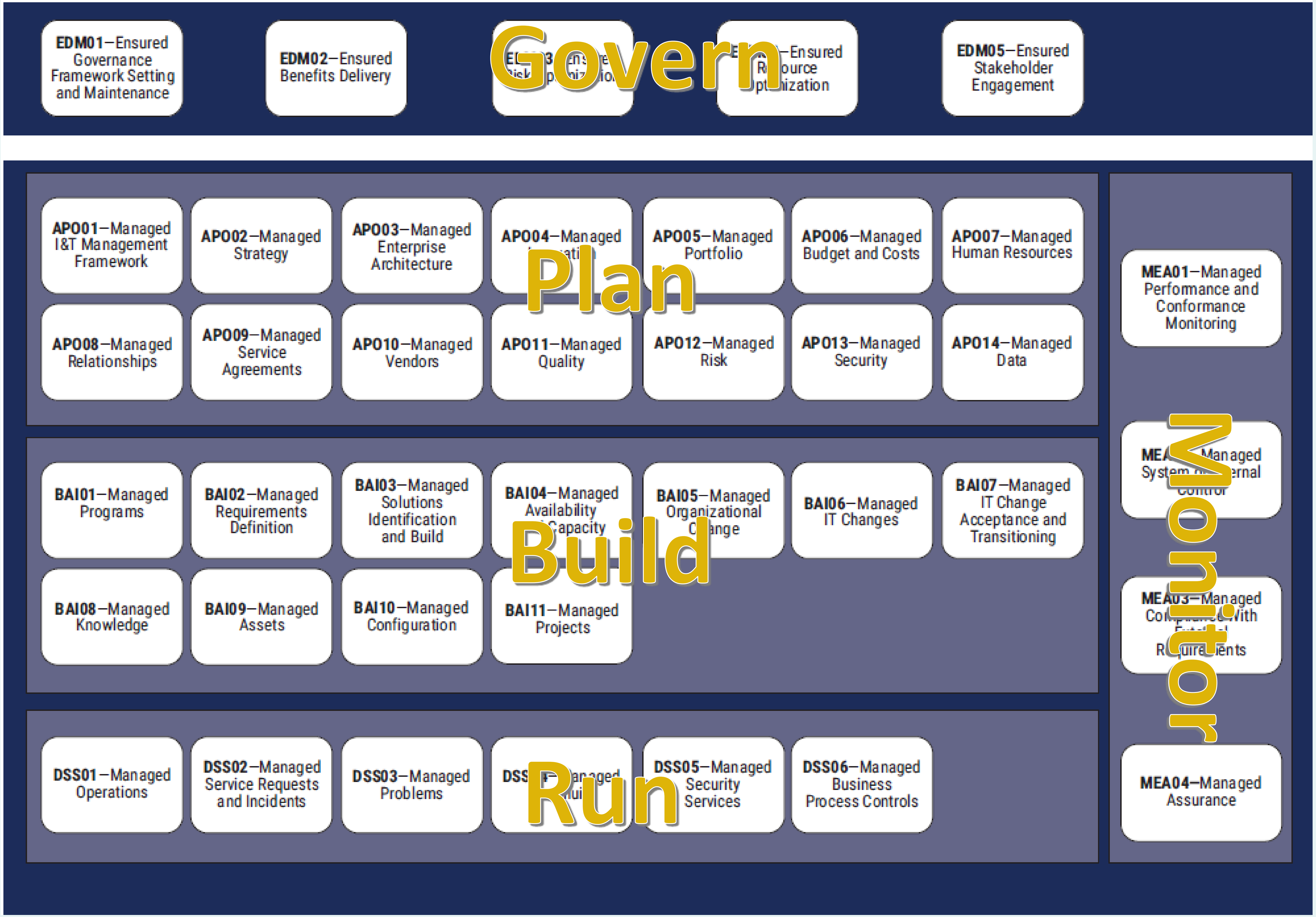
Managed organizational Change (BAI05)

Run

Managed Operations (DSS01)

Managed Security Services (DSS05)

Monitor



Govern

EDM01—Ensured Governance Framework Setting and Maintenance

EDM02—Ensured Benefits Delivery

EDM03—Ensured Risk Optimization

EDM04—Ensured Resource Optimization

EDM05—Ensured Stakeholder Engagement

Plan

APO01—Managed I&T Management Framework

APO02—Managed Strategy

APO03—Managed Enterprise Architecture

APO04—Managed Innovation

APO05—Managed Portfolio

APO06—Managed Budget and Costs

APO07—Managed Human Resources

APO08—Managed Relationships

APO09—Managed Service Agreements

APO10—Managed Vendors

APO11—Managed Quality

APO12—Managed Risk

APO13—Managed Security

APO14—Managed Data

Build

BAI01—Managed Programs

BAI02—Managed Requirements Definition

BAI03—Managed Solutions Identification and Build

BAI04—Managed Availability and Capacity

BAI05—Managed Organizational Change

BAI06—Managed IT Changes

BAI07—Managed IT Change Acceptance and Transitioning

BAI08—Managed Knowledge

BAI09—Managed Assets

BAI10—Managed Configuration

BAI11—Managed Projects

Run

DSS01—Managed Operations

DSS02—Managed Service Requests and Incidents

DSS03—Managed Problems

DSS04—Managed Continuity

DSS05—Managed Security Services

DSS06—Managed Business Process Controls

Monitor

MEA01—Managed Performance and Conformance Monitoring

MEA02—Managed System of Internal Control

MEA03—Managed Compliance With External Requirements

MEA04—Managed Assurance

EDM01 Governance Framework Setting and Maintenance

EDM03 Risk Optimization

EDM05 Stakeholder Engagement

APO04 Innovation

BAI01 Programs

EDM02 Benefits Delivery

EDM04 Resource Optimization

DSS05 Security Services

APO05 Portfolio

APO01 Management Framework

APO02 Strategy

BAI05 Organizational Change

APO03 Enterprise Architecture

BAI04 Availability and Capacity

APO07 Human Resources

APO08 Relationships

DSS03 Problems

APO10 Vendors

APO13 Security

APO14 Data

APO09 Service Agreements

BAI07 IT Change Acceptance and Transitioning

BAI10 Configuration

BAI08 Knowledge

APO06 Budget and Costs

BAI03 Solutions Identification and

MEA01 Performance and Conformance

APO12 Risk

BAI06 IT Changes

BAI02 Requirements Definition

APO14 Communication

DSS02 Service Requests and Incidents

DSS04 Continuity

DSS06 Business Process Controls

APO11 Quality

DSS01 Operations

MEA02 System of Internal Control

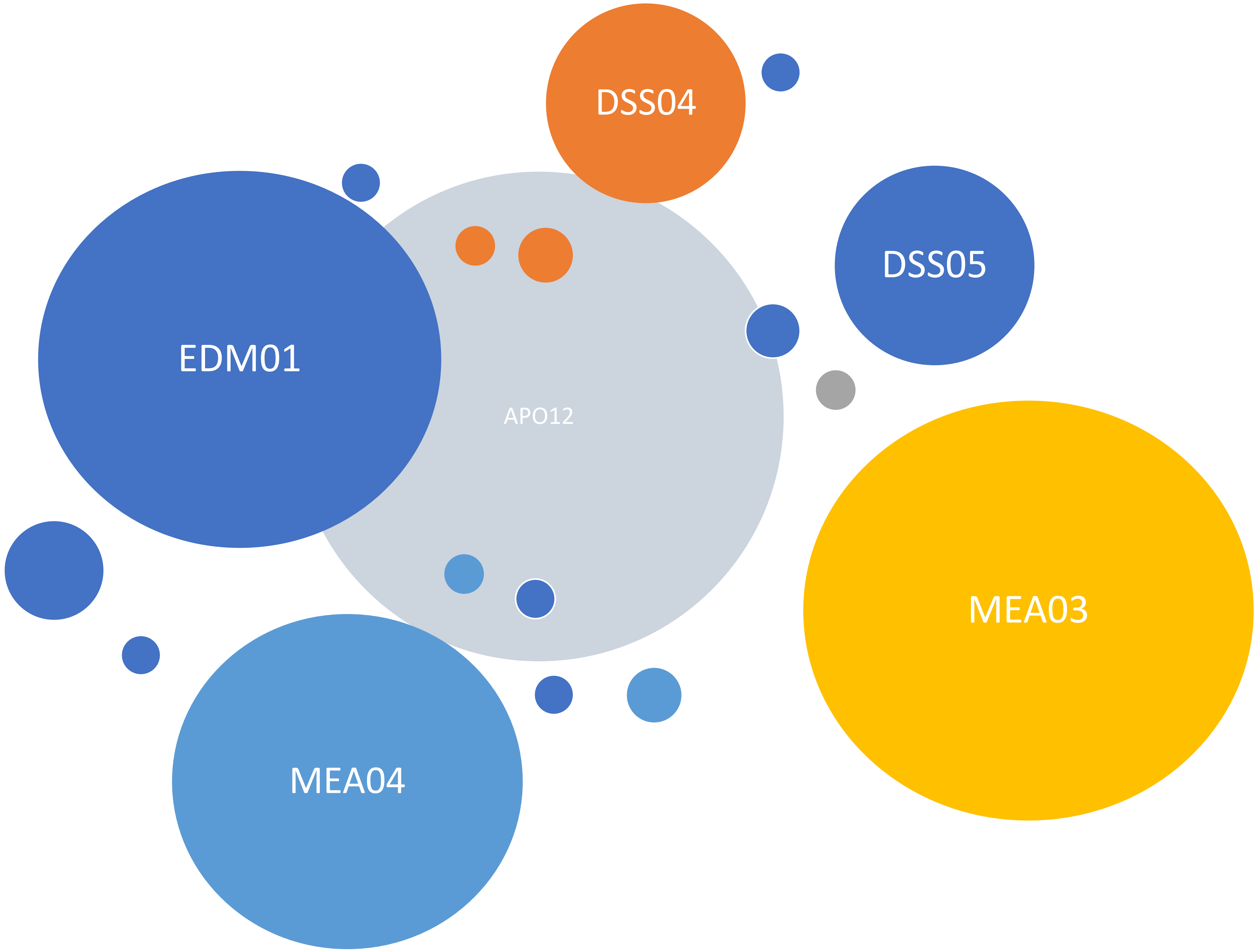
MEA03 Compliance With External Requirements

