ISDPTool

INFORMATION SECURITY & DATA PRIVACY MANAGEMENT

Agenda

01 Challenges

Three common challenges in information security and data privacy management.

02 Threat modelling insight

Introduction to threat modelling and how threat modelling integrates into ISDPTool.

03 ISDPTool

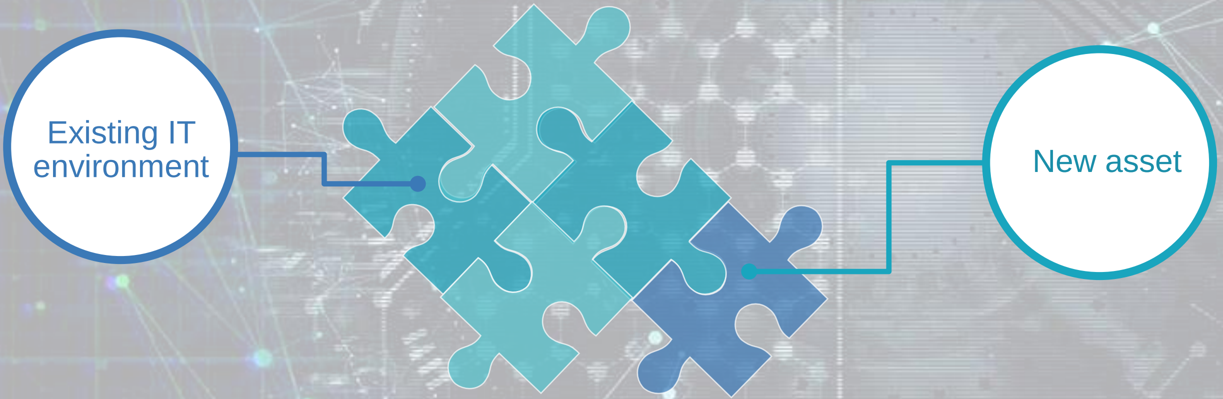
Overview of the ISDPTool features.

01 Challenges

Three common challenges in information security and data privacy management.

Information security & change management

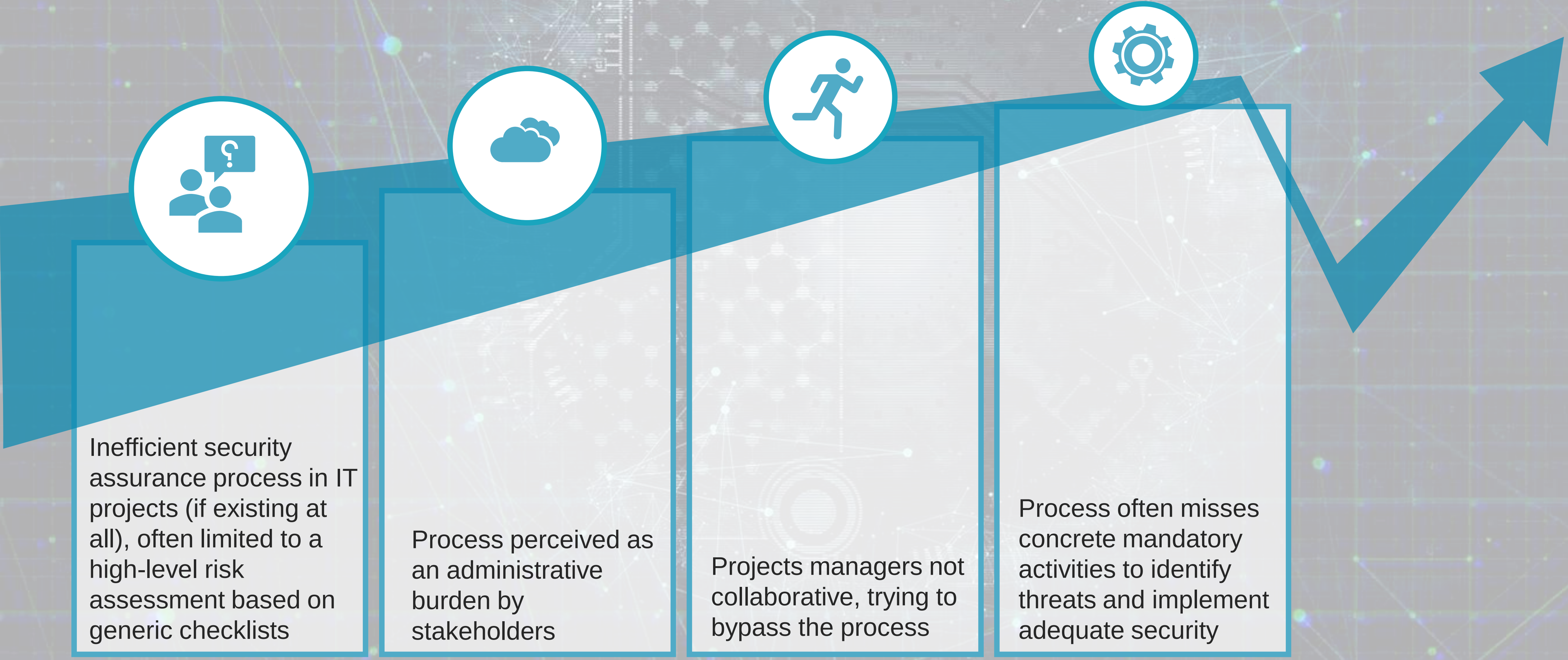
Challenge



> How to ensure that integrating a new asset in our environment does not create security issues ?

Information security & change management

Common pitfalls



Inefficient security assurance process in IT projects (if existing at all), often limited to a high-level risk assessment based on generic checklists

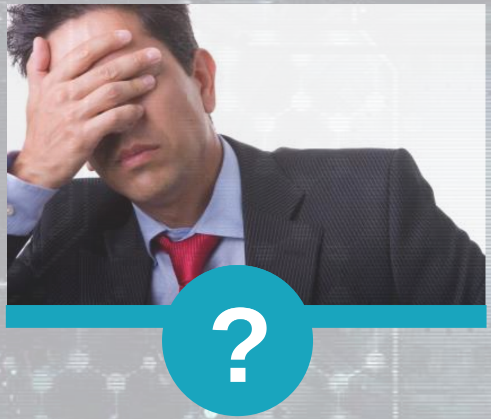
Process perceived as an administrative burden by stakeholders

Projects managers not collaborative, trying to bypass the process

Process often misses concrete mandatory activities to identify threats and implement adequate security

