Cybersecurity and Privacy by Design in Digital Transformation

Christos K. Dimitriadis, PhD, CISA, CISM, CRISC
Group Director of Information Security, INTRALOT
International Chair of the Board 2015-2017, ISACA

intralot

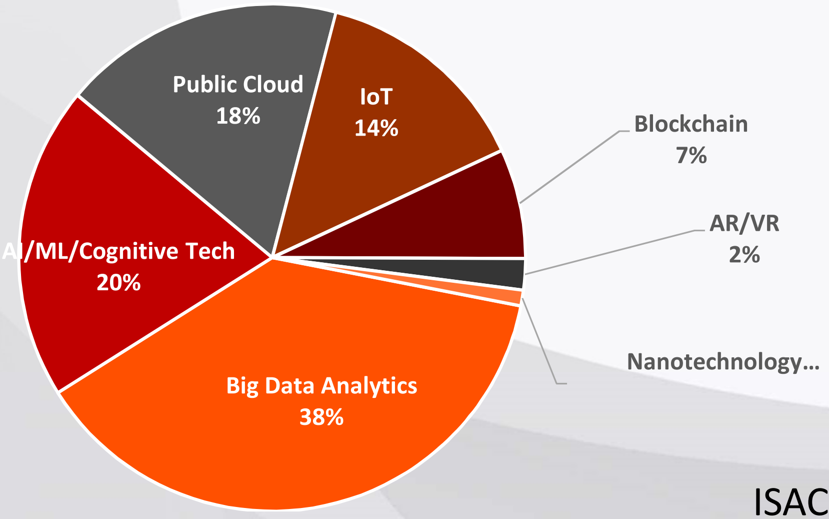
Agenda

- Technology as an enabler of innovation
- Cybersecurity, Privacy and the Cyberthreat landscape
- Responsible Digital Transformation
- Focus Areas

The impact of digital transformation

"A notable outcome of this work is the development of our distinctive economic framework, which quantifies the impact of digitalization on industry and society. It can be applied consistently at all levels of business and government to help unlock the estimated ***$100 trillion of value that digitalization*** *could create over the* ***next decade****."*

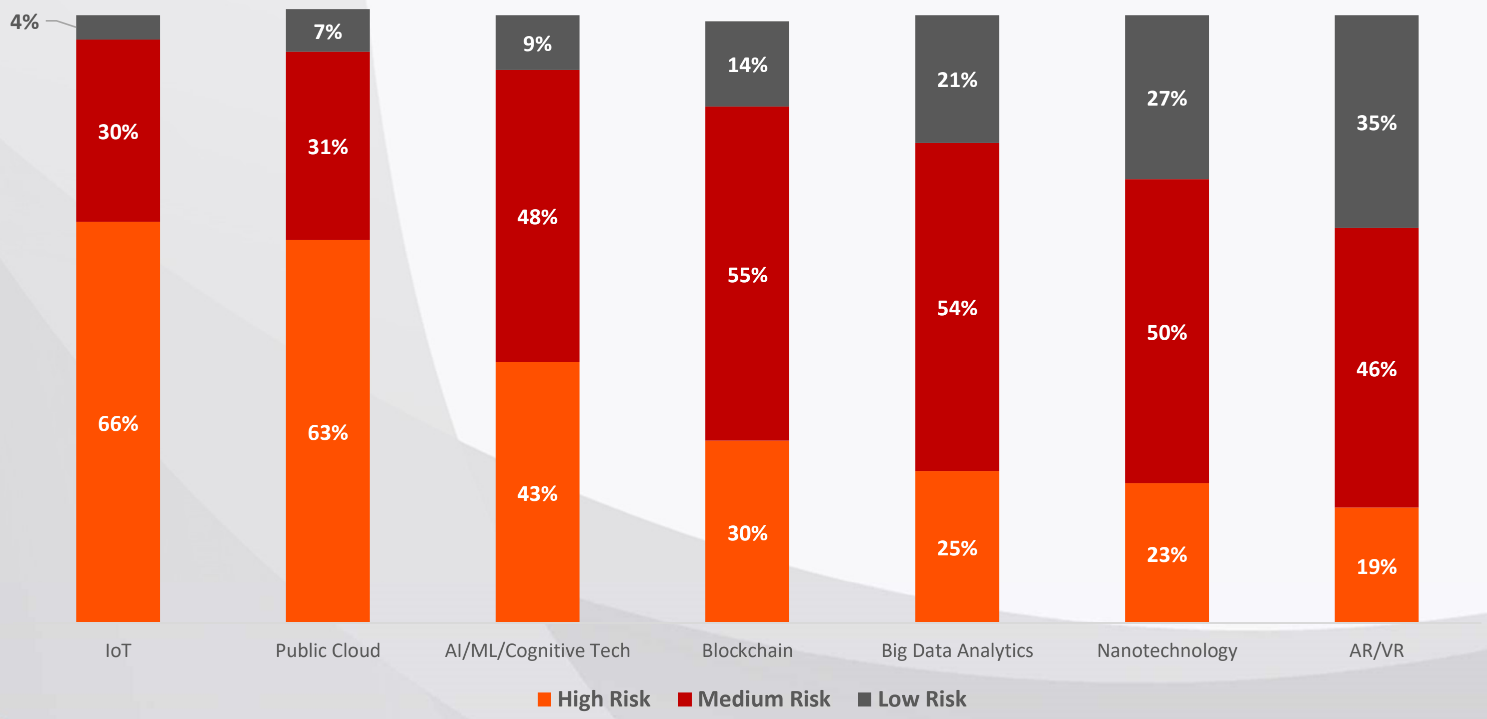
World Economic Forum Digital Transformation Initiative in collaboration with Accenture