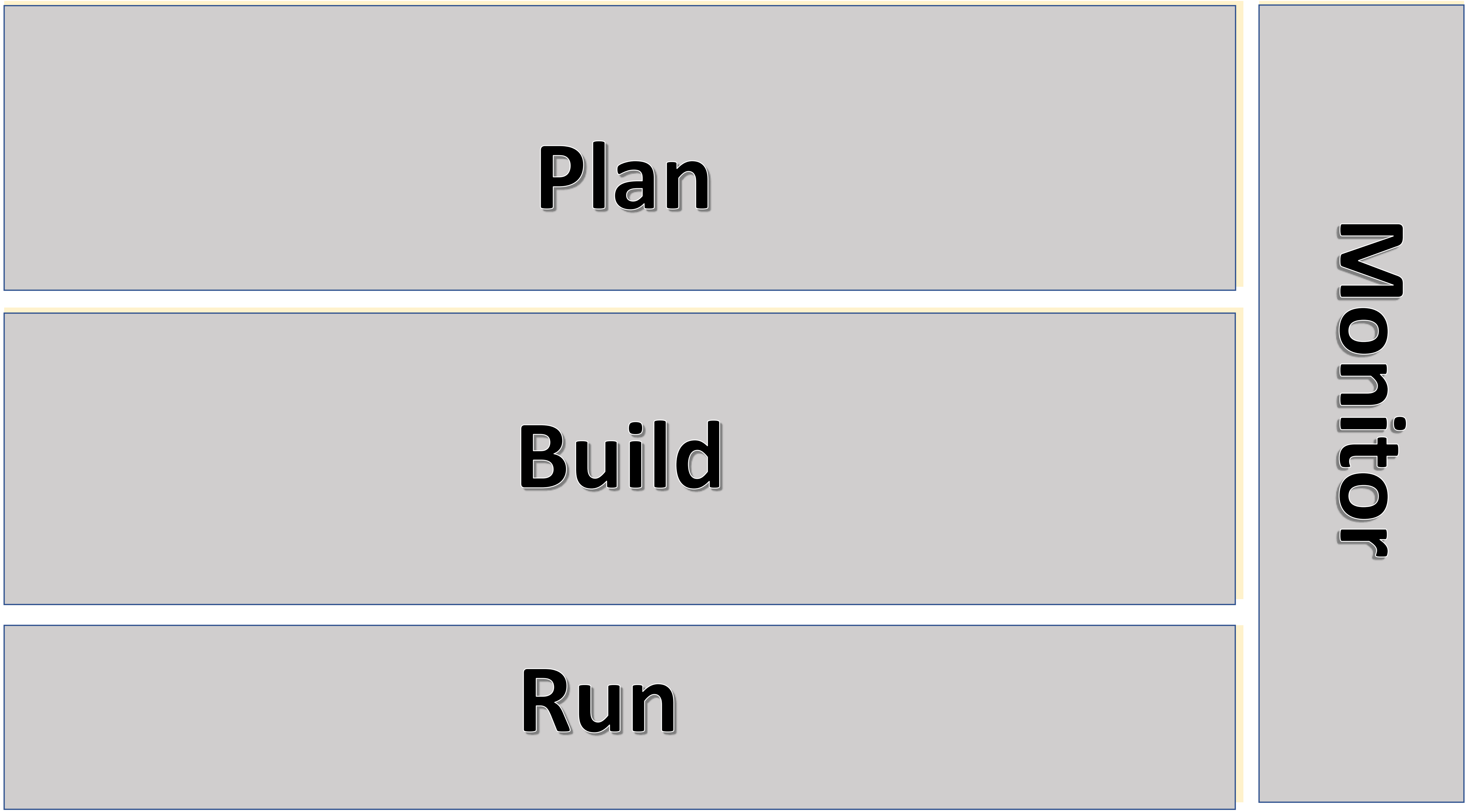
BAI09 Assets

MEA04 Assurance

Mapping Compliance Requirements

to Governance and Management Objectives (source COBIT annexes)





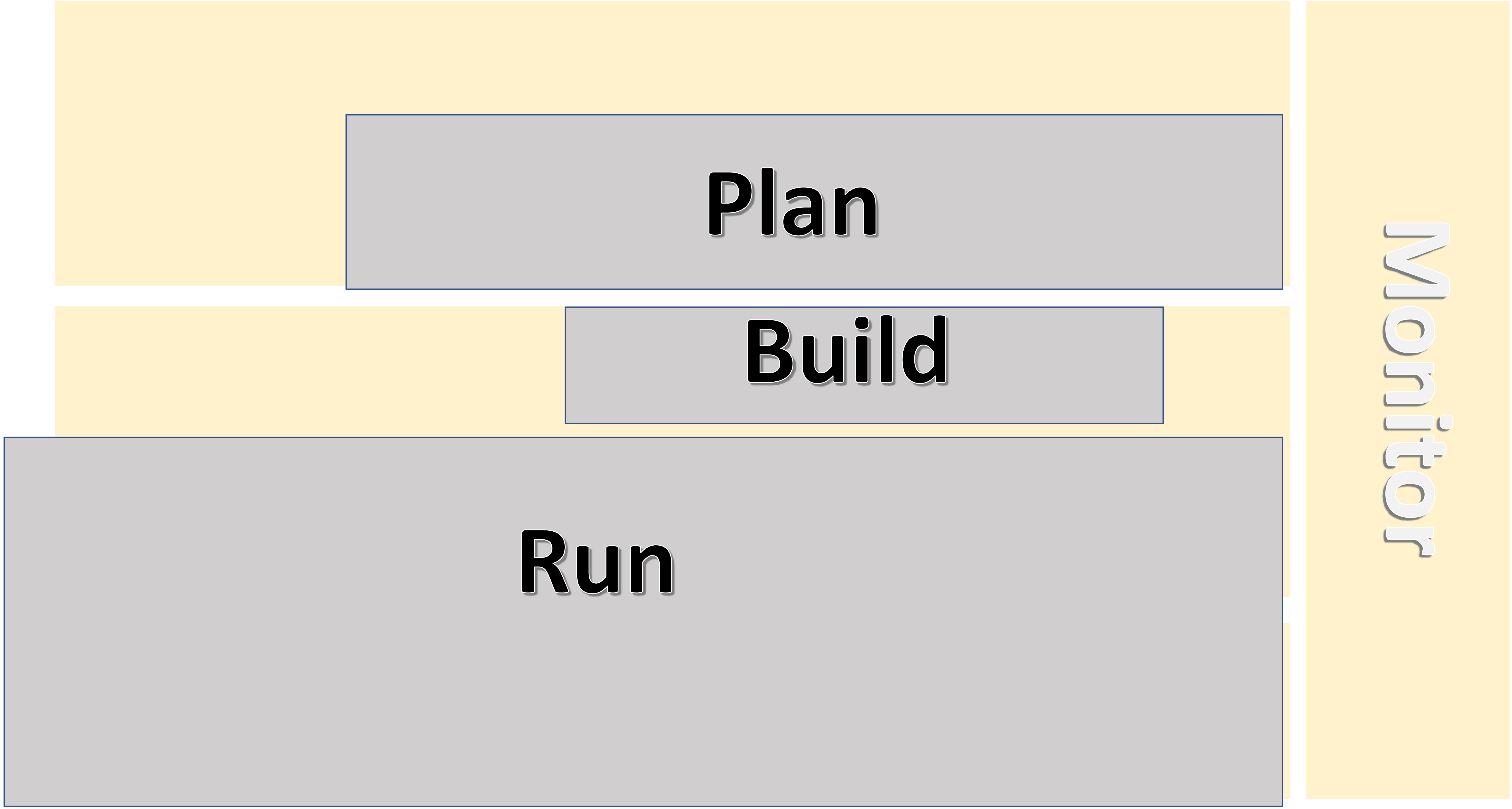
Plan

Build

Run

Monitor

Sample organisation 1



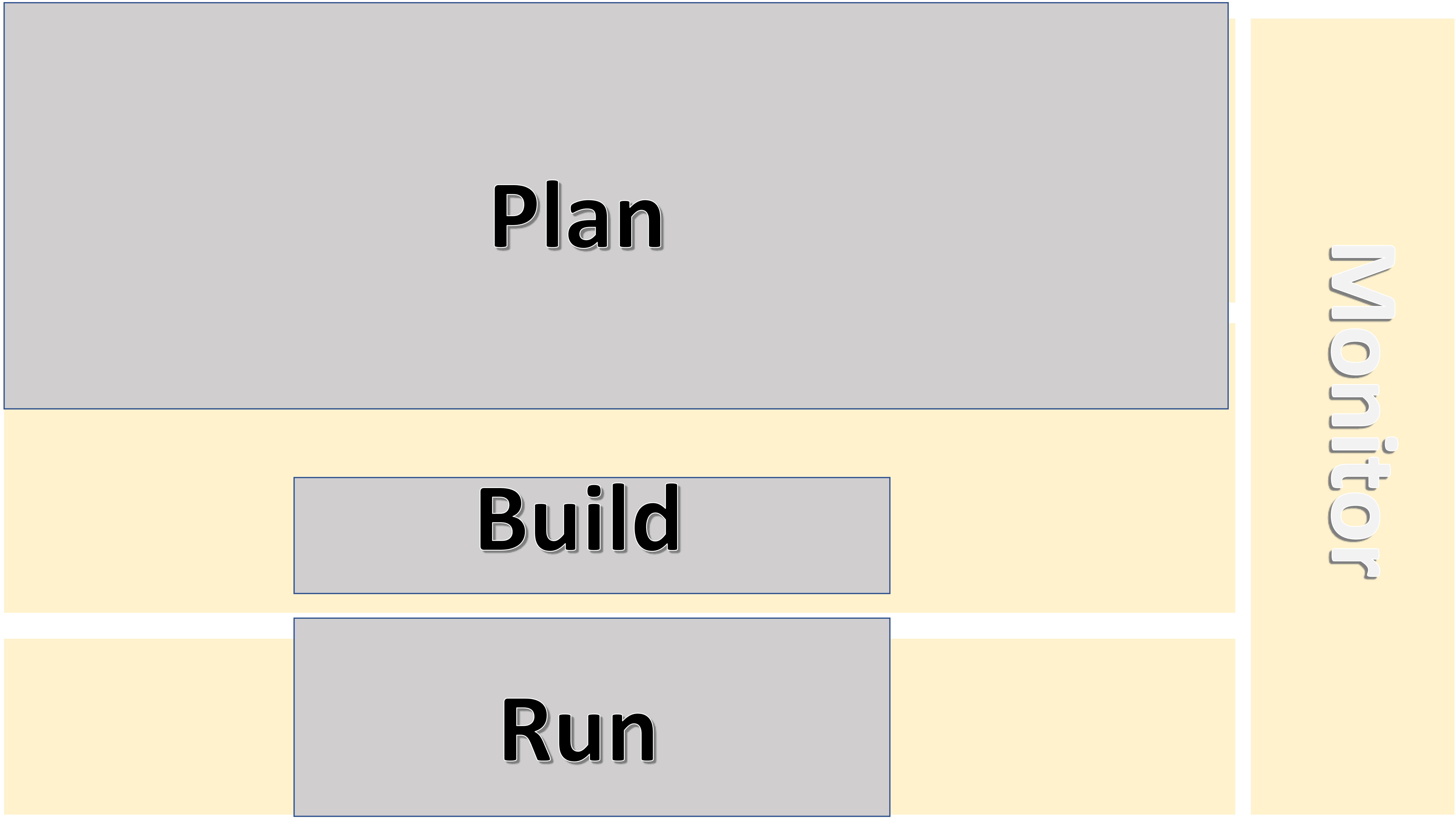
Plan

Build

Run

Monitor

Sample organisation 2



Plan

Build

Run

Monitor

CyBOK

EXECUTIVE MASTER IN CYBERSECURITY MANAGEMENT

DEVELOP YOUR CAREER AS A CYBERSECURITY LEADER - GET THE PRACTICES, SKILLS AND KNOWLEDGE.

Solvay Lifelong Learning

ULB

ISO 31000 Risk-Management

ISACA COBIT 2019

ISO 27005

CRISC Certified in Risk and Information Systems Control™ An ISACA® Certification

CISA Certified Information Systems Auditor® An ISACA® Certification

C|CISO™ CERTIFIED CHIEF INFORMATION SECURITY OFFICER

ISO 38500

ISO/IEC 27035 INCIDENT MANAGER

CSX CYBERSECURITY NEXUS

CISSP® Certified Information Systems Security Professional

CISM Certified Information Security Manager® An ISACA® Certification

TOGAF®

CompTIA Security+

ISO 27032

ISO 27001 Certified Lead Implementer

ITIL® 4 FOUNDATION

ISO 22301

NIST CYBER SECURITY FRAMEWORK

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

ISO 31000 Risk-Management

CRISC Certified in Risk and Information Systems Control™ An ISACA® Certification

ISO 22301

CSX CYBERSECURITY NEXUS

TOGAF®

CISA Certified Information Systems Auditor® An ISACA® Certification

C|CISO™ CERTIFIED CHIEF INFORMATION SECURITY OFFICER

CISSP® Certified Information Systems Security Professional

CompTIA Security+

ISO 38500

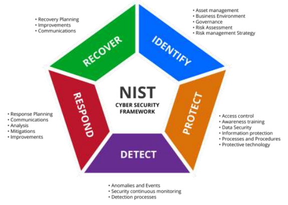
ISO/IEC 27035 INCIDENT MANAGER

CISM® Certified Information Security Manager® An ISACA® Certification

ISO 27032

CyBOK

ISO 27005



enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

ECSF

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

SEPTEMBER 2022

ISO 27001 Certified Lead Implementer

ISACA COBIT 2019

ITIL®4 FOUNDATION

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

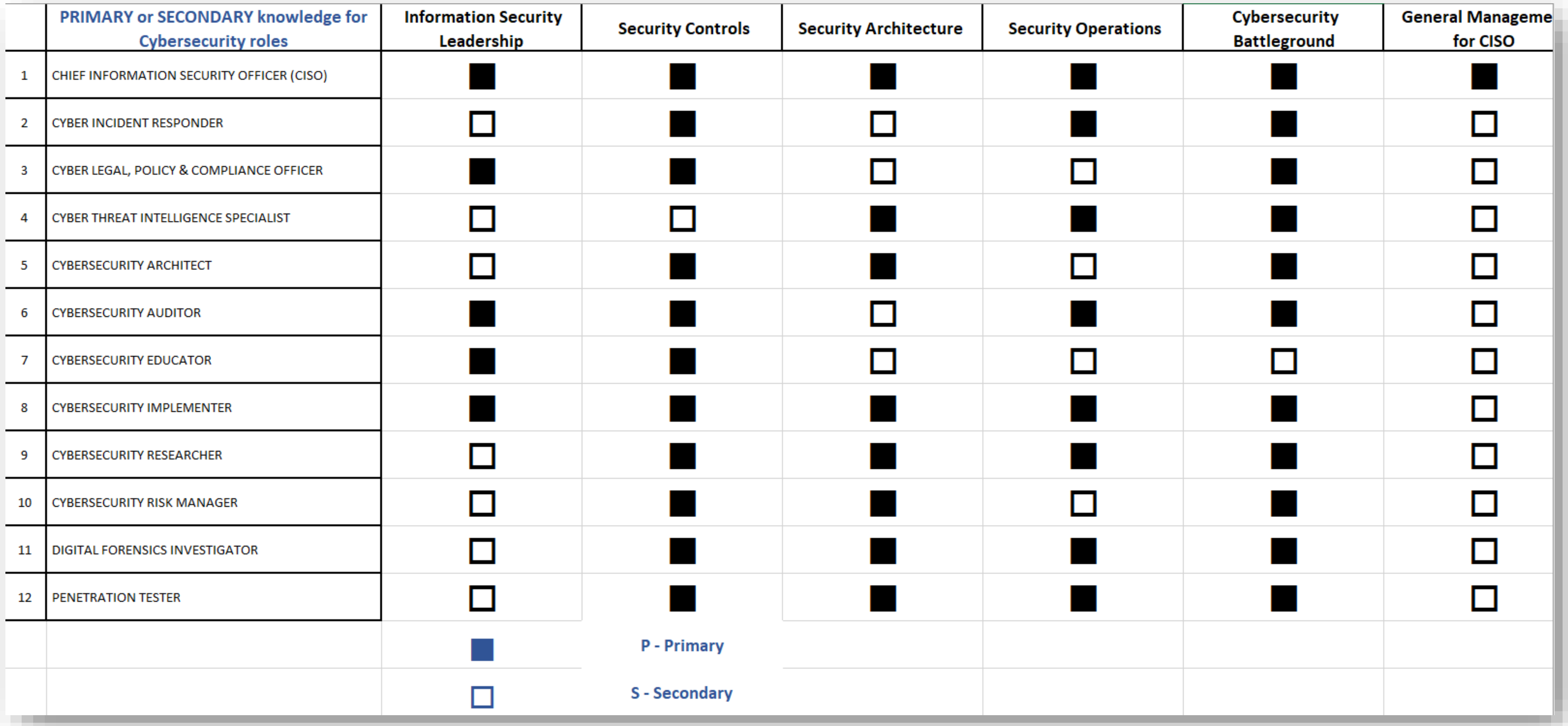
EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

ECSF

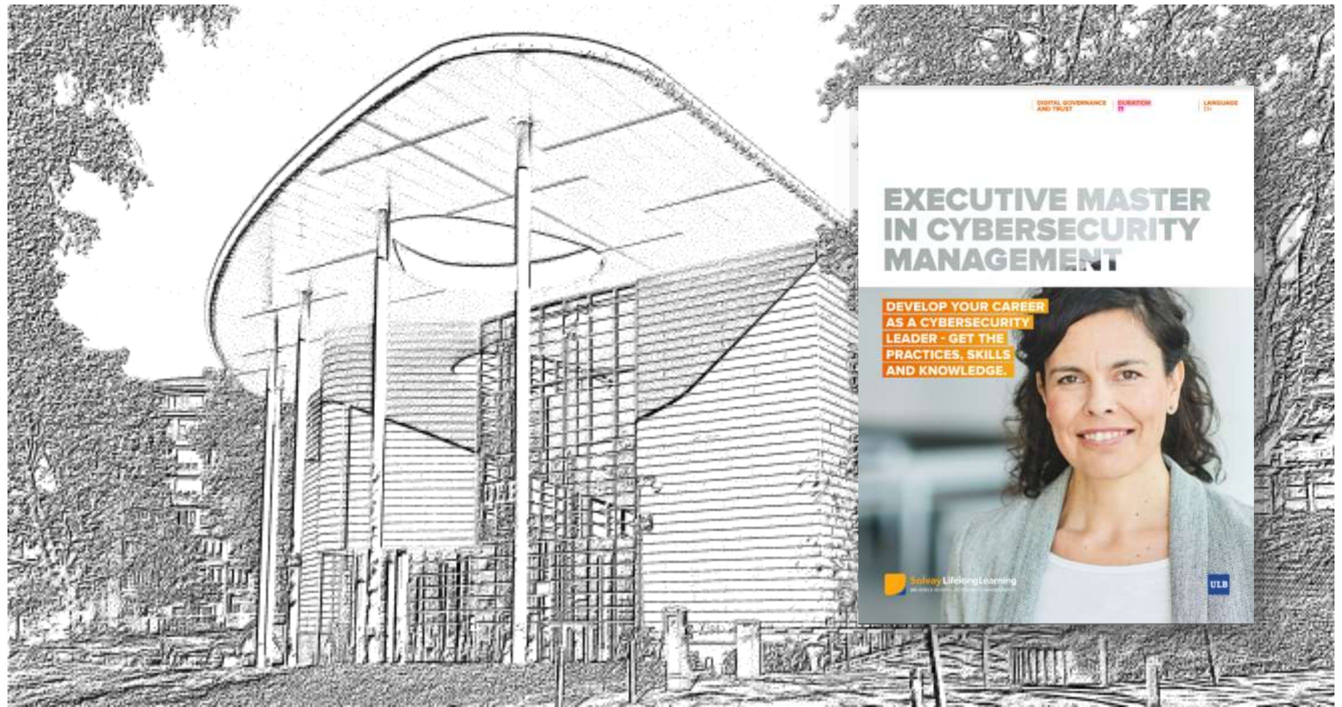
EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

SEPTEMBER 2022

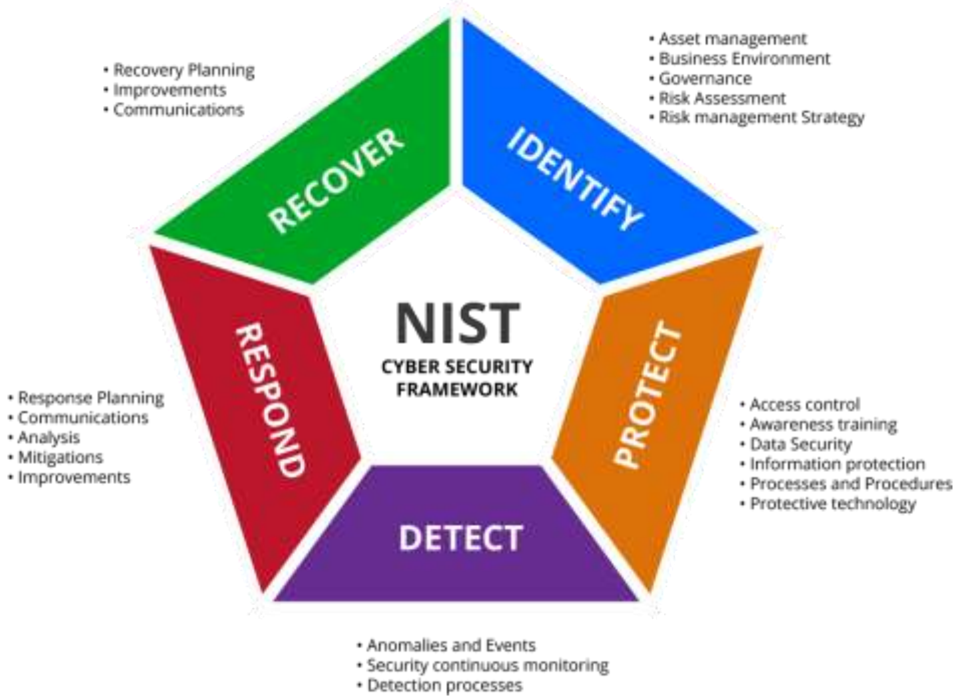
Alignment mapping



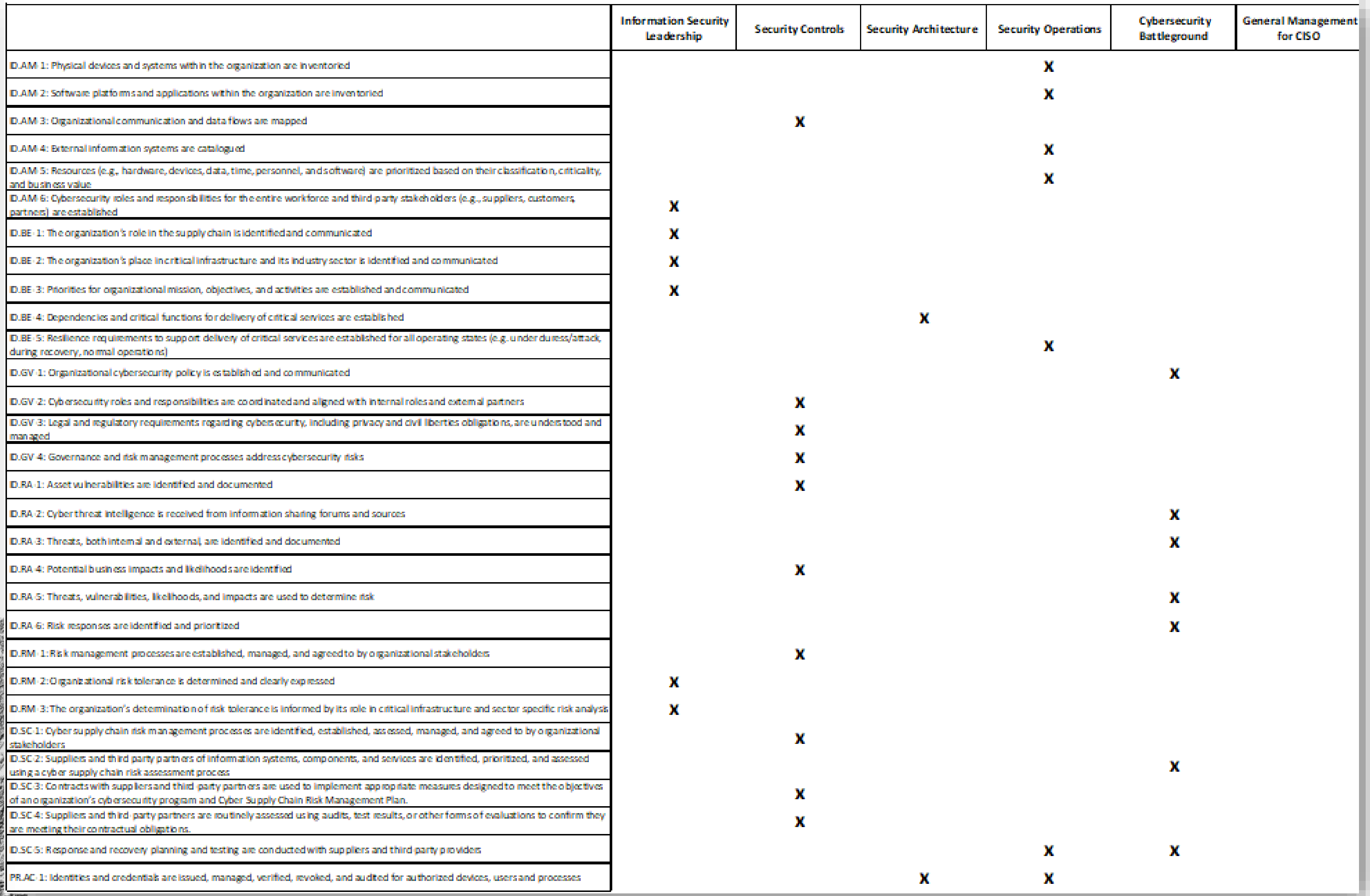
	PRIMARY or SECONDARY knowledge for Cybersecurity roles	Information Security Leadership	Security Controls	Security Architecture	Security Operations	Cybersecurity Battleground	General Manageme for CISO
1	CHIEF INFORMATION SECURITY OFFICER (CISO)	■	■	■	■	■	■
2	CYBER INCIDENT RESPONDER	□	■	□	■	■	□
3	CYBER 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				



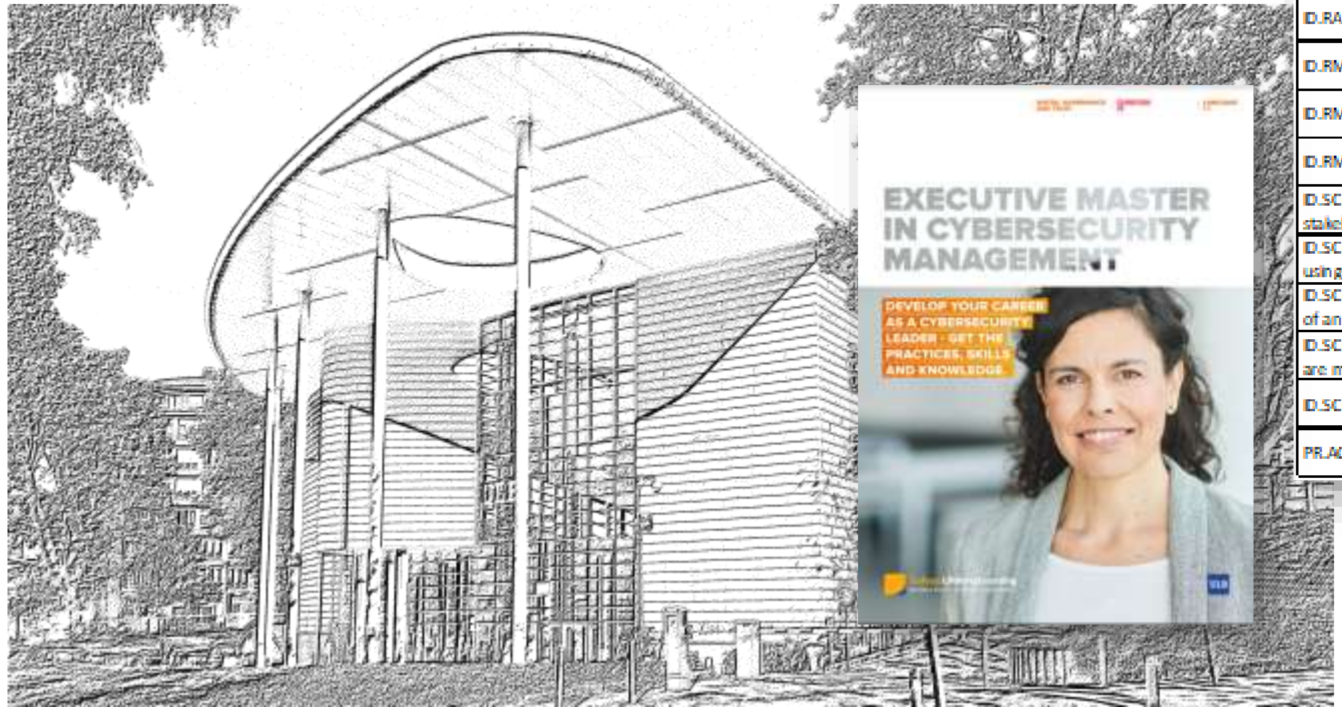
EXECUTIVE MASTER IN CYBERSECURITY MANAGEMENT
DEVELOP YOUR CAREER AS A CYBERSECURITY LEADER · GET THE PRACTICES, SKILLS AND KNOWLEDGE.



Alignment mapping



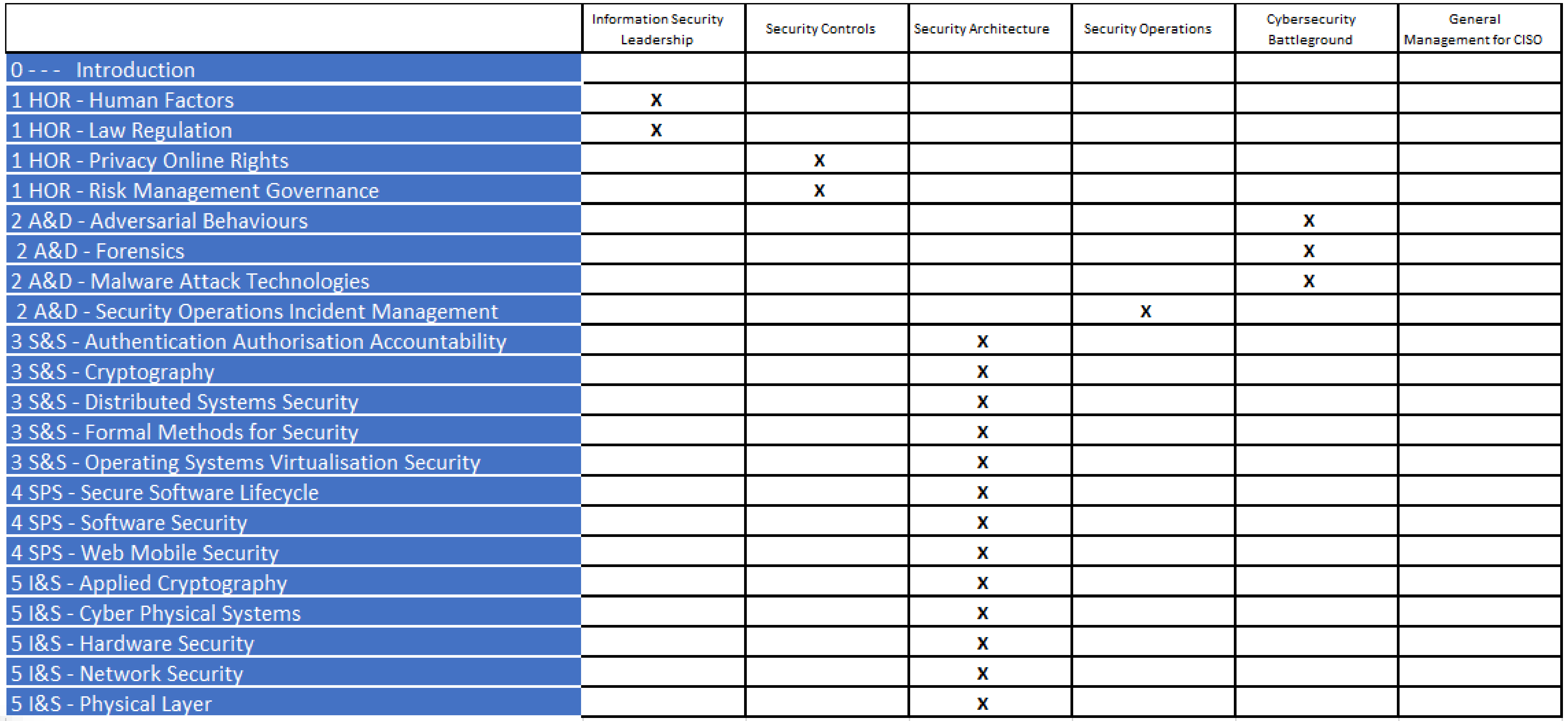
	Information Security Leadership	Security Controls	Security Architecture	Security Operations	Cybersecurity Battleground	General Management for CISO
ID.AM-1: Physical devices and systems within the organization are inventoried				X		
ID.AM-2: Software platforms and applications within the organization 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		


EXECUTIVE MASTER IN CYBERSECURITY MANAGEMENT
DEVELOP YOUR CAREER AS A CYBERSECURITY LEADER · GET THE PRACTICES, SKILLS AND KNOWLEDGE.