Corporate information risk management

Challenge



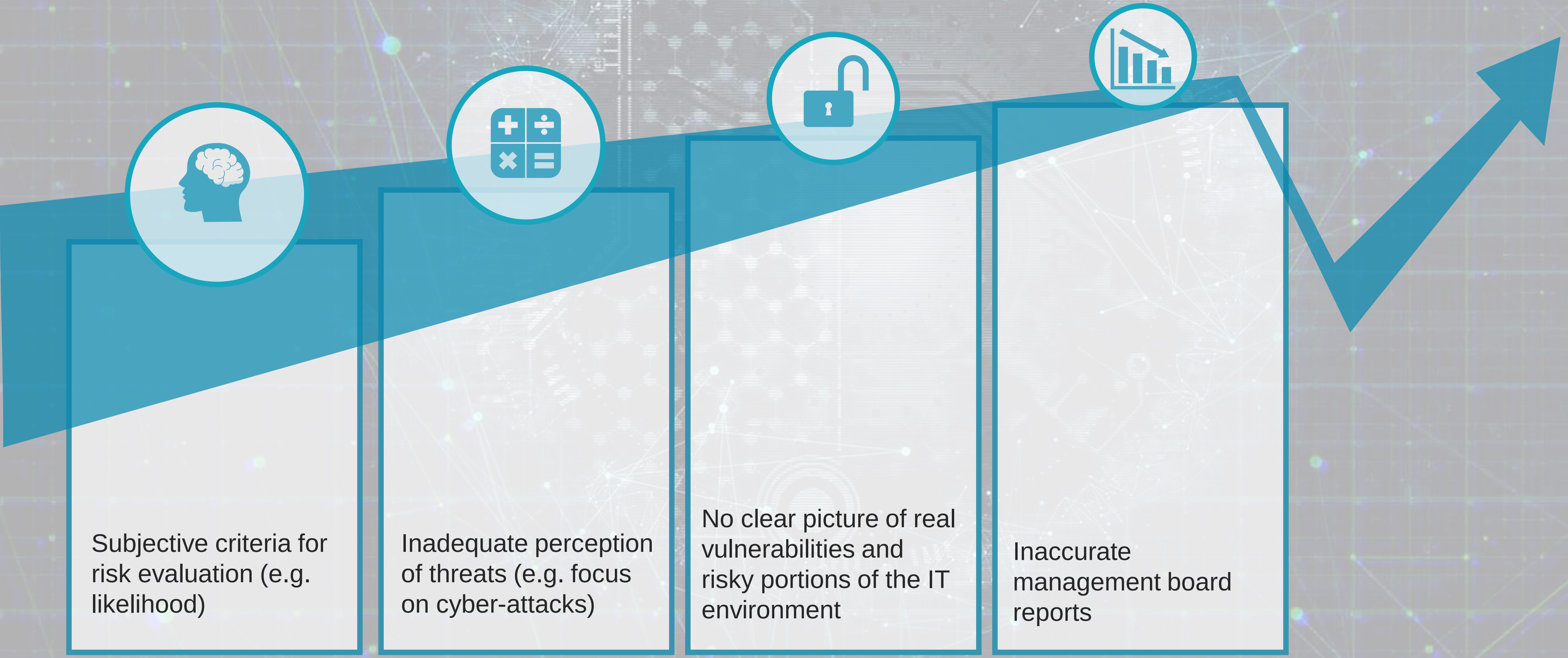
Corporate risk assessment process

Real exposure of systems to threats

> How well is the organization protected against threats?

Corporate information risk management

Common pitfalls



Subjective criteria for risk evaluation (e.g. likelihood)

Inadequate perception of threats (e.g. focus on cyber-attacks)

No clear picture of real vulnerabilities and risky portions of the IT environment

Inaccurate management board reports

Data privacy management

Challenge

Principles

Lawfulness, fairness, transparency, purpose, proportionality of data processing activities, data subjects' rights

Data flows

Personal data inventory, data recipients, data transfers, data processor relationships

GDPR compliancy

Transparency

Personal data inventory, data subjects' information, records of processing activities

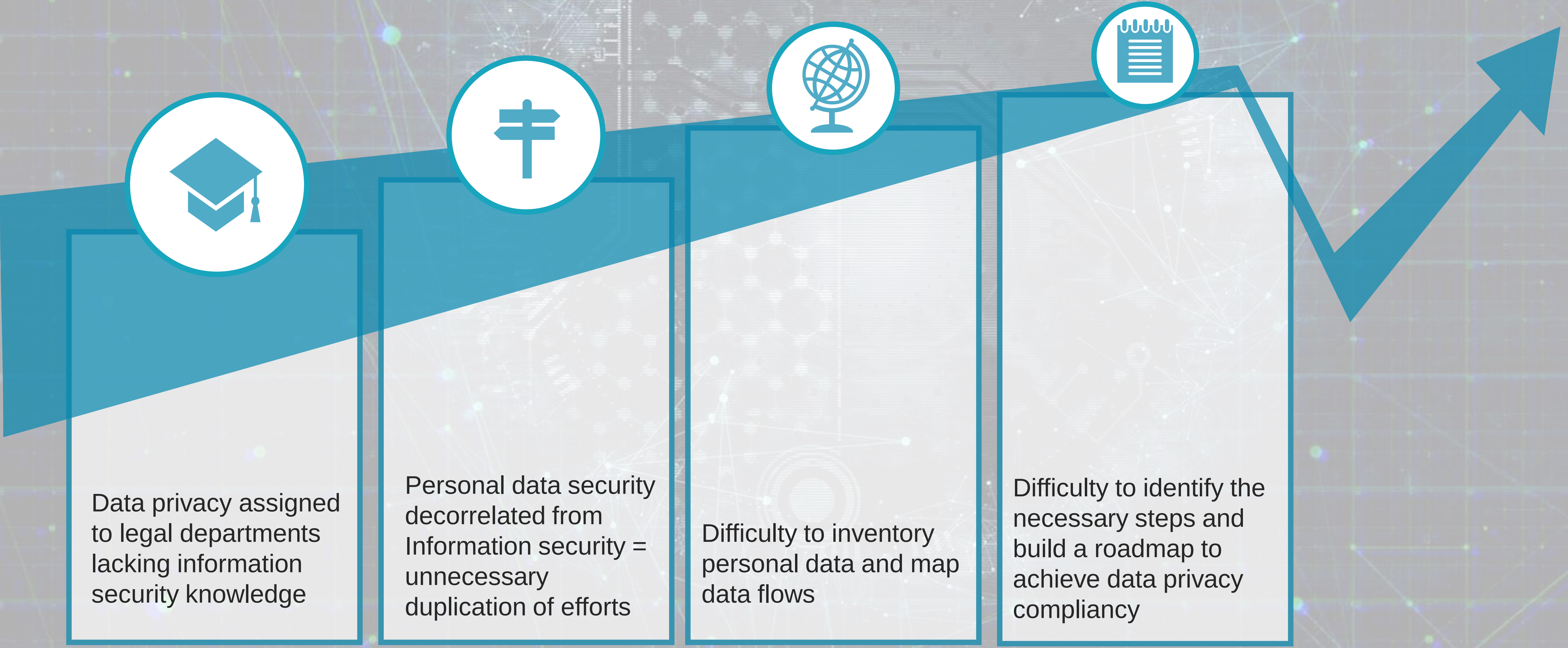
Data security

Data protection Impact assessments, privacy by design and by default, TOM's, data retention periods, data breach management

> “What steps do we need to take to comply with GDPR requirements ?”

Data privacy management

Common pitfalls



Data privacy assigned to legal departments lacking information security knowledge

Personal data security decorrelated from Information security = unnecessary duplication of efforts

Difficulty to inventory personal data and map data flows

Difficulty to identify the necessary steps and build a roadmap to achieve data privacy compliancy