ISACA 2017 Digital Transformation Barometer

Risks introduced by new technologies

- ISACA 2017 Digital Transformation Barometer



CYBERTHREATS

~Attack cost: **$3,62**million

2017 Ponemon Cost of Data Breach Study

~DDoS cost: **$2,5**million

Worldwide DDoS Attacks & Cyber Insights Research Report - NEUSTAR

Social Engineering cost **$5**billion since 2014

FBI

Increasingly demanding regulation
(i.e. Privacy Reform / NIS)

Our thirst to consume new
Technologies,
many times,
exceeds our capability
to secure them

Responsible Digital Transformation

BUILDING the FRAMEWORK

CYBER SECURITY

- IDENTIFY
- PROTECT
- DETECT
- RESPOND
- RECOVER

Digital Transformation

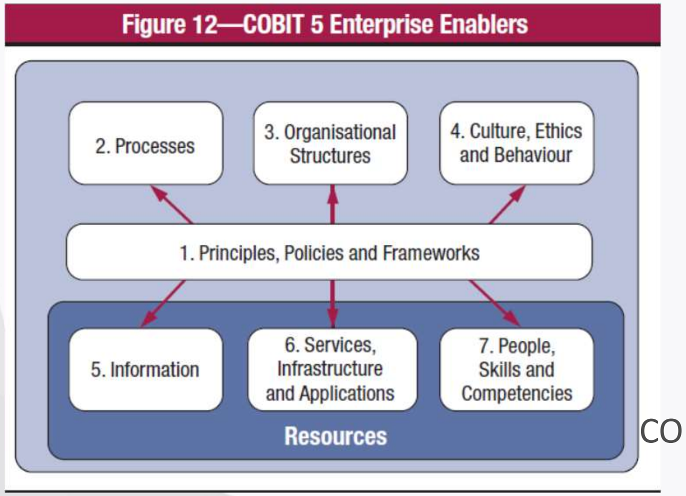


Figure 12—COBIT 5 Enterprise Enablers

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

COBIT 5

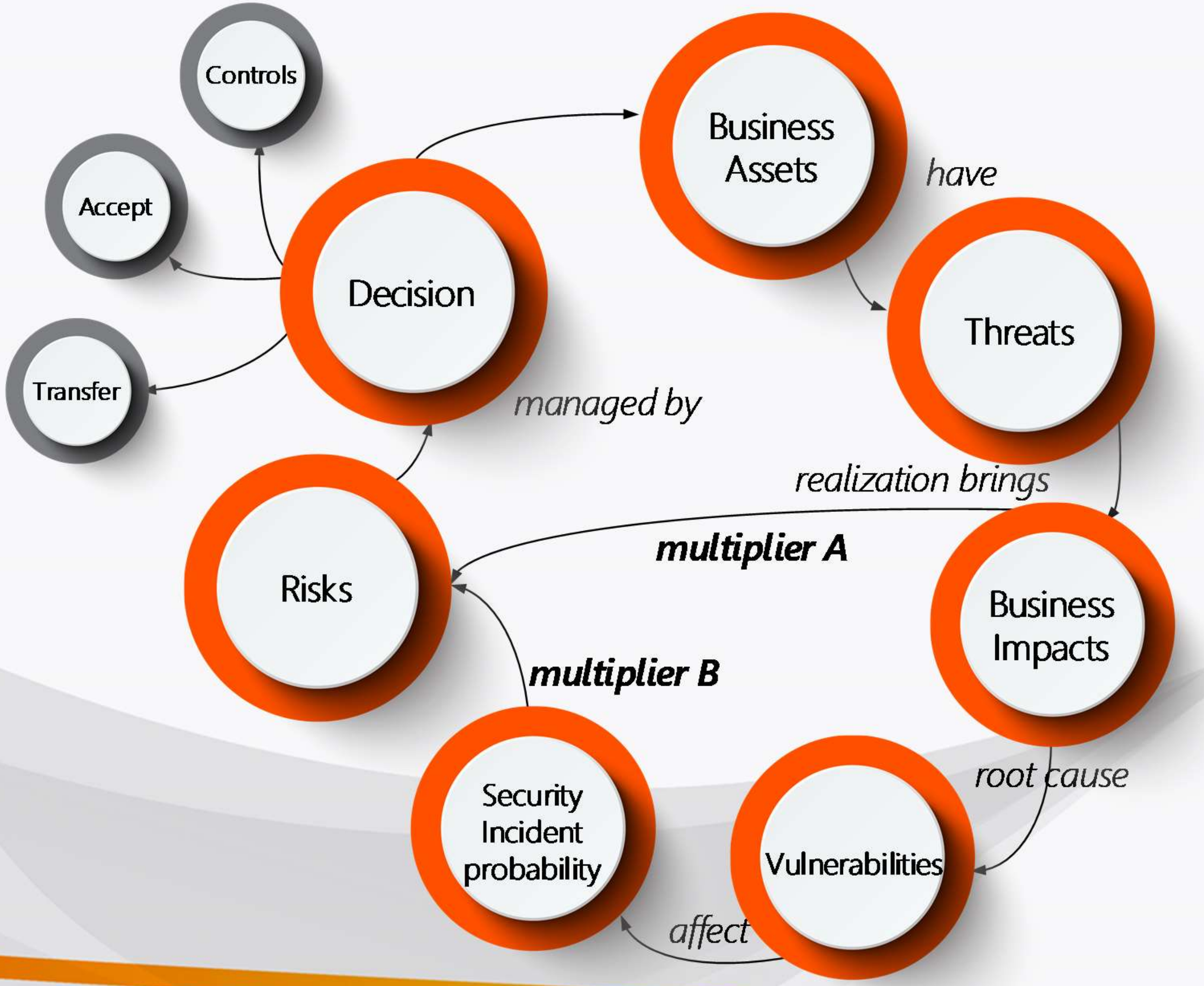
Products and Services

Privacy

- IDENTIFY DATA and Purpose
- PROTECT DATA and Rights
- DETECT Breaches
- RESPOND to Breaches and Objections
- Report and RECOVER

IDENTIFY

- Understand and Map the threat
- Obtain Threat Intelligence



Build a data and processing register

Data Type	Owner	Source and Flow	Form	Purpose / Processing	Consent (if PII)	Place of Storage	Retention	Exports	Impact

Deliverable

- Business Case with incorporated risks and controls
- Make cybersecurity and privacy embedded features
- Communicate the importance of business-aligned risks to the competitiveness of products and services (internal, external)
- Avoid using compliance as the main driver – present the business value of leading a trusted digital transformation that serves the business interests

Protect

- Organization: required changes for implementing security and privacy requirements (e.g. DPO, incorporate security and privacy clauses in contracts)

- People: New skills and competencies required (e.g. managing subcontractors, skills in operating new technologies), employee training and awareness

- Technology: New security and privacy technologies (e.g. threat intelligence extension, DLP, mobile device management, pseudonymization/encryption), high availability and backup requirements implementation

- Process: Incorporation of new controls in processes or new processes (e.g. revisit operations manuals, source code reviews of outsourcers, new audit processes in cybersecurity, new policies and procedures for addressing privacy rights of data subjects)

Detect

- Organization: setup/extend security and privacy monitoring (decide on internal/external, incorporate detection and notification requirements in contracts / SLAs)

- People: New skills and competencies (e.g. cyber skills security and privacy monitoring, analysis of events, configuration of monitoring platforms or managing outsourcers)

- Technology: New security and privacy technologies (e.g. SIEM extensions, alerting on critical data access, fraud detection, behavior analytics)

- Process: Incorporation of new controls in processes or new processes (e.g. revisit the security monitoring process and event analysis methods, managing outsourced security services in detection, testing of detection methods)

Respond

- Organization: required changes for addressing transformation (e.g. revisit BCP roles, incident management roles, create/amend SLAs for incident response)
- People: New skills and competencies required (e.g. cyber expertise in technology-specific incident response)
- Technology: Required tools for attack mitigation (e.g. system-specific ransomware mitigation tools)
- Process: Revisit response processes (e.g. incorporate new response time requirements, retest plans in transformed ecosystem, agree on processes with subcontractors/partners and jointly manage communications), incorporate processes on objections, addressed incident reporting/disclosure requirements

Recover

- Organization: required changes for implementing security and privacy requirements (e.g. revisit BCP roles, revisit cyber insurance contracts, 3rd party contracts and SLAs for recovery times)

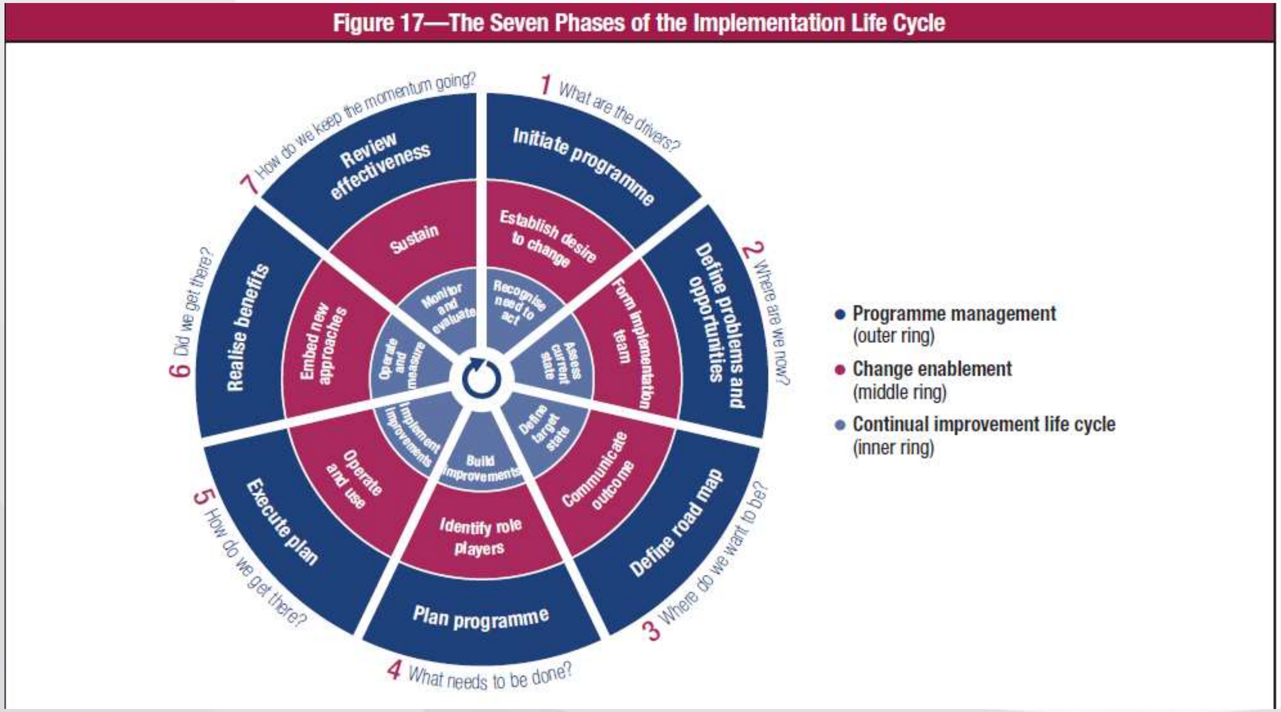
- People: New skills and competencies required (e.g. training of personnel in new/changed recovery processes)

- Process: Incorporation of new controls in processes or new processes (e.g. revisit BCP)