5 Functions   23 Categories   108 Subcategories

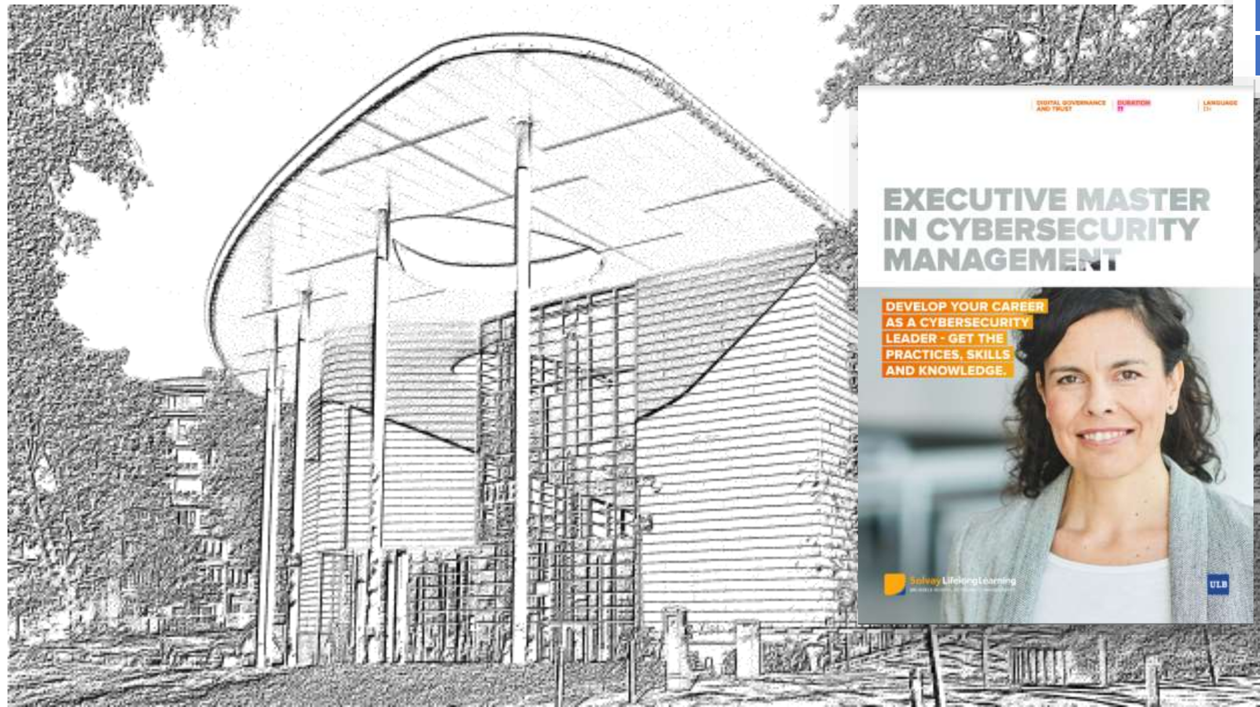
CyBOK

Alignment mapping

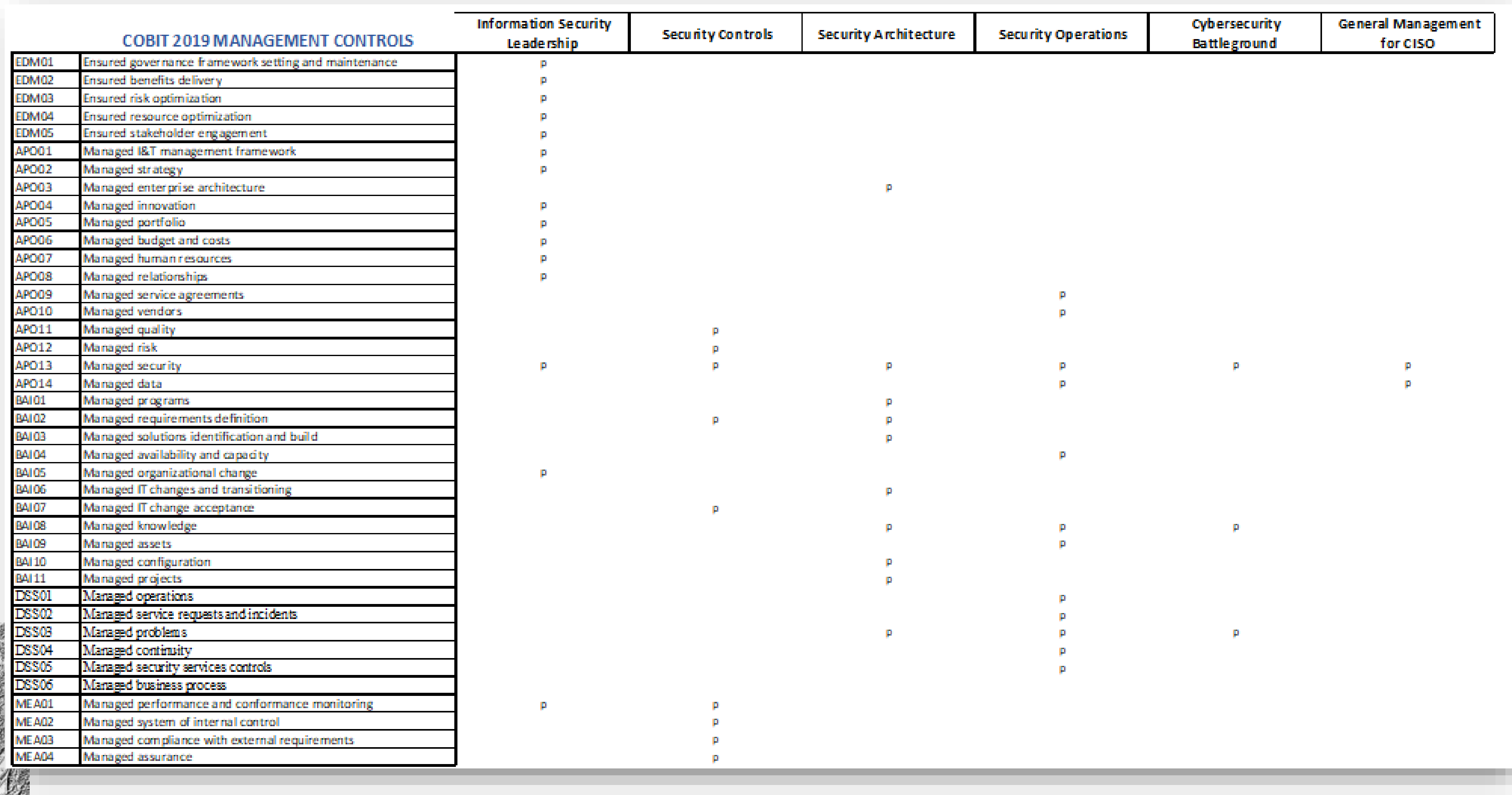


	Information Security Leadership	Security Controls	Security Architecture	Security Operations	Cybersecurity Battleground	General Management for CISO
0 - - - Introduction						
1 HOR - Human Factors	x					
1 HOR - Law Regulation	x					
1 HOR - Privacy Online Rights		x				
1 HOR - Risk Management Governance		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

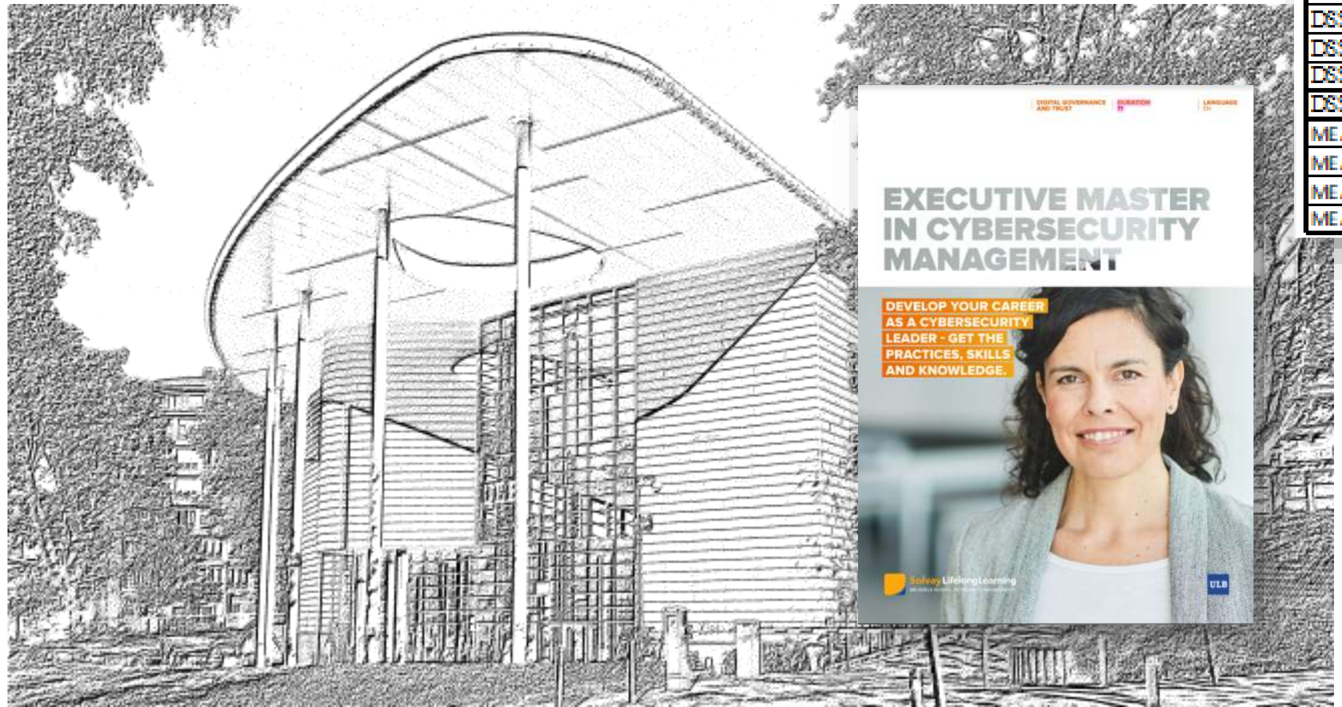

EXECUTIVE MASTER IN CYBERSECURITY MANAGEMENT
DEVELOP YOUR CAREER AS A CYBERSECURITY LEADER - GET THE PRACTICES, SKILLS AND KNOWLEDGE.
Solvay Lifelong Learning
ULB

Alignment mapping



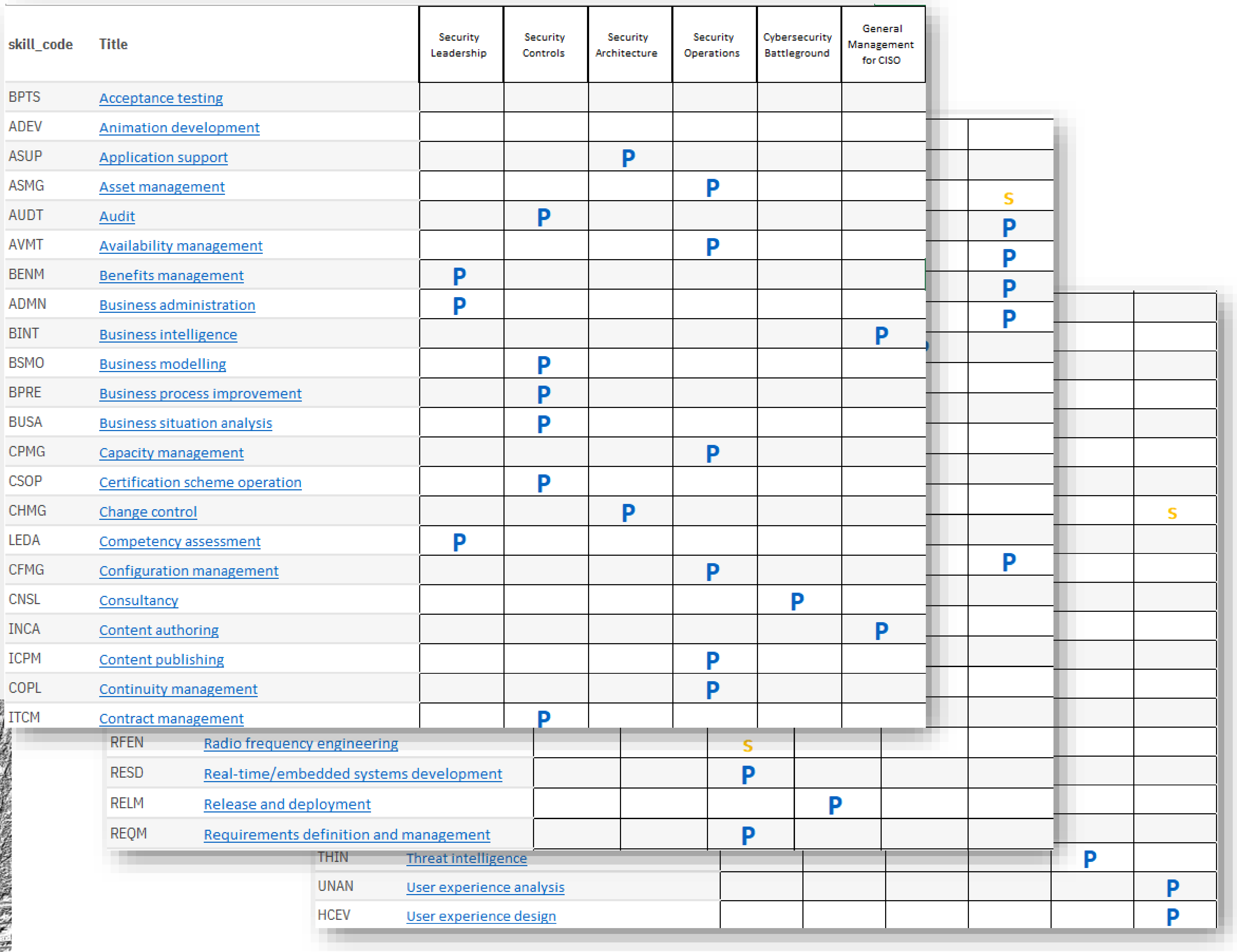
	COBIT 2019 MANAGEMENT CONTROLS	Information Security Leadership	Security Controls	Security Architecture	Security Operations	Cybersecurity Battleground	General Management for CISO
EDM01	Ensured governance framework setting and maintenance	p					
EDM02	Ensured benefits delivery	p					
EDM03	Ensured risk 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						
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


EXECUTIVE MASTER IN CYBERSECURITY MANAGEMENT
DEVELOP YOUR CAREER AS A CYBERSECURITY LEADER · GET THE PRACTICES, SKILLS AND KNOWLEDGE.
Solvay Lifelong Learning
ULB

SFIA® FOUNDATION

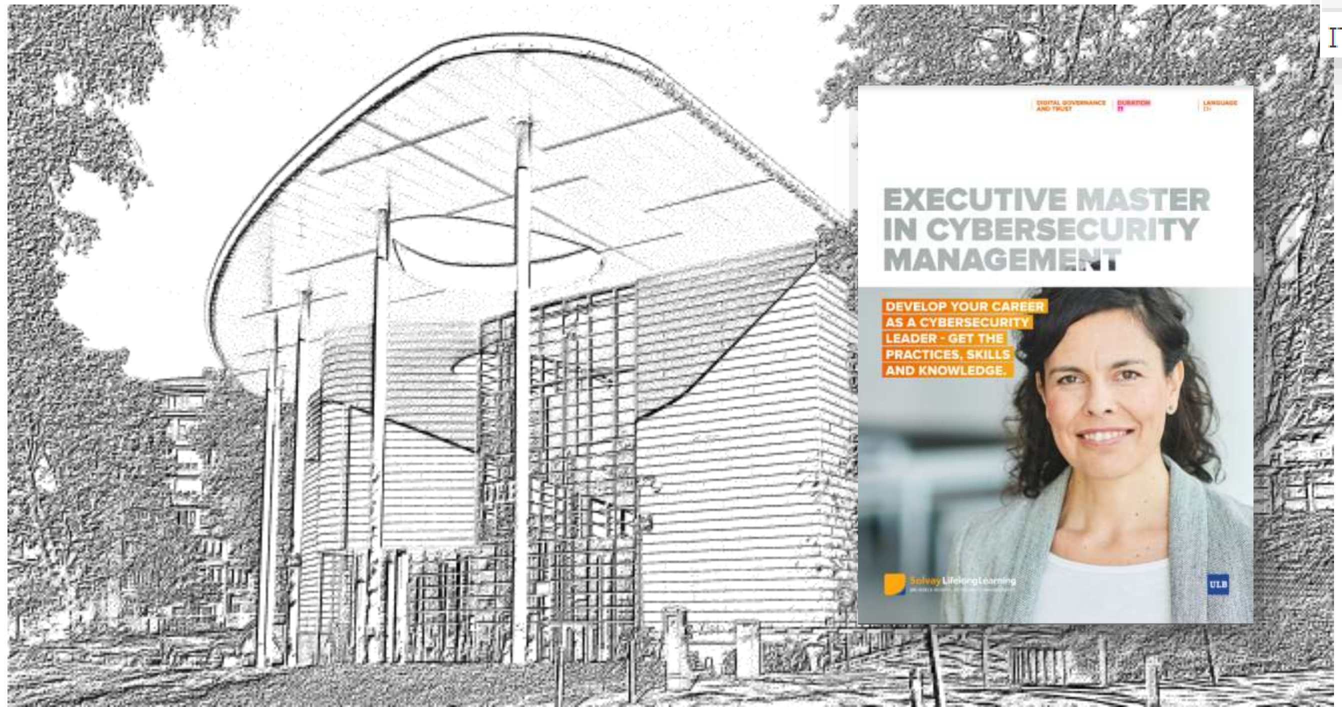
Alignment mapping



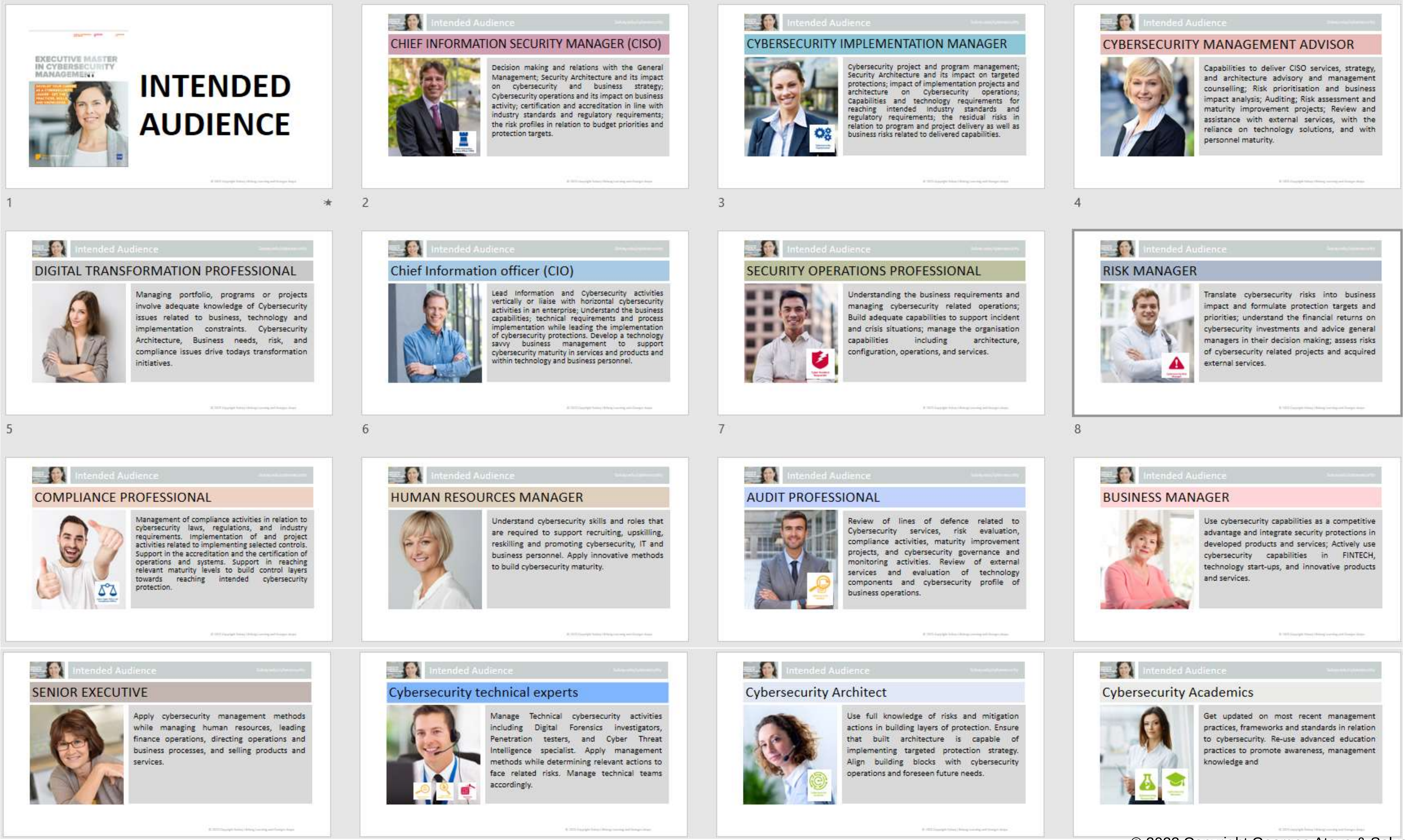
skill_code	Title	Security Leadership	Security Controls	Security Architecture	Security Operations	Cybersecurity Battleground	General Management for CISO
BPTS	Acceptance testing						
ADEV	Animation development						
ASUP	Application support			P			
ASMG	Asset management				P		
AUDT	Audit		P				
AVMT	Availability management				P		
BENM	Benefits management	P					
ADMN	Business administration	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			
LEDA	Competency assessment	P					
CFMG	Configuration management				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


EXECUTIVE MASTER IN CYBERSECURITY MANAGEMENT
DEVELOP YOUR CAREER AS A CYBERSECURITY LEADER · GET THE PRACTICES, SKILLS AND KNOWLEDGE.