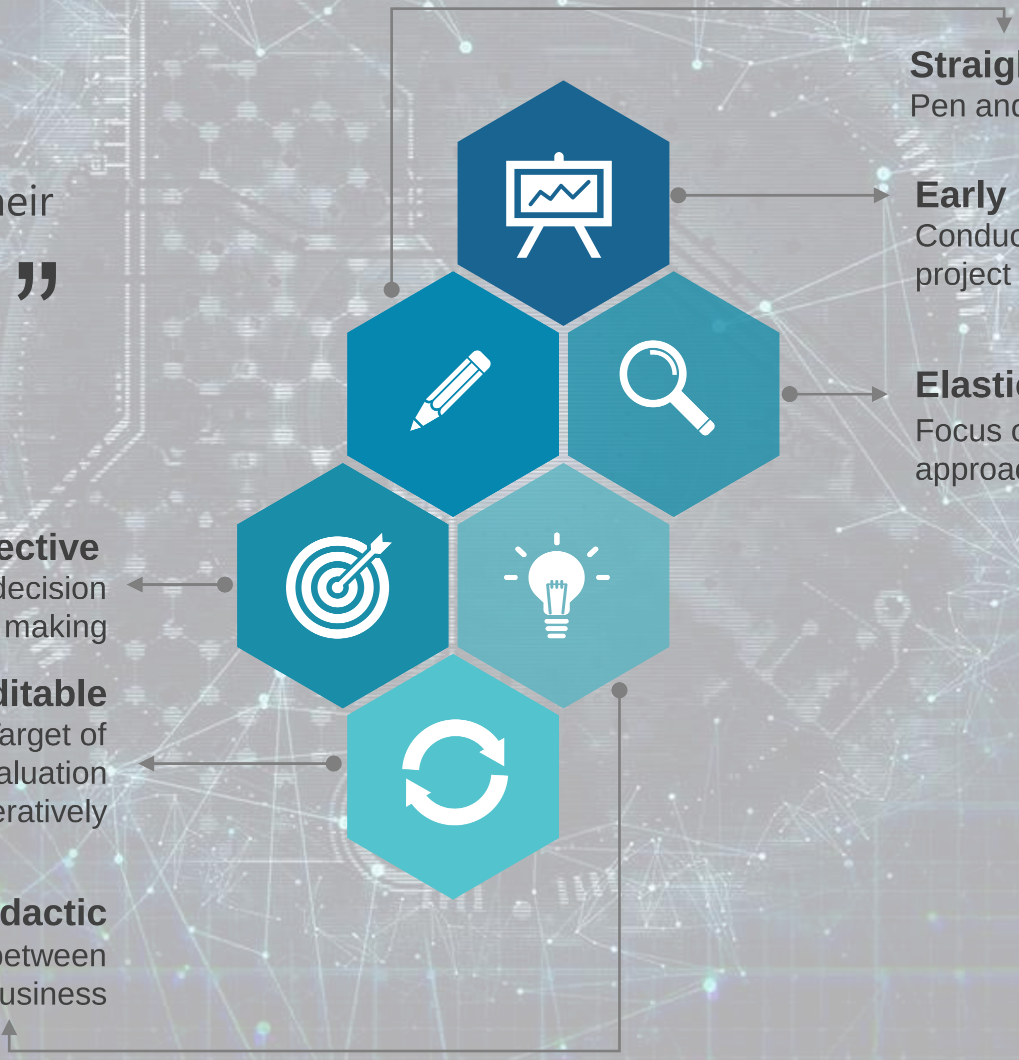
02 Threat modelling insight

Introduction to threat modelling and how threat modelling integrates into ISDPTool.

Threat modelling

Definition & properties

> “A process to identify and document threats to a particular system and their most appropriate countermeasures.”



Straightforward
Pen and paper activity

Early
Conducted at the design phase of a project

Elastic
Focus on main threats vs exhaustive approach

Objective
Provides rationale basis for decision making

Editable
Can be updated along with the Target of evaluation
Can be applied iteratively

Didactic
Allows bridging the gap between technique and business

Threat modelling flavours

Asset-centric

- Asset = something of value (vague)
- Determine assets
  - What we want to protect
  - What attackers want
  - Stepping stones
- Identify threats
  - No direct line from assets to threats

Attacker-centric

- Identify types of “profiles” likely to threaten the system
- E.g. script kiddie vs state
- E.g. Human unintentional / human intentional (insider, outsider), natural (flood, fire, lightning, etc.)
- Subjectivity / projection

Software-centric

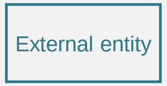
- Focus on the system being built
- Based on a graphical representation of the system
- More objective / systematic

Data flow diagrams

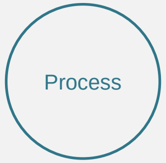
OVERVIEW

Data flow diagram (DFD)

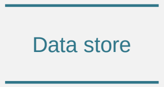
> “graphical representation of the "flow" of data through an information system, modelling its process aspects”



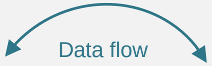
an outside system that sends or receives data, communicating with the system being diagrammed.



any process that changes the data, producing an output.



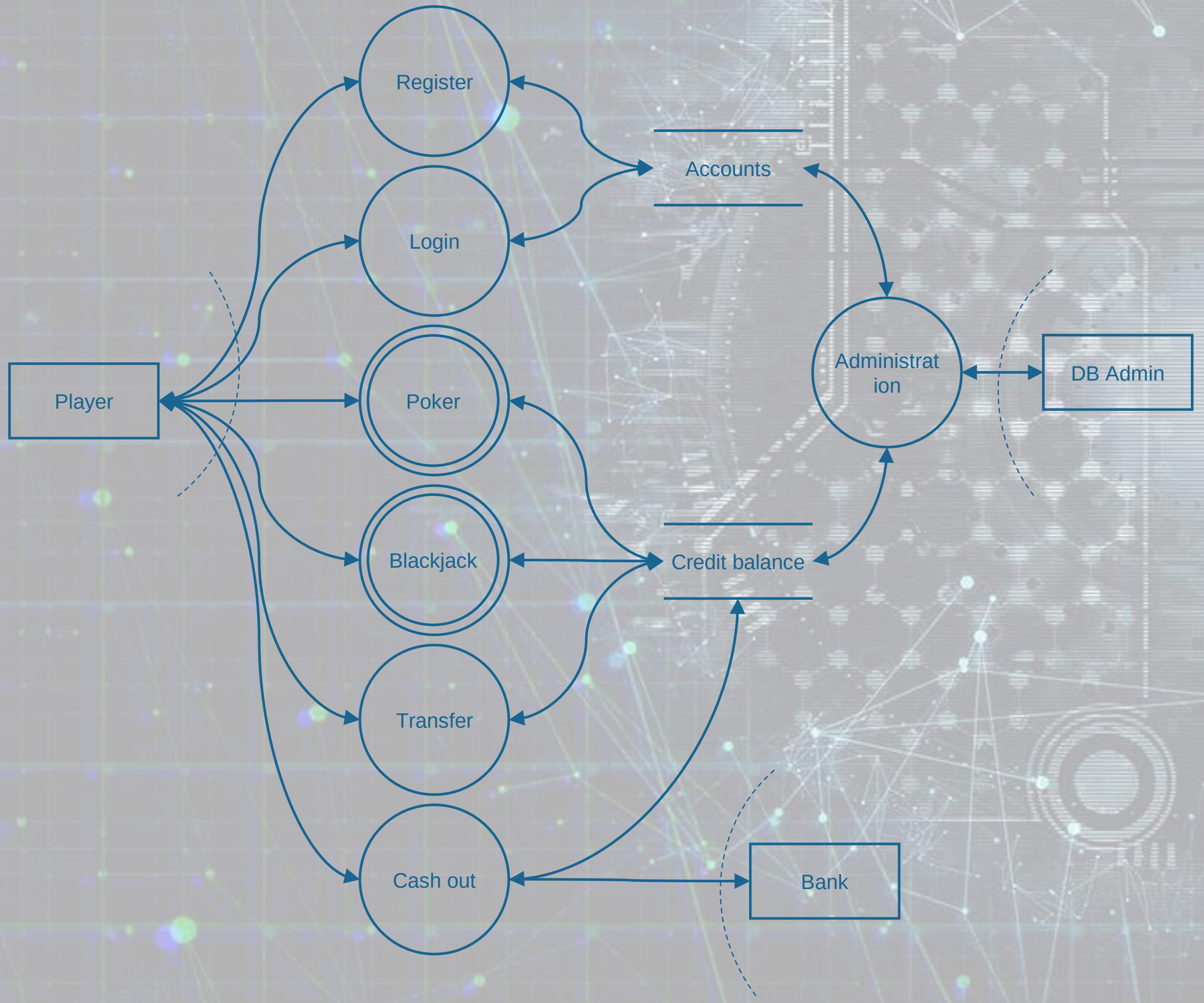
files or repositories that hold information for later use.



the route that data takes between the external entities, processes and data stores.

Threat modelling example – hacme casino

Data flow diagram

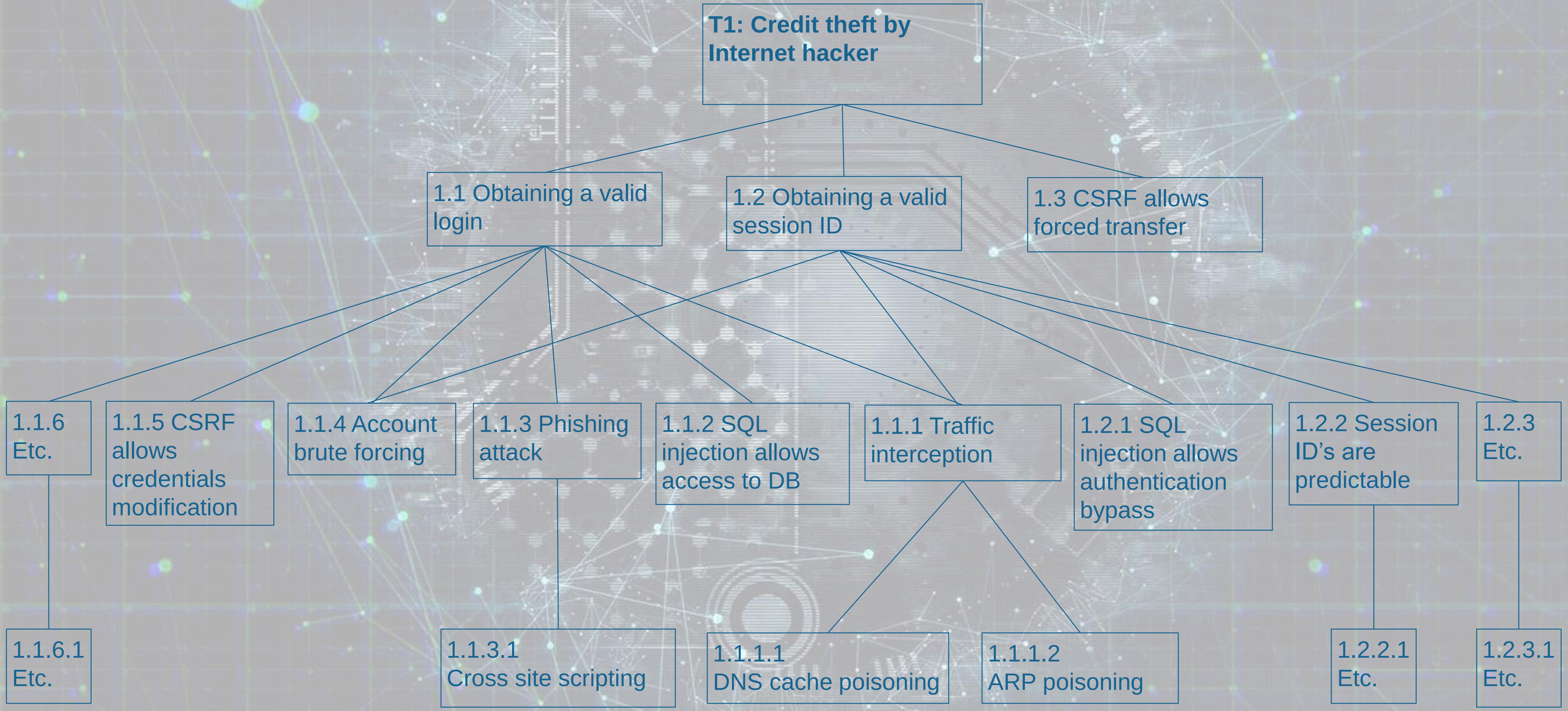


Information asset	C	I	A
Credits		x	x
Gambling amount		x	x
Players’ cards	x	x	x
Casino’s cards	x	x	x
Players’ personal data	x	x	x

#	Threat scenarios	Threat agent
T1	Credit theft	Player, Internet hacker
T2	Personal data theft	Player, Internet hacker, competitor, DB admin
T3	Game manipulation	Player
T4	Denial of service	Competitor

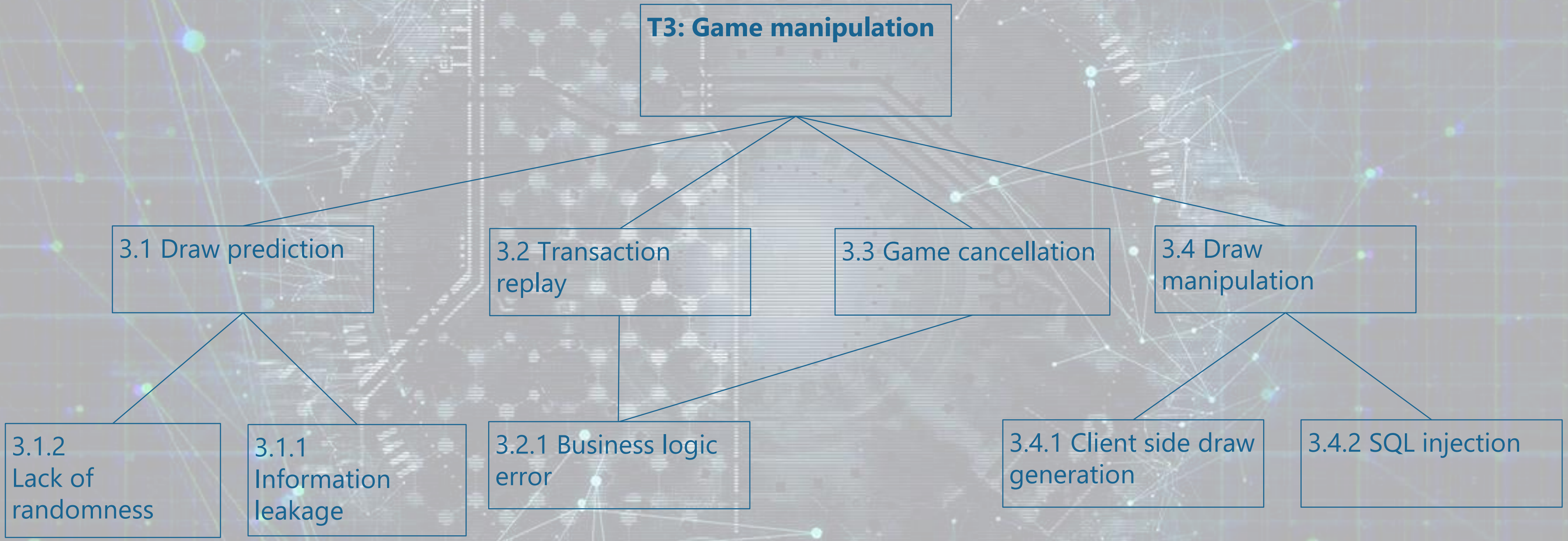
Threat modelling example – hacme casino

Threat trees


T1: Credit theft by Internet hacker
1.1 Obtaining a valid login
1.2 Obtaining a valid session ID
1.3 CSRF allows forced transfer
1.1.6 Etc.
1.1.5 CSRF allows credentials modification
1.1.4 Account brute forcing
1.1.3 Phishing attack
1.1.2 SQL injection allows access to DB
1.1.1 Traffic interception
1.2.1 SQL injection allows authentication bypass
1.2.2 Session ID's are predictable
1.2.3 Etc.
1.1.6.1 Etc.
1.1.3.1 Cross site scripting
1.1.1.1 DNS cache poisoning
1.1.1.2 ARP poisoning
1.2.2.1 Etc.
1.2.3.1 Etc.