Focus Areas

Design and Implement a Continuous Program

Figure 17—The Seven Phases of the Implementation Life Cycle



COBIT 5

Be Holistic

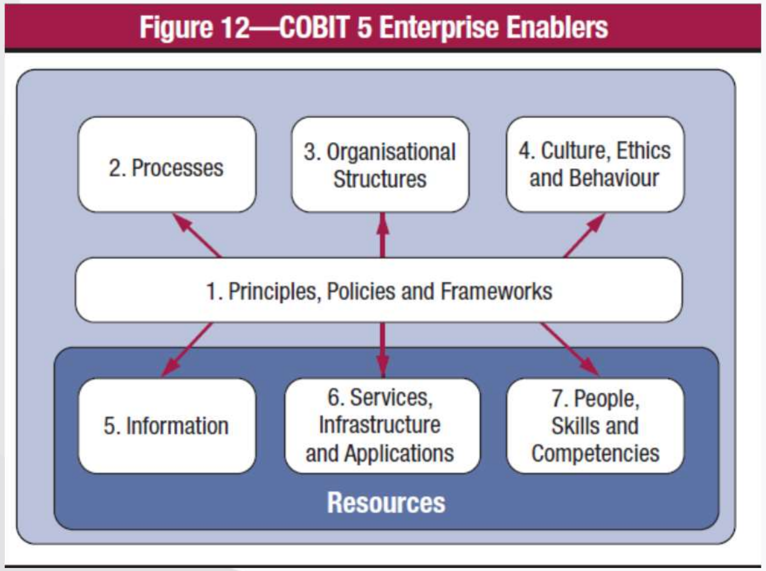
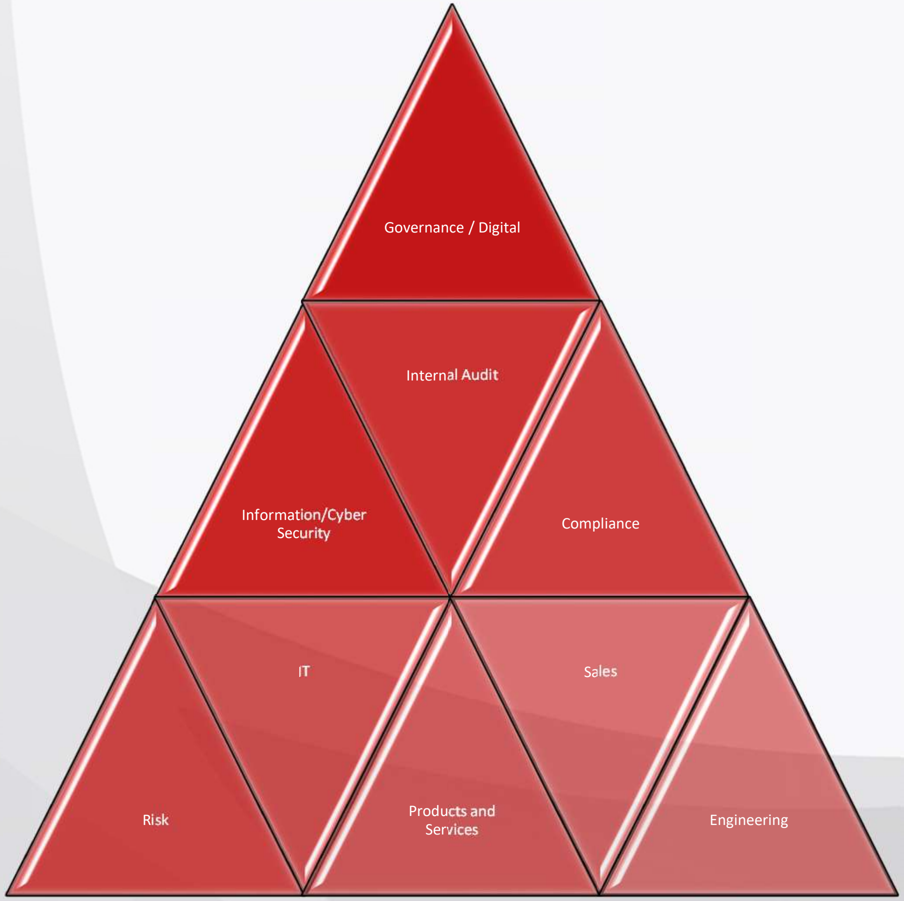


Figure 12—COBIT 5 Enterprise Enablers

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

Break the silos



At the end of the day the target is creating ***value from information****,* ***securely****,* ***safely*** *and* ***responsibly***

THANK YOU!