120 total skills



EXECUTIVE MASTER IN CYBERSECURITY MANAGEMENT

INTENDED AUDIENCE

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.

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.

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.

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 todays transformation initiatives.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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

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

Cyber Incident Responder

Chief Information Security Officer (CISO)

Cybersecurity Educator

Cybersecurity Auditor

Cybersecurity Implementer

Cybersecurity Architect

Cyber Legal, Policy and Compliance Officer

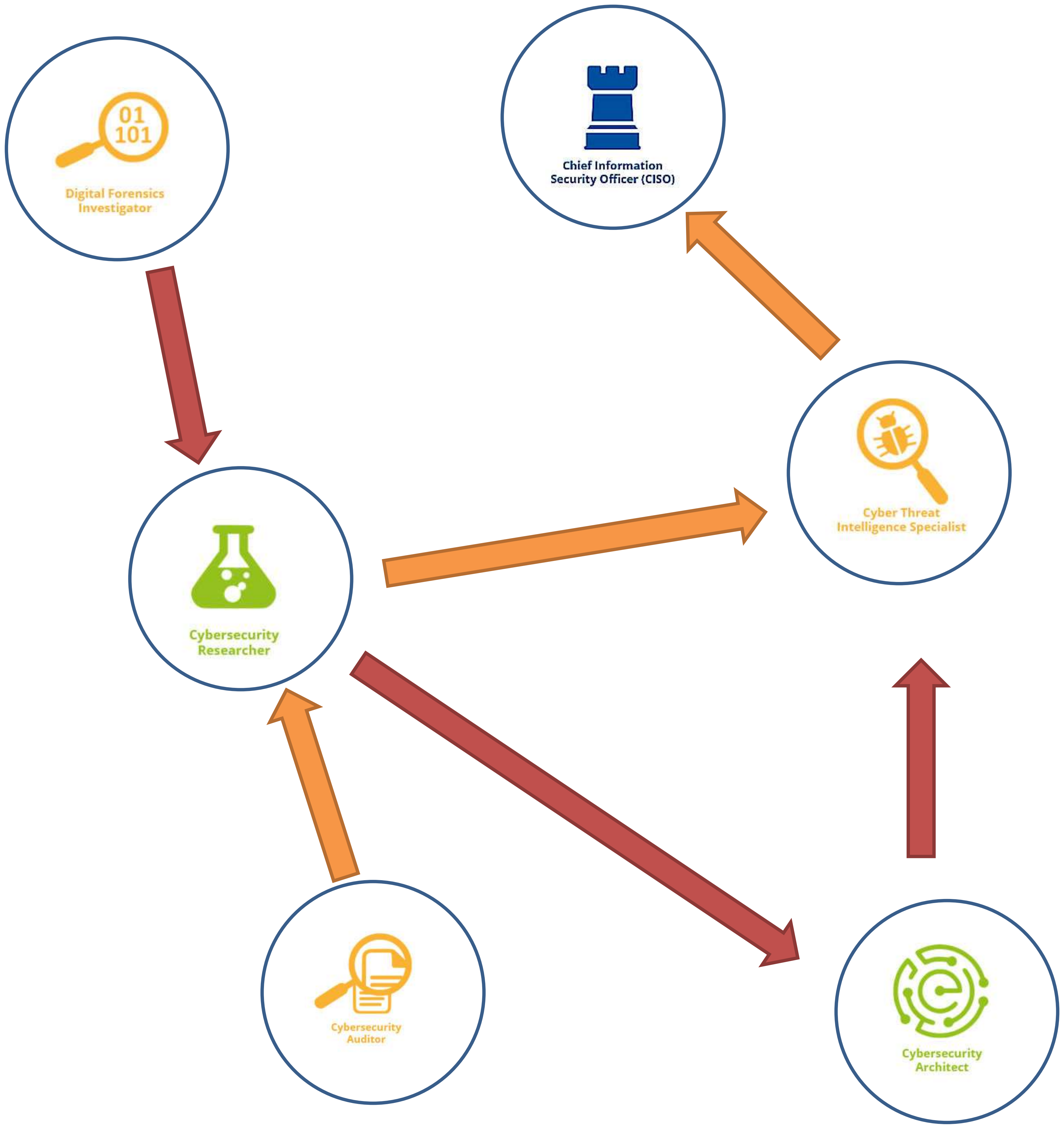
Cyber Threat Intelligence Specialist

Penetration Tester

Cybersecurity Researcher

Cybersecurity Risk Manager

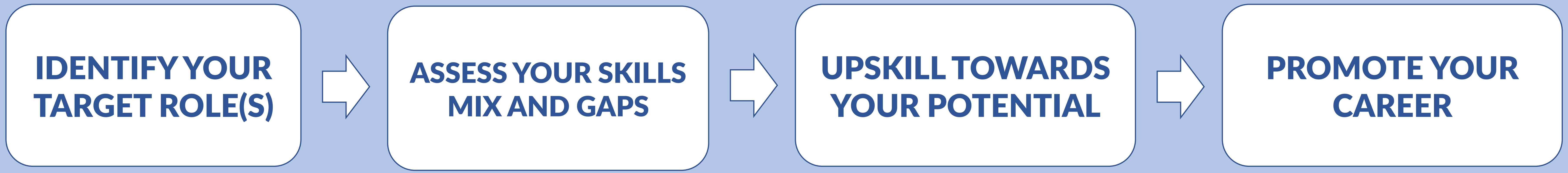
Digital Forensics Investigator


Digital Forensics Investigator
Chief Information Security Officer (CISO)
Cybersecurity Researcher
Cyber Threat Intelligence Specialist
Cybersecurity Auditor
Cybersecurity Architect

Cybersecurity Career Companion

THROUGH

Life-Long learning



IDENTIFY YOUR TARGET ROLE(S)

ASSESS YOUR SKILLS MIX AND GAPS

UPSKILL TOWARDS YOUR POTENTIAL

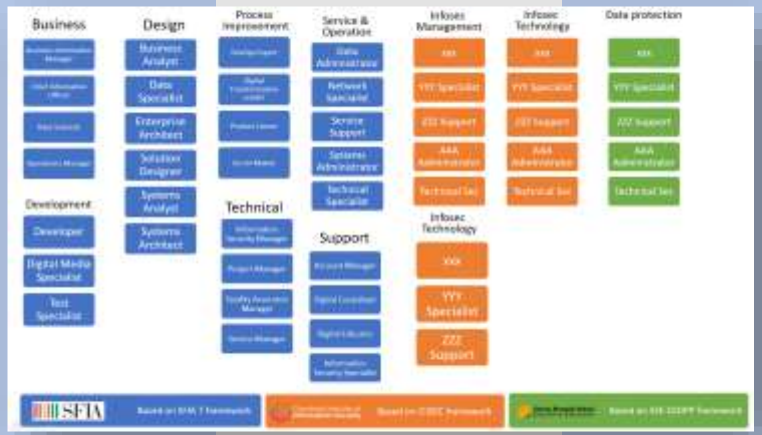
PROMOTE YOUR CAREER

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

Skillsbeam.io

CYBERSECURITY EXECUTIVE EDUCATION

Skillsbeam.io

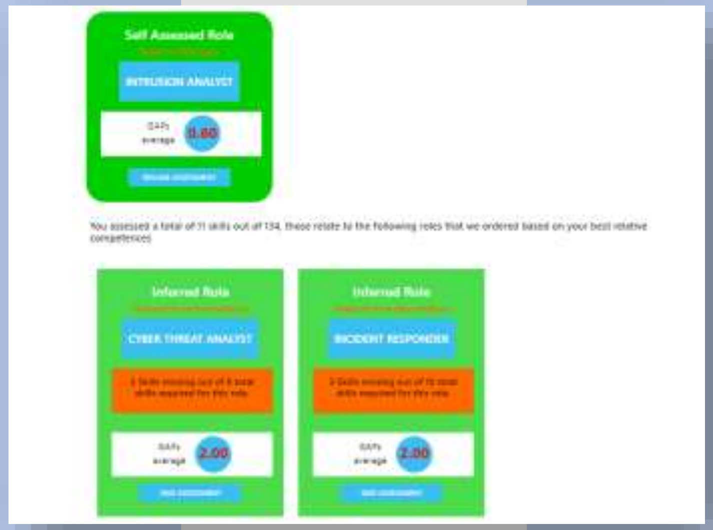


SELECT ROLE TO ASSESS

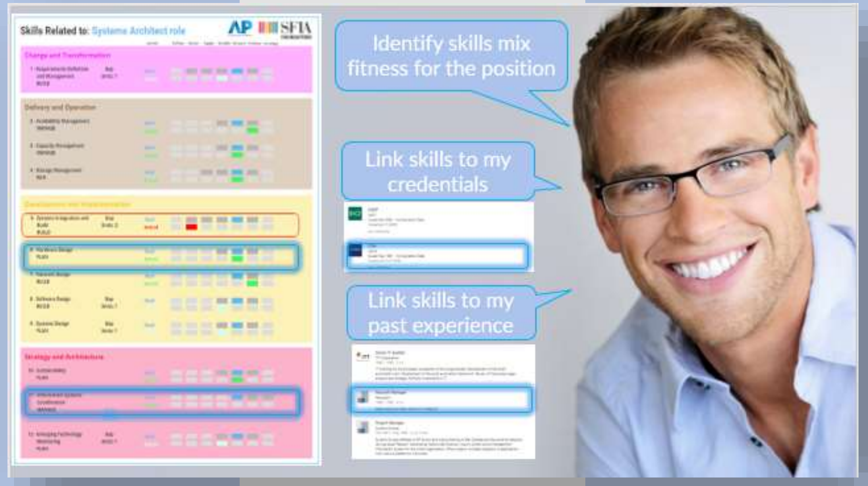
CATEGORY: STRATEGY AND ARCHITECTURE
Skill 1 - Methods and tools
Description

ASSESS ALL SKILLS FOR THAT ROLE

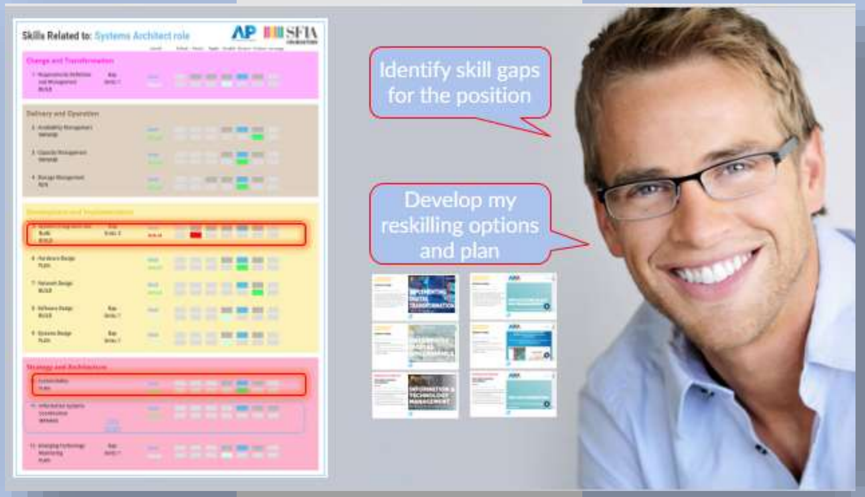
Skills Related to: Cyber Threat Analyst
Skills Related to: Incident Responder



OBTAIN RESULTS AND IDENTIFY OTHER RELEVANT ROLES


Skills Related to: Systems Architect role
Identify skills mix fitness for the position
Link skills to my credentials
Link skills to my past experience

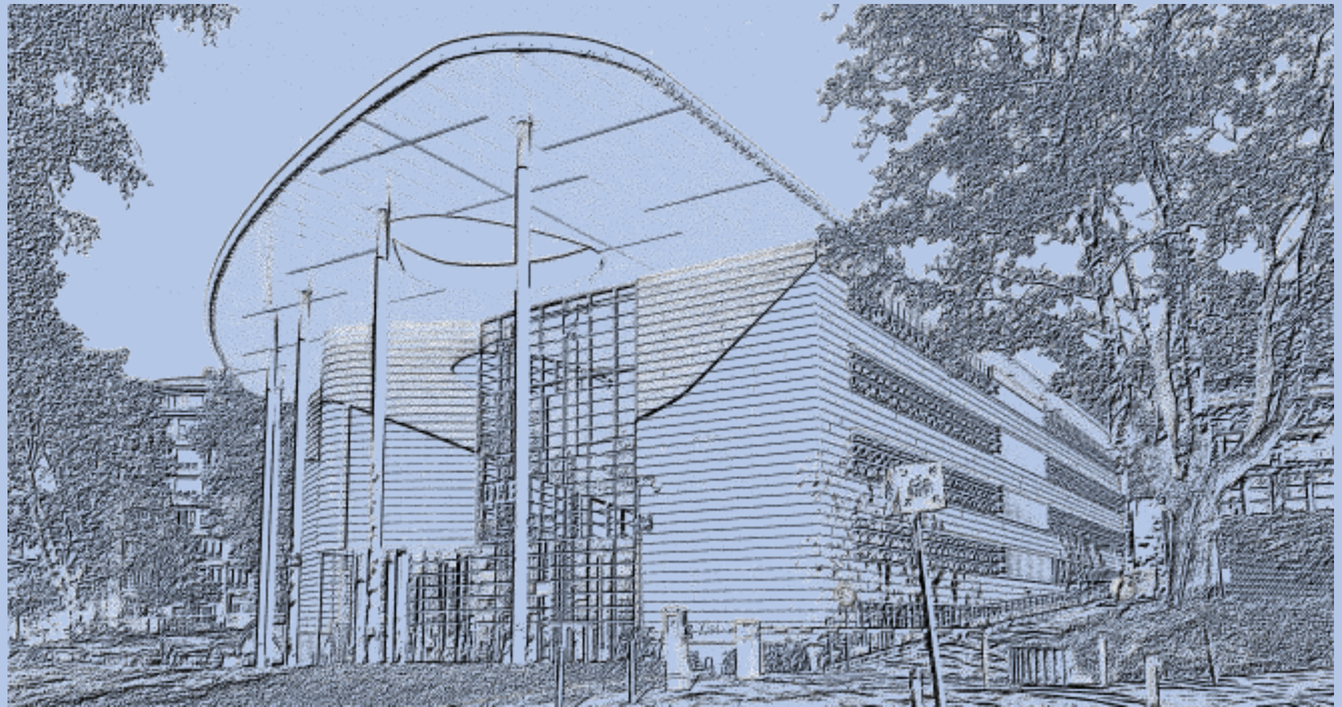
Reference Strong skills


Skills Related to: Systems Architect role
Identify skill gaps for the position
Develop my reskilling options and plan

BUILD UPSKILLING PLAN

OBTAIN THE ROLE QUALIFICATION AND UPSKILLING REPORTS

PERSONAL CURRICULUM



IDENTIFY TARGET ROLES

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

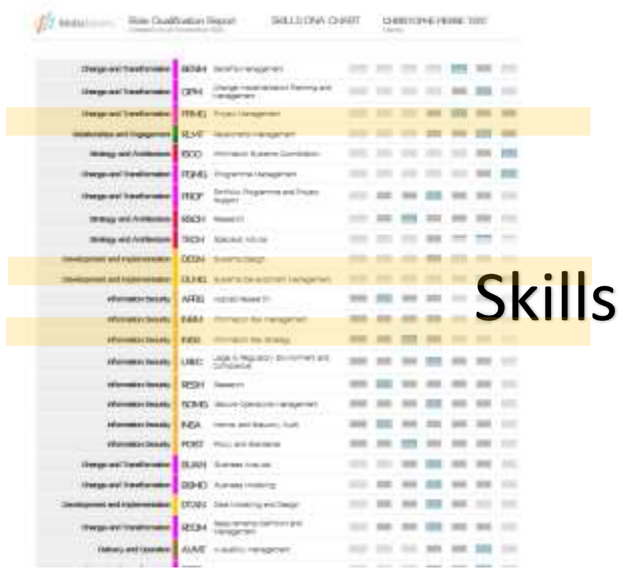
Cybersecurity Implementer

Digital Forensics Investigator

Cyber Incident Responder

ASSESS SKILLS MIX AND GAPS

Skillsbeam.io

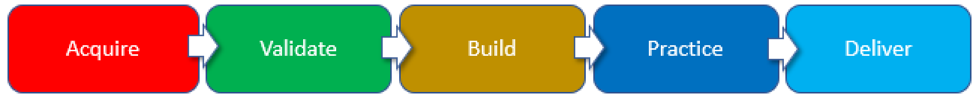


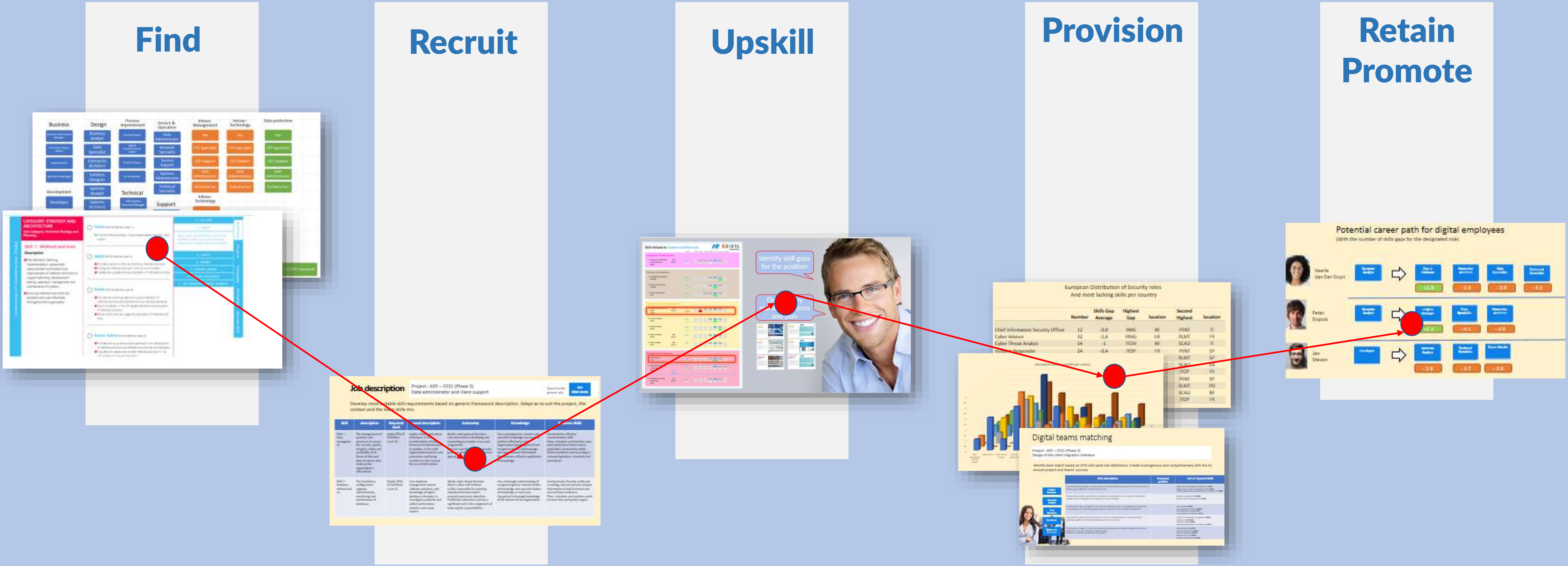
Skills DNA

DEVELOP OWN CURRICULUM

CYBERSECURITY
EXECUTIVE EDUCATION

CISO FUNDAMENTALS	GRC AND CERTIFICATION	SECURITY ARCHITECT
CONTINUITY AND CRISIS MANAGER)	CYBER SECURITY LEADER	GENERAL MANAGEMENT





Find

Recruit

Upskill

Provision

Retain
Promote

Business
Design
Process Improvement
Service & Operation
Infosec Management
Infosec Technology
Data protection
Development
Technical
Support
CATEGORY: STRATEGY AND ARCHITECTURE
Job description
Project : ADF – 2231 (Phase 3)
Data administrator and client support
Develop most suitable skill requirements based on generic framework description. Adapt as to suit the project, the context and the team skills mix.
Skill
description
Required level
Level description
Autonomy
Knowledge
Business Skills
Identify skill gaps for the position
Potential career path for digital employees
(With the number of skills gaps for the designated role)
Veerle Van Der Duyn
Peter Dupuis
Jan Steven
Digital teams matching
Project : ADF – 2231 (Phase 3)

European Distribution of Security roles
And most lacking skills per country

	Number	Skills Gap Average	Highest Gap	location	Second Highest	location
Chief Information Security Officer	12	-0,8	INAS	BE	PENT	IT
Cyber Advisor	32	-1,6	IRMG	UK	RLMT	FR
Cyber Threat Analyst	14	-1	ITCM	BE	SCAD	IT
Incident Responder	24	-0,4	ITOP	FR	PENT	SP
					RLMT	SP
					SCAD	UK
					ITOP	ES
					PENT	SP
					RLMT	PO
					SCAD	BE
					ITOP	FR

Skillsbeam.io

ENTERPRISES

MANAGEMENT MODEL

ATAYA&PARTNERS

Solvay Brussels School
Economics & Management

Georges Ataya

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.

Linkedin: ataya
gataya@solvay.edu
+32475705709

Thank You

Solvay Lifelong Learning
BRUSSELS SCHOOL. ECONOMICS. MANAGEMENT