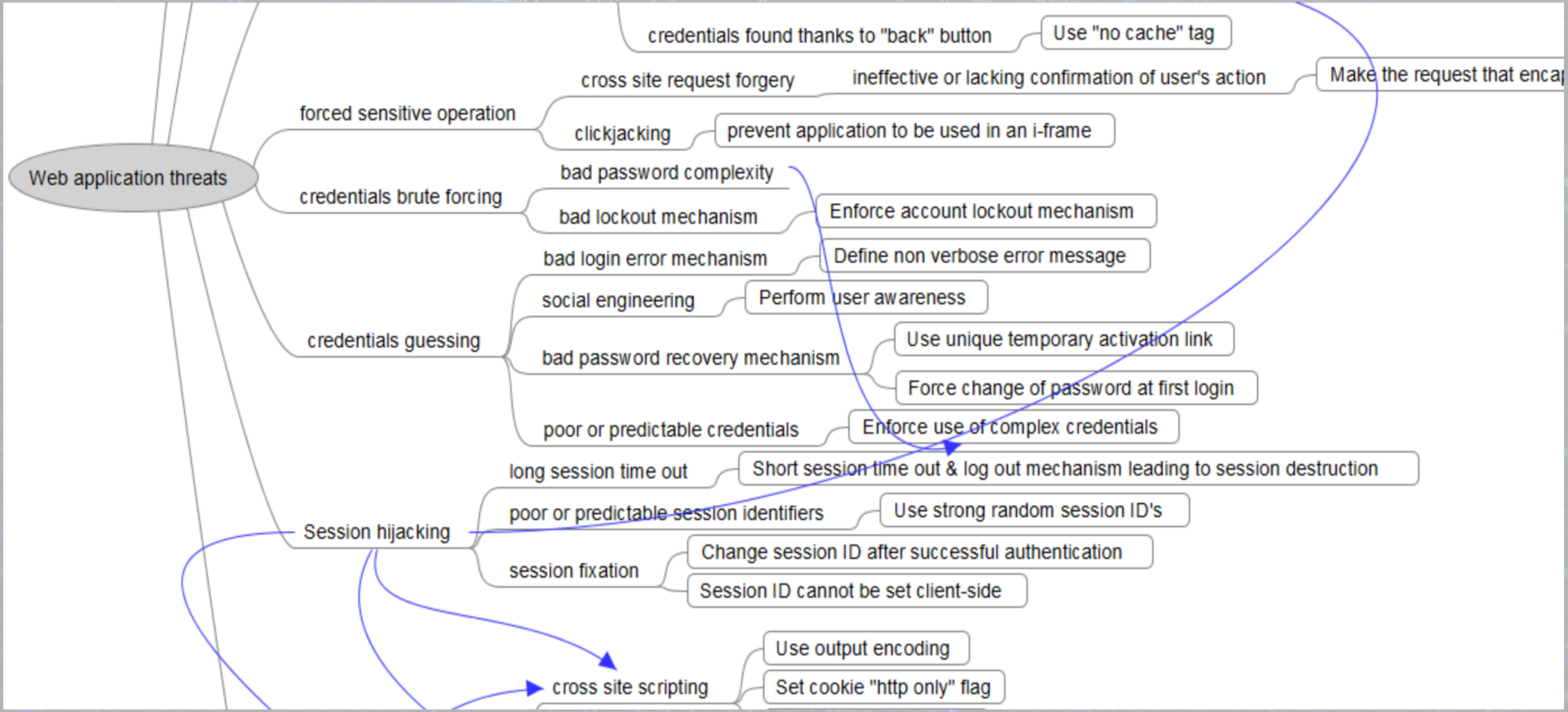
Threat modelling example – hacme casino

Threat trees



Automating threat modelling

Generic threat trees



credentials found thanks to "back" button

Use "no cache" tag

cross site request forgery

ineffective or lacking confirmation of user's action

Make the request that encap

forced sensitive operation

clickjacking

prevent application to be used in an i-frame

Web application threats

bad password complexity

credentials brute forcing

bad lockout mechanism

Enforce account lockout mechanism

bad login error mechanism

Define non verbose error message

social engineering

Perform user awareness

Use unique temporary activation link

credentials guessing

bad password recovery mechanism

Force change of password at first login

poor or predictable credentials

Enforce use of complex credentials

long session time out

Short session time out & log out mechanism leading to session destruction

poor or predictable session identifiers

Use strong random session ID's

Session hijacking

Change session ID after successful authentication

session fixation

Session ID cannot be set client-side

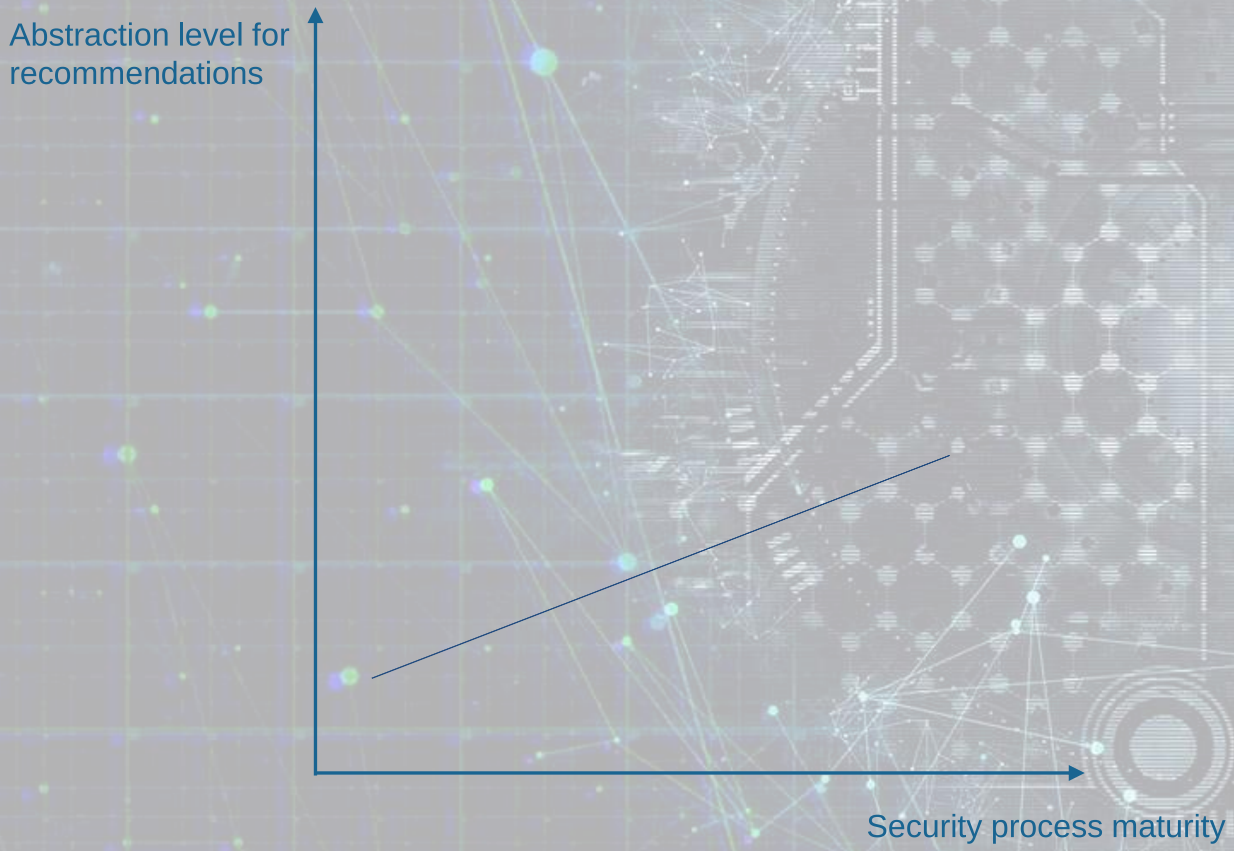
Use output encoding

cross site scripting

Set cookie "http only" flag

Evolution of needs in terms of threat modelling

“Maturity-awareness” concept

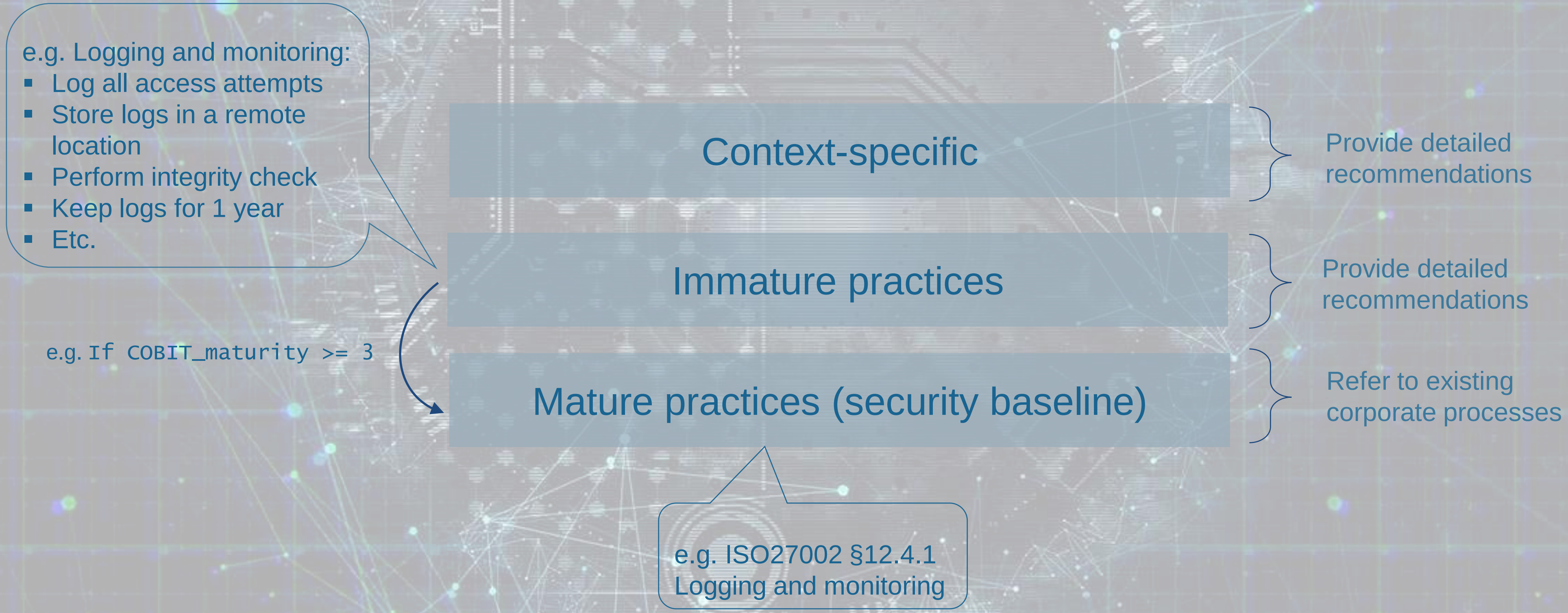


Threat	Attack means	Mitigation
Credentials theft	SQL injection	Use parameterized queries
Credentials theft	XSS	Encode output
Etc.	Etc.	Etc.

Threat	Attack means	Mitigation
Credentials theft	SQL injection	Apply secure development practices
Credentials theft	XSS	
Etc.	Etc.	

Granularity of recommendations in threat modelling

ISDPTool approach



e.g. Logging and monitoring:
- Log all access attempts
- Store logs in a remote location
- Perform integrity check
- Keep logs for 1 year
- Etc.

Context-specific — Provide detailed recommendations

Immature practices — Provide detailed recommendations

e.g. `If COBIT_maturity >= 3`

Mature practices (security baseline) — Refer to existing corporate processes

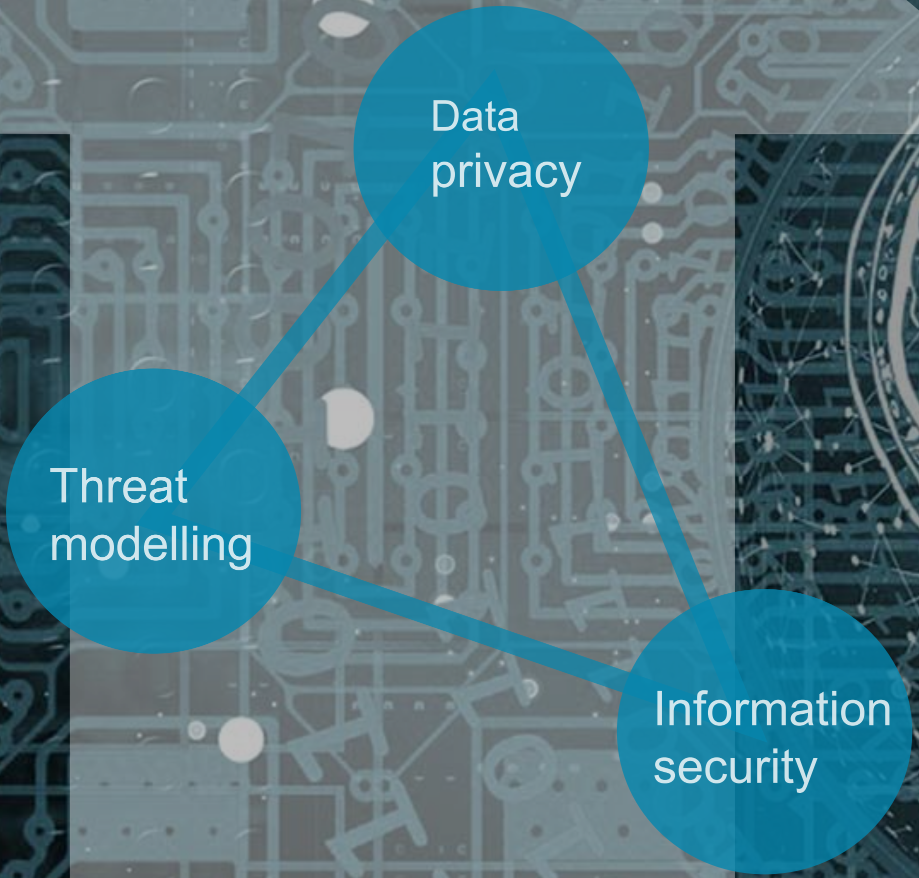
e.g. ISO27002 §12.4.1
Logging and monitoring

ISO27002 controls vs detailed recommendations

Target of evaluation	Threat agents	Threats	Mitigations (ISO27002 controls)	Protection profiles
Internet facing web application	Internet hacker	Interception/alteration of data during transport	A10.1.1 Policy on the use of cryptographic controls	TLS
			A10.1.2 Key management	
			A13.1.2 Security of network services	
			14.1.2 Securing applications services on public networks	
	Etc.	Etc.	Etc.	Etc.

03 ISDPTool

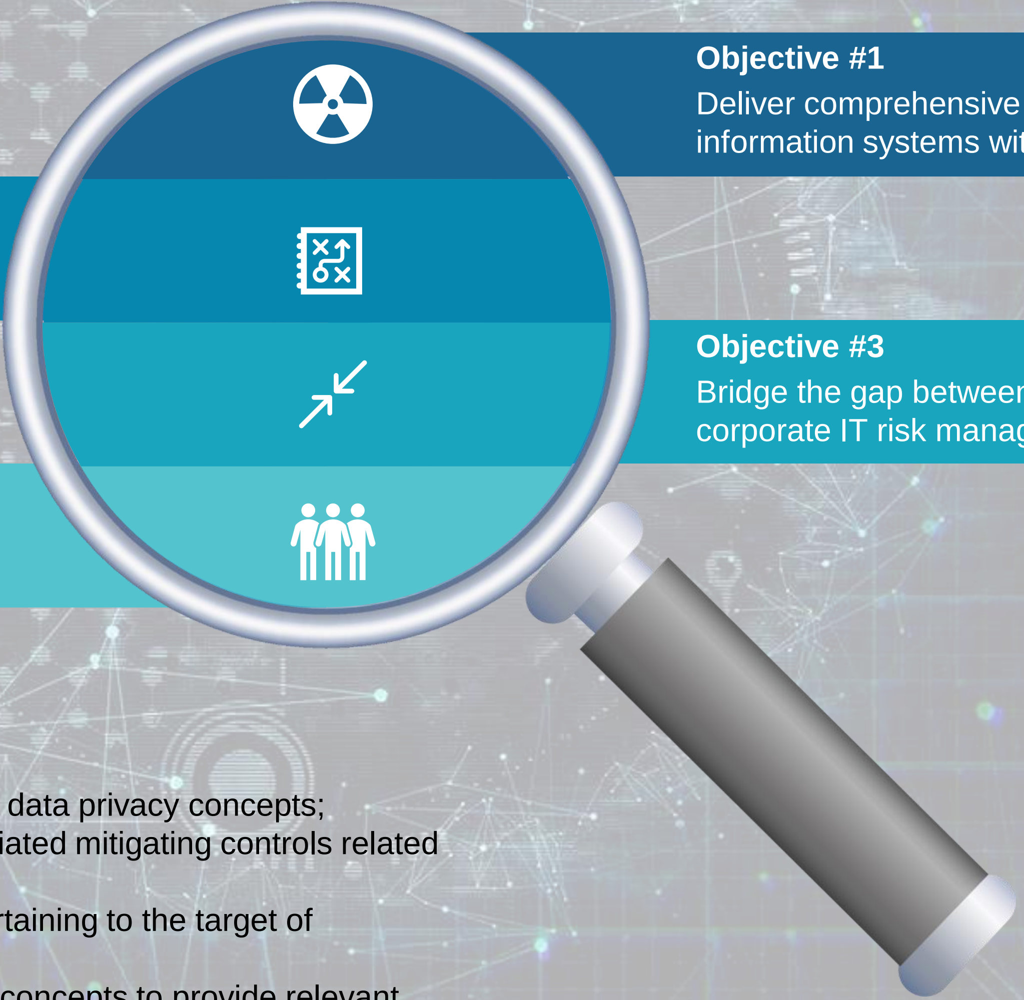
Overview of the ISDPTool features.



Leveraging threat modelling techniques for efficient information security and data privacy management

ISDPTool

ISDPTool objectives



Objective #1

Deliver comprehensive threat analysis of information systems with reduced effort.

Objective #2

Provide concrete guidance to address information security and data privacy in IT projects.

Objective #3

Bridge the gap between field security and corporate IT risk management.

Objective #4

Avoid duplication of efforts between information security and data privacy management.

In brief

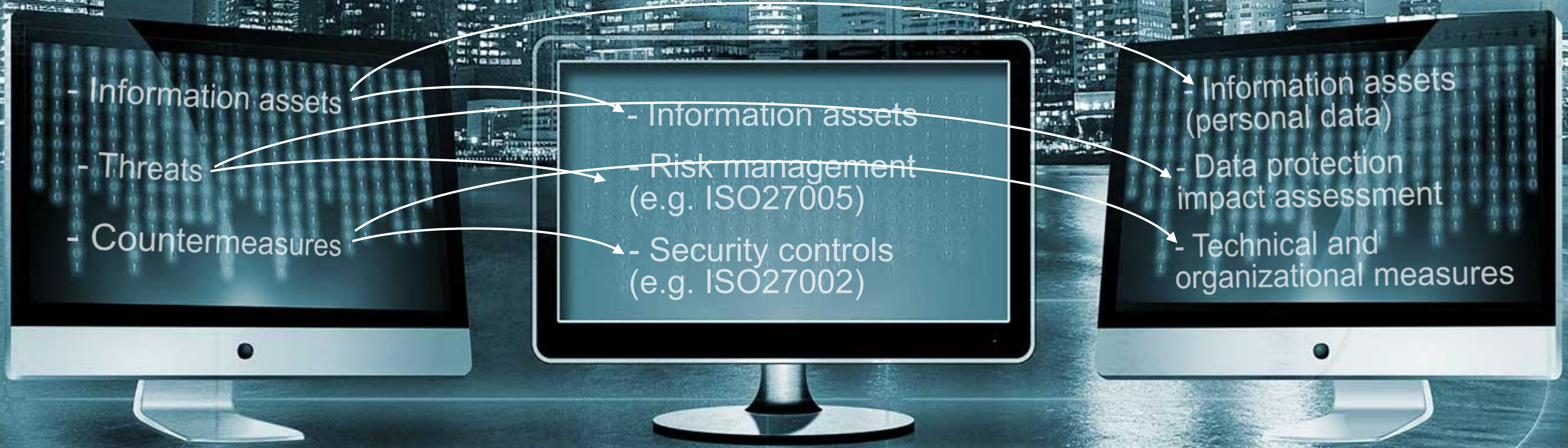
- ISDPTool allows performing information security and data privacy concepts;
- It specifies all information security threats and associated mitigating controls related to a given information system;
- It provides rationales for estimating residual risks pertaining to the target of evaluation;
- ISDPTool also aggregates results of individual ISDP concepts to provide relevant consolidated figures.

●→◆ ↓ ■←● Threat modelling

Information security management

Data privacy management

Using threat modelling for information security and data privacy management



- Information assets
- Threats
- Countermeasures

- Information assets
- Risk management (e.g. ISO27005)
- Security controls (e.g. ISO27002)

- Information assets (personal data)
- Data protection impact assessment
- Technical and organizational measures

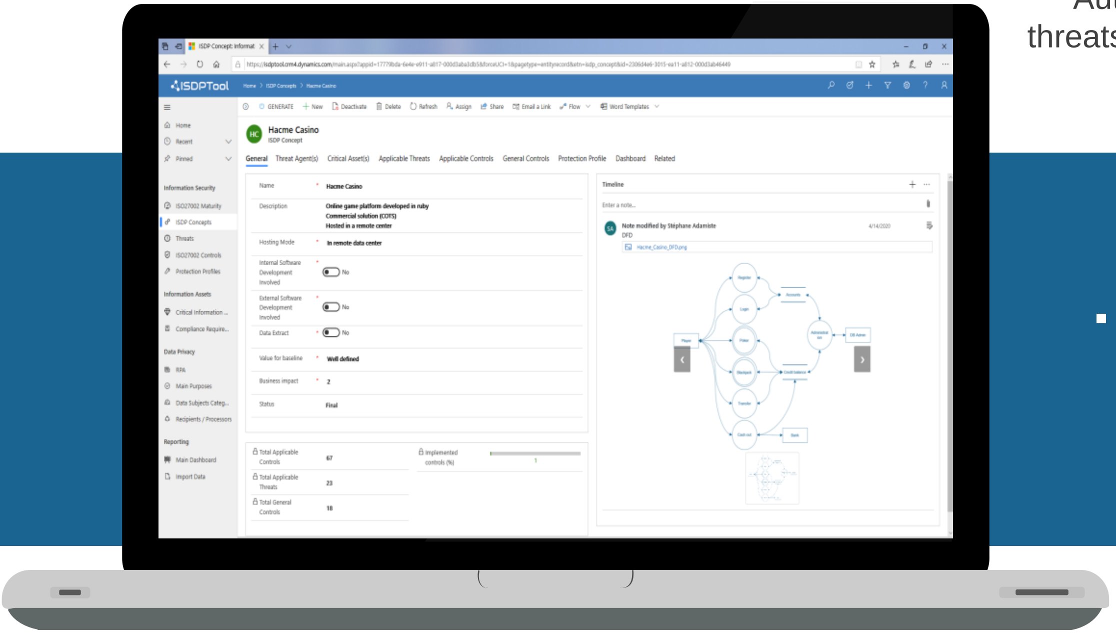
ISDPTool features

Methodological references

- Threat modelling
- ISO27002
- ISO27005
- OCTAVE Allegro

Automation

Automatic listing of applicable threats and associated mitigating controls to any IT system



Hacme Casino
ISDP Concept

Name * Hacme Casino

Description Online game platform developed in ruby
Commercial solution (COTS)
Hosted in a remote center

Hosting Mode * In remote data center

Internal Software Development Involved * No

External Software Development Involved * No

Data Extract * No

Value for baseline * Well defined

Business impact * 2

Status Final

Total Applicable Controls 67

Total Applicable Threats 23

Total General Controls 18

Implemented controls (%) 1

Note modified by Stéphane Adamiste 4/14/2020
DFD
Hacme_Casino_DFD.png

Output optimisation

- Filtering of mature controls (a.k.a. “security baseline”)
- Specific controls vs general controls

Granularity of controls

- Implementation hints for ISO27002 controls
- Protection profiles

Records of processing activities

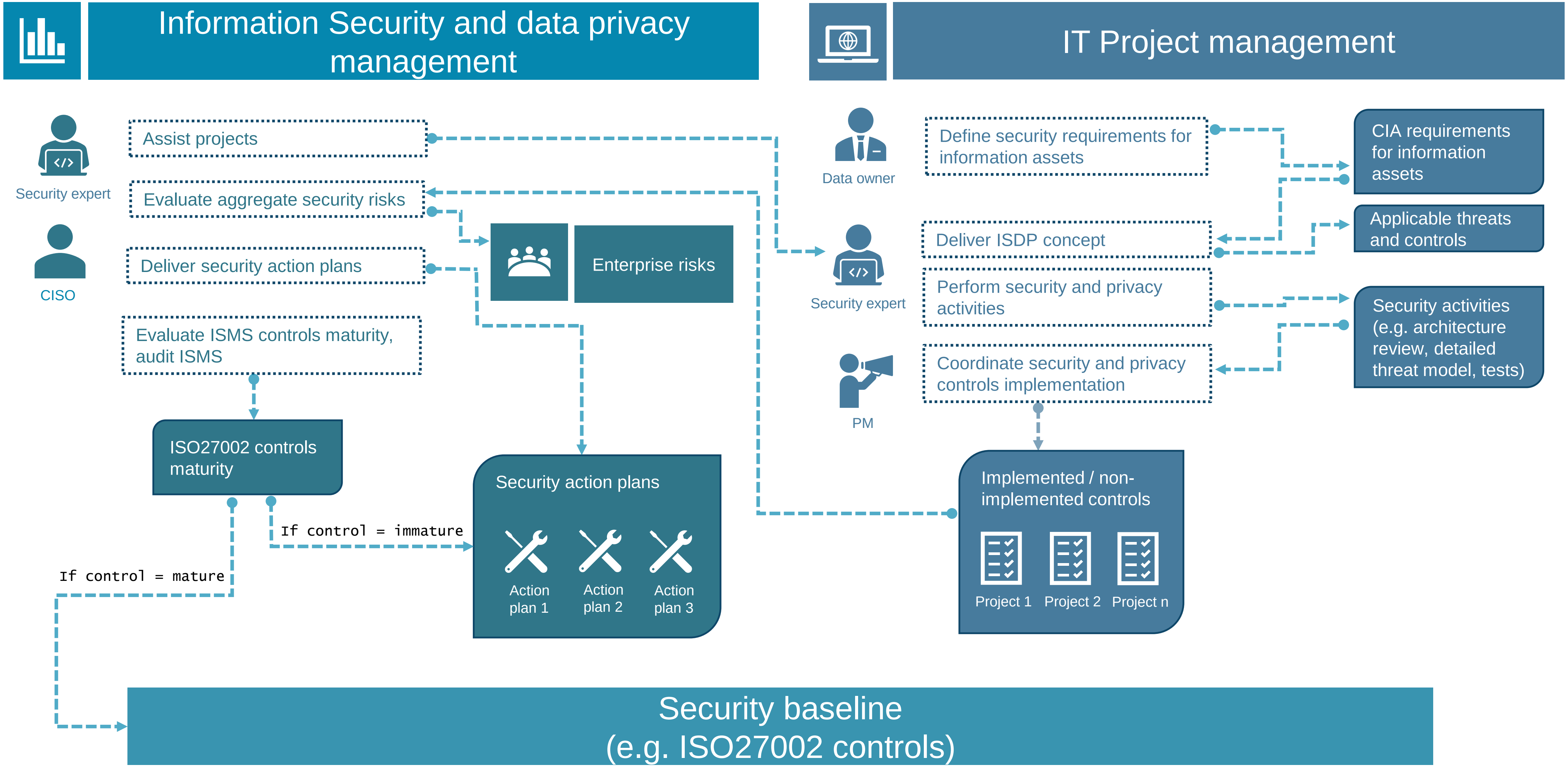
Assisted mode for the drafting of RPA to ease GDPR compliance

ISMS management

- Follow-up of control implementation status
- Aggregated stats for realistic security posture evaluation and enterprise risk reporting

Information security & data privacy management in IT projects

Target organisation



Information Security and data privacy management
IT Project management
Security expert
CISO
Assist projects
Evaluate aggregate security risks
Deliver security action plans
Evaluate ISMS controls maturity, audit ISMS
Enterprise risks
ISO27002 controls maturity
If control = immature
If control = mature
Security action plans
Action plan 1
Action plan 2
Action plan 3
Data owner
Security expert
PM
Define security requirements for information assets
Deliver ISDP concept
Perform security and privacy activities
Coordinate security and privacy controls implementation
CIA requirements for information assets
Applicable threats and controls
Security activities (e.g. architecture review, detailed threat model, tests)
Implemented / non-implemented controls
Project 1
Project 2
Project n
Security baseline
(e.g. ISO27002 controls)

THANK YOU

Information security and data privacy management with ISDPTool

Music: AShamaluevMusic
Template: allppt.com

✉ contact@isdptool.com