

RESEARCH & TECHNOLOGY

Campus Polytechnique
1, avenue Augustin Fresnel
91767 Palaiseau cedex France
Tel : +33 (0)1 69 41 55 00
Fax : +33 (0)1 69 41 59 69
www.thalesgroup.com

REPORT / TECHNICAL DOCUMENT

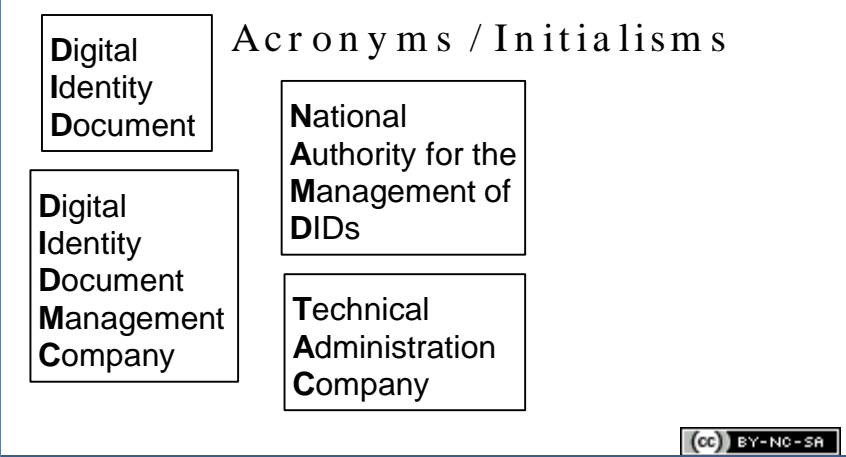
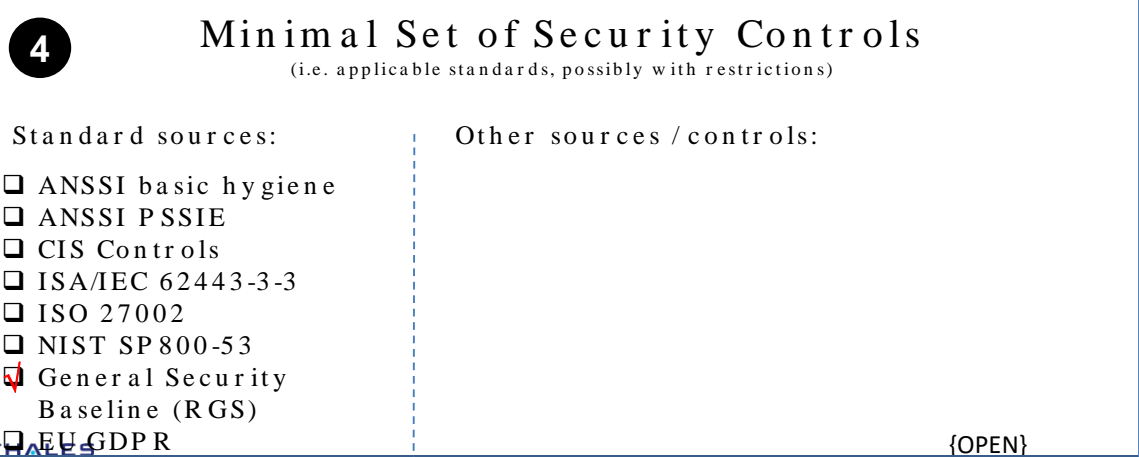
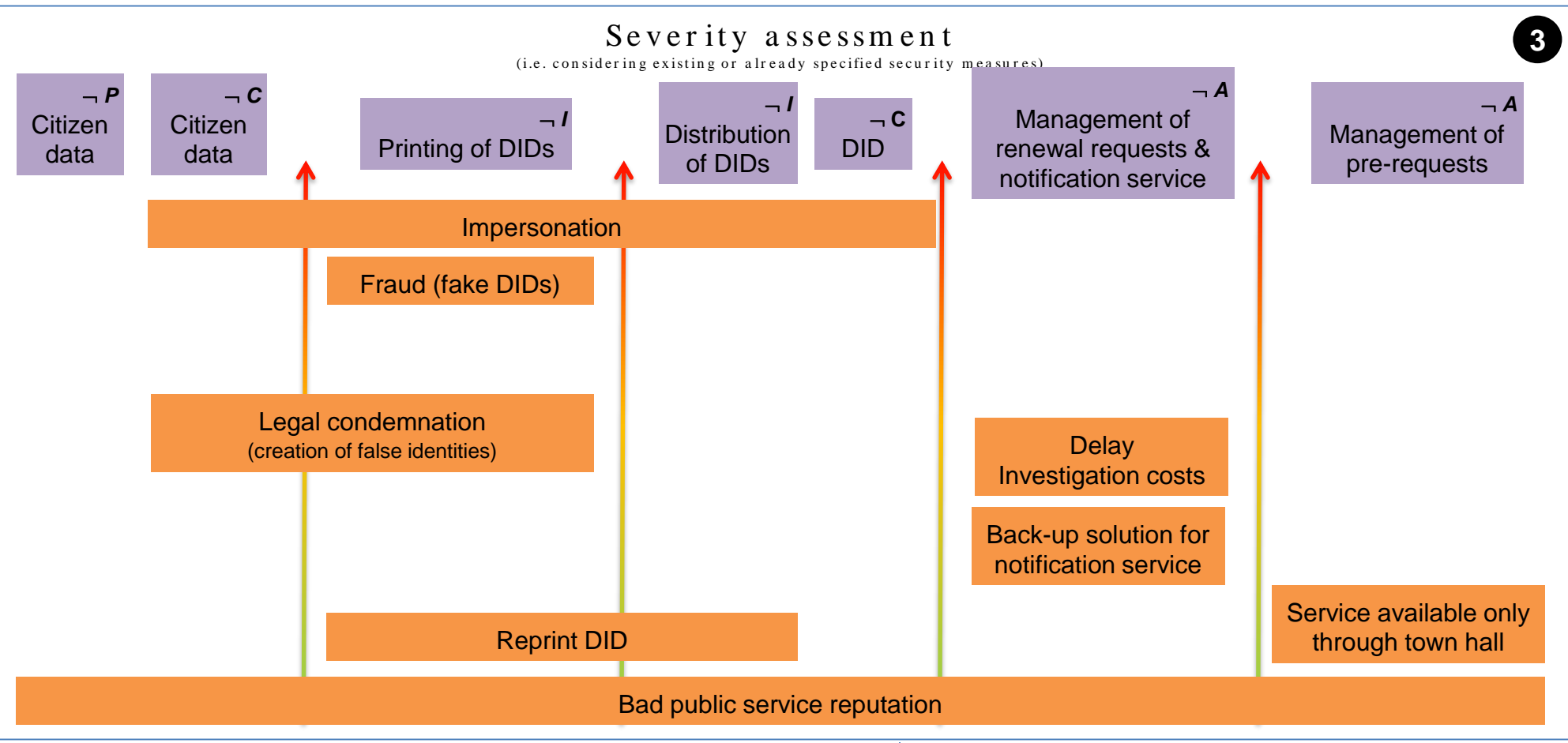
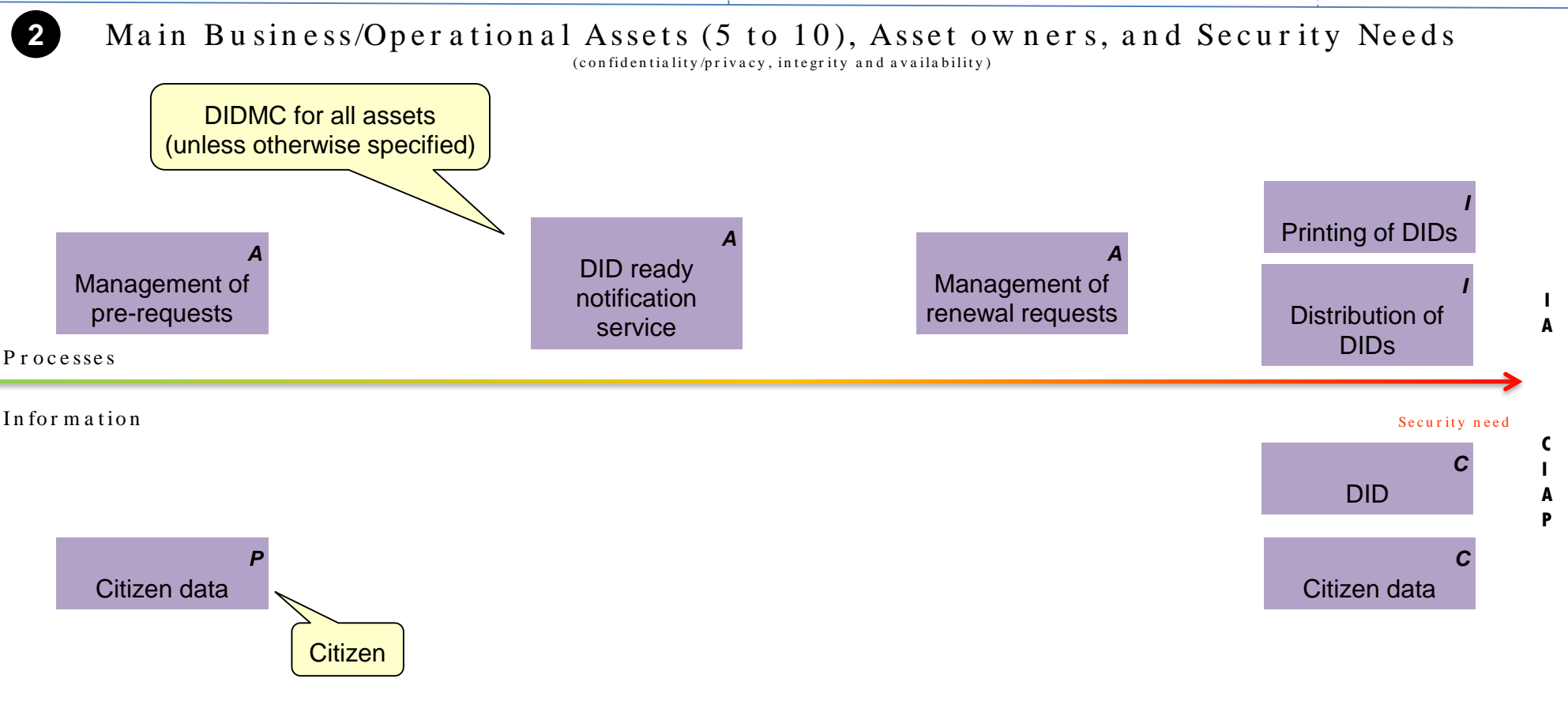
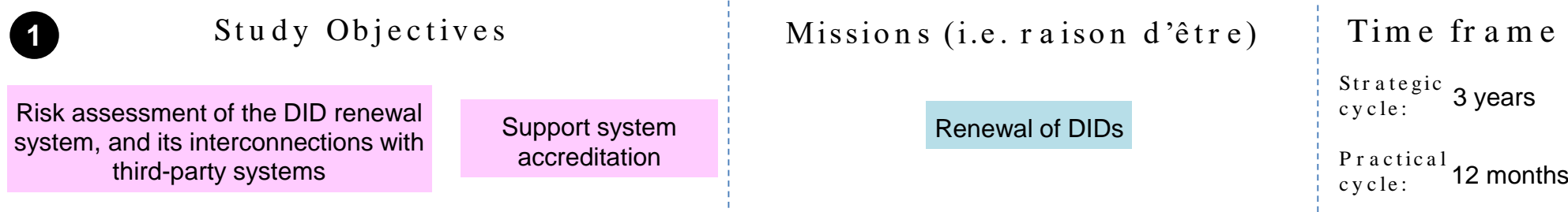
RENEWAL OF DIGITAL IDENTITY DOCUMENTS

CYBERSECURITY RISK ASSESSMENT REPORT

TRAINER: STÉPHANE PAUL

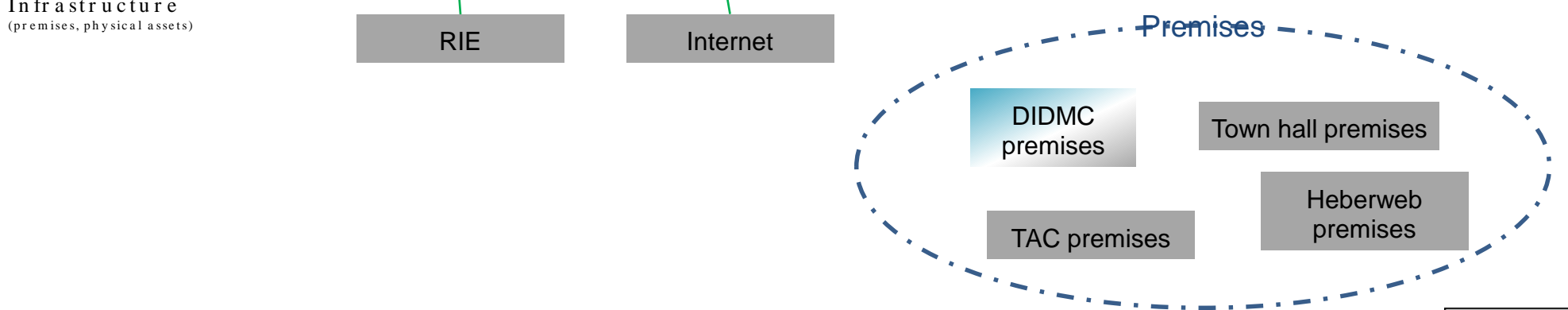
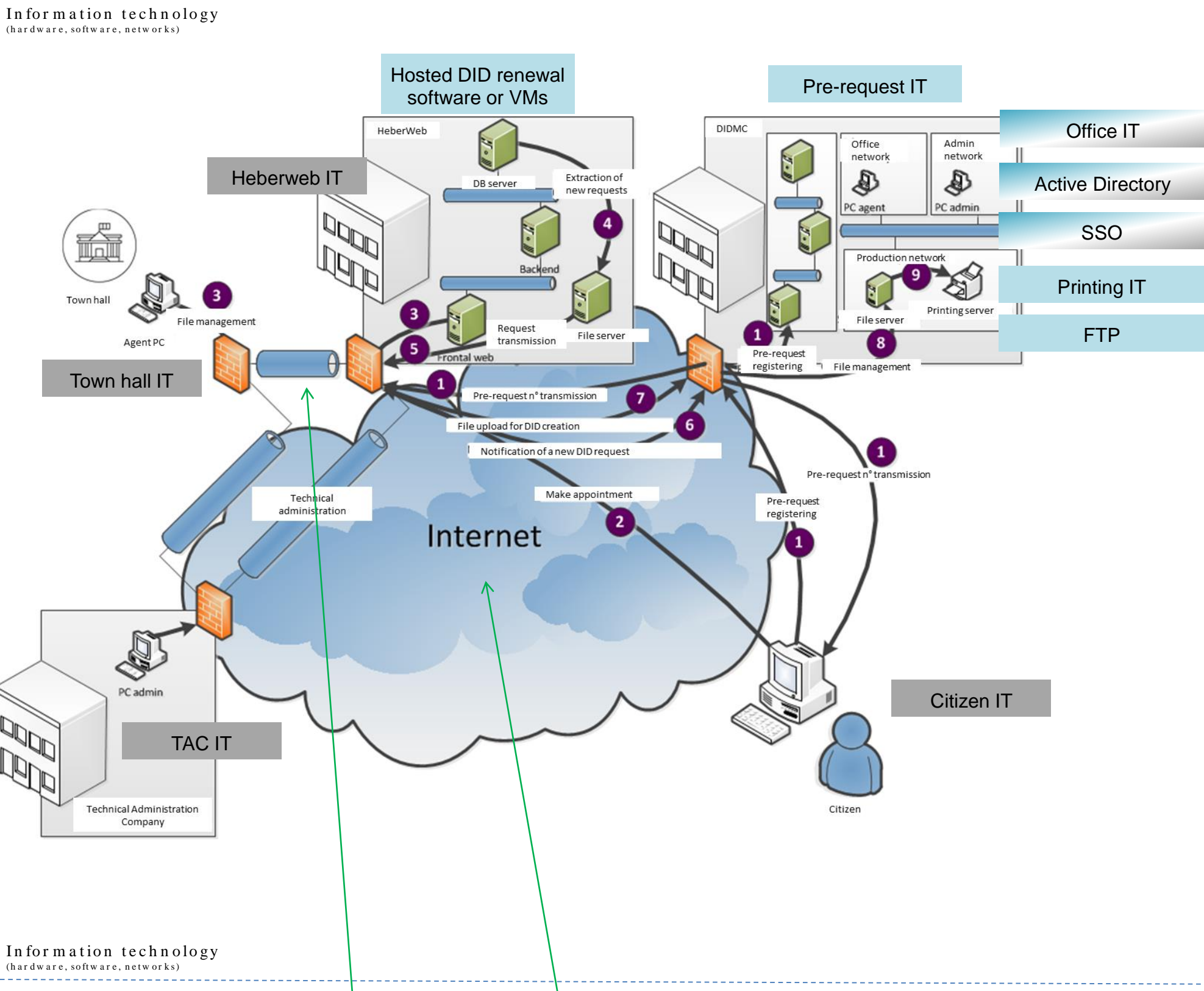
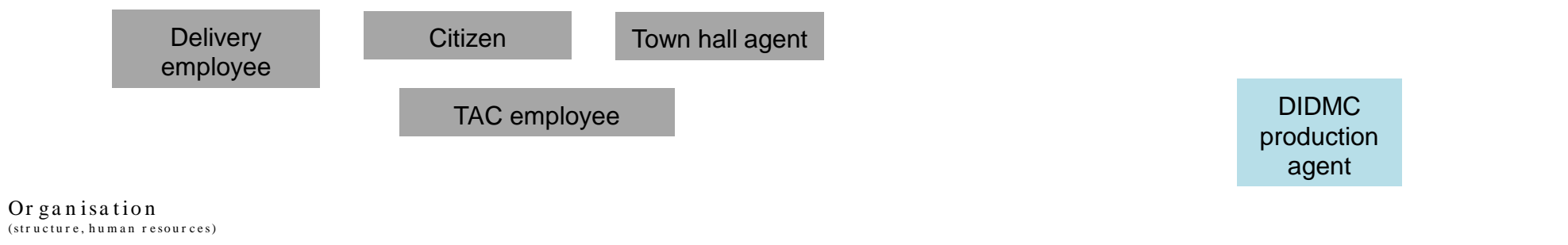
TRAINEES:

.....
.....
.....
.....



4

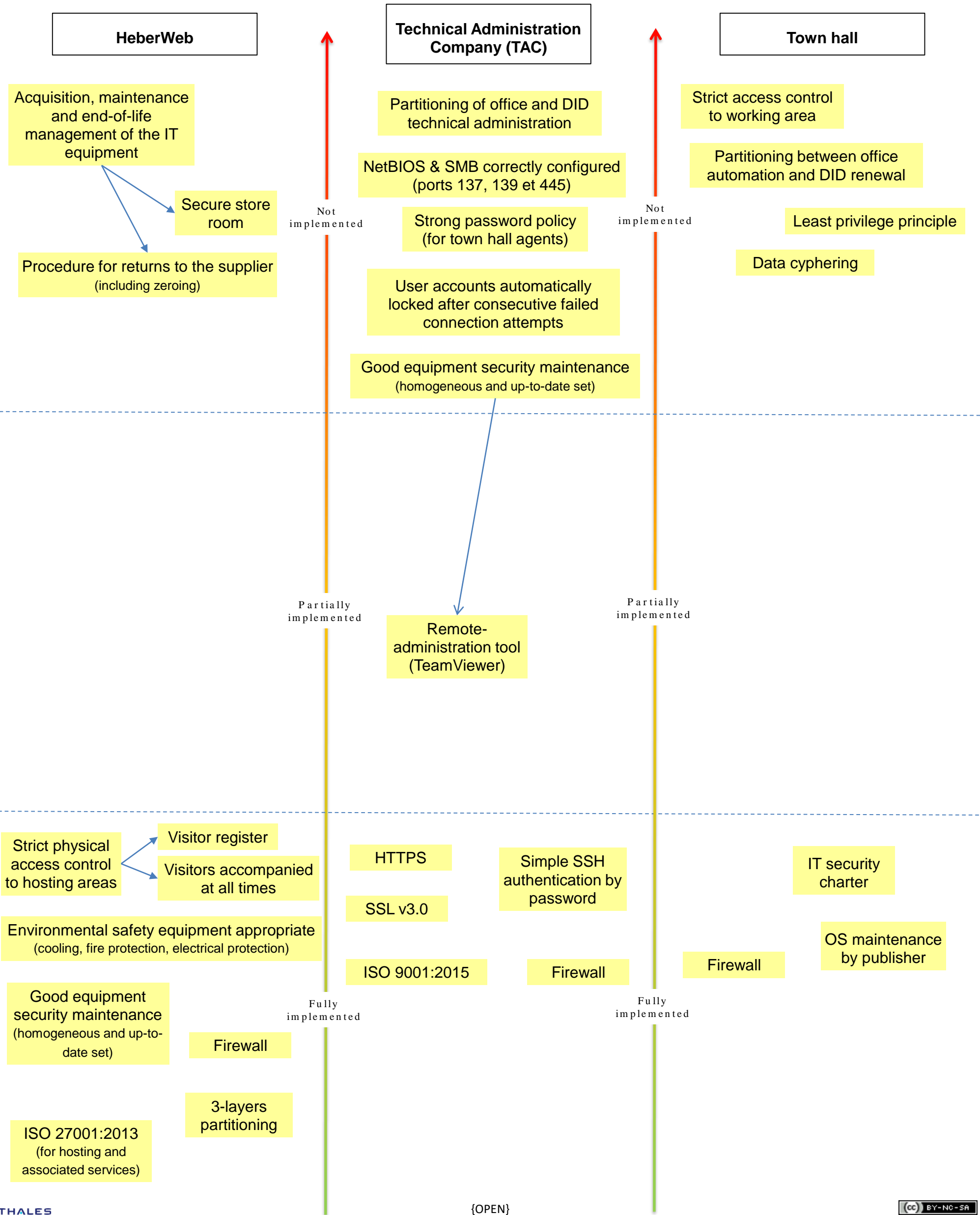
Main supporting assets



5

Existing or already specified security controls

(assessment of implementation status)



5

Existing or already specified security controls

(assessment of implementation status)

DIDMC

Input data validation
(from HerberWeb)

Incident management (audits)

Secure WAN communication

Strict access control to directories
related to DID renewal activities

Space partitioning between
DID renewal activities and
other activities
(based on separate
directories)

Authentication via
centralised SSO and AD

3-layer
partitioning

Firewall

Network segmentation (pre-
request, printing...)

Not
implemented

Not
implemented

Partially
implemented

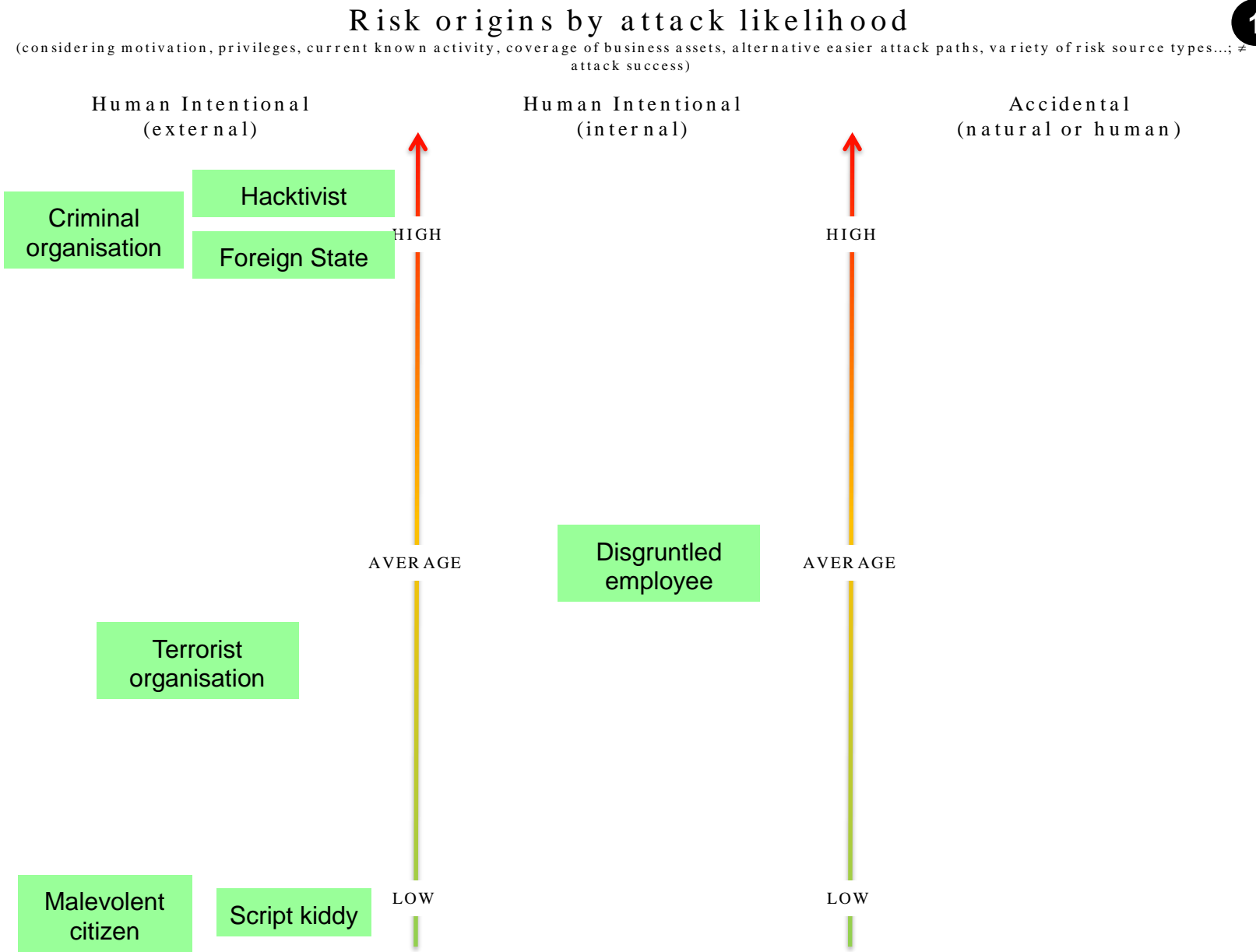
Partially
implemented

Fully
implemented

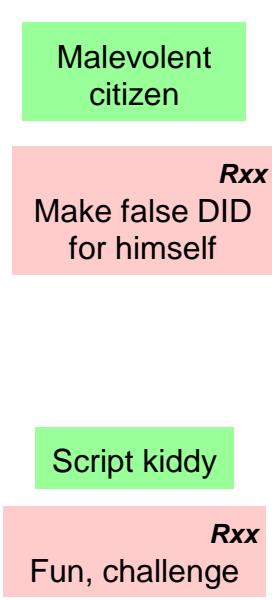
Fully
implemented

1

Rejected risk origins

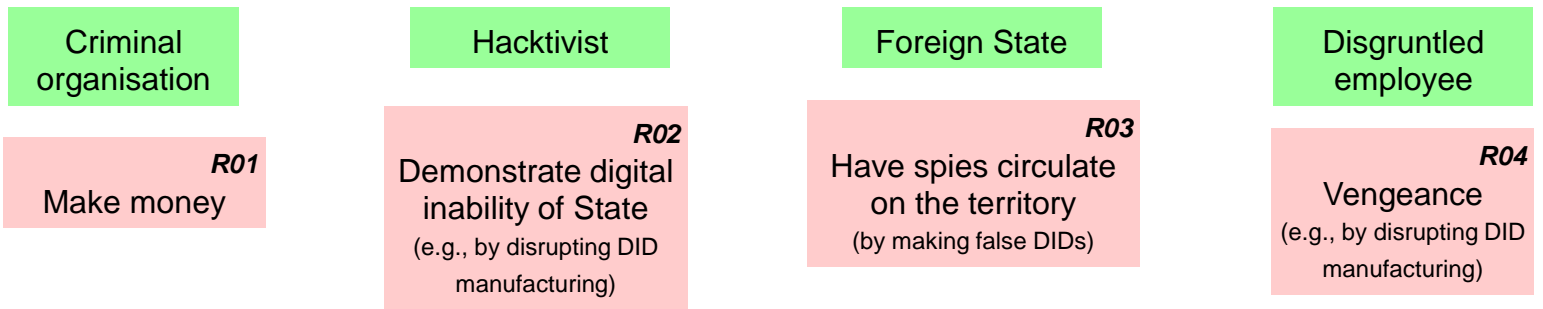


Rejected RO / TO

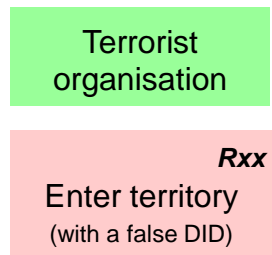


Retained risk origins / target objectives

(i.e., considering security needs, and existing or already specified security measures)



(consider now)
(consider later)

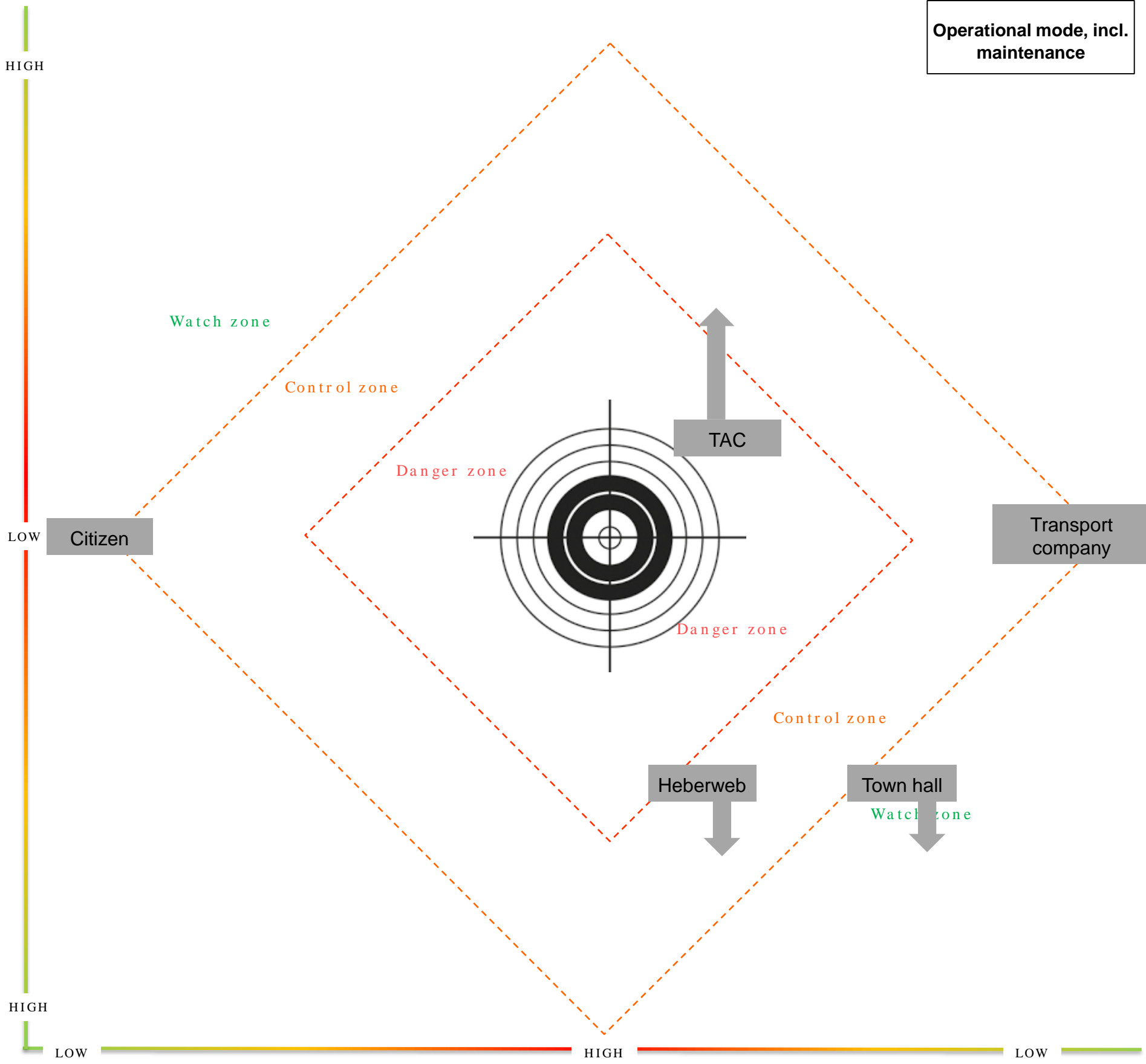


Ecosystem

(i.e., dependency on participant, participant rights, participant maturity, trust in participant...)

Operational mode, incl. maintenance

Participant cyber-reliability



System exposure to participant

3 Derived minimal set of security controls / security objectives on the ecosystem

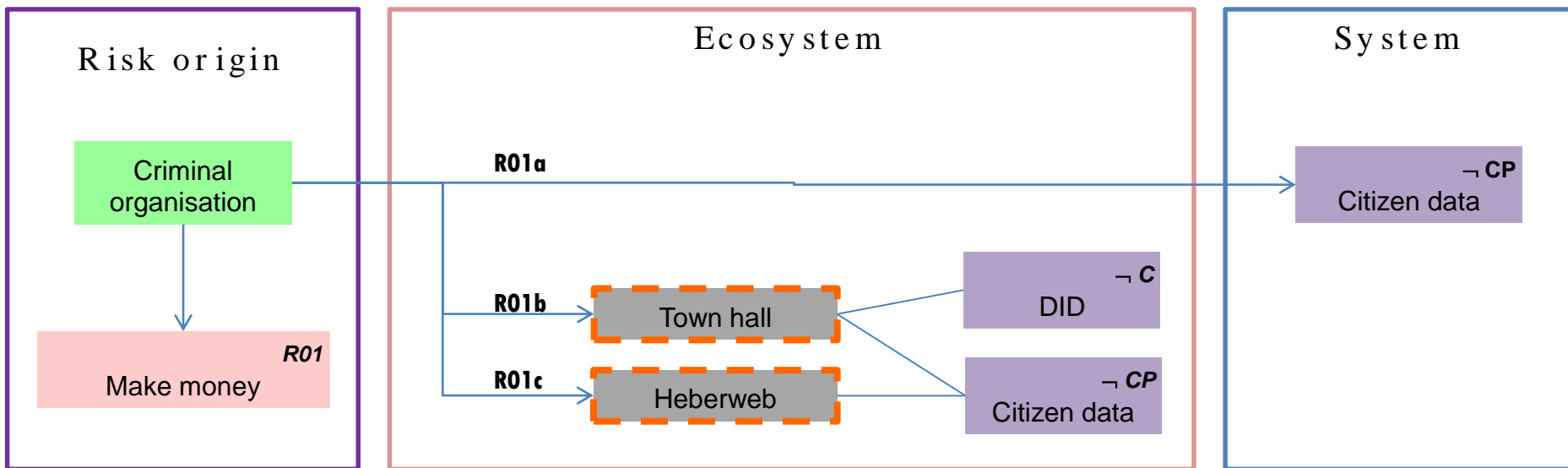
(the grey arrows indicate the evolution of the criticality of the participants after application of the security measures)

Standard sources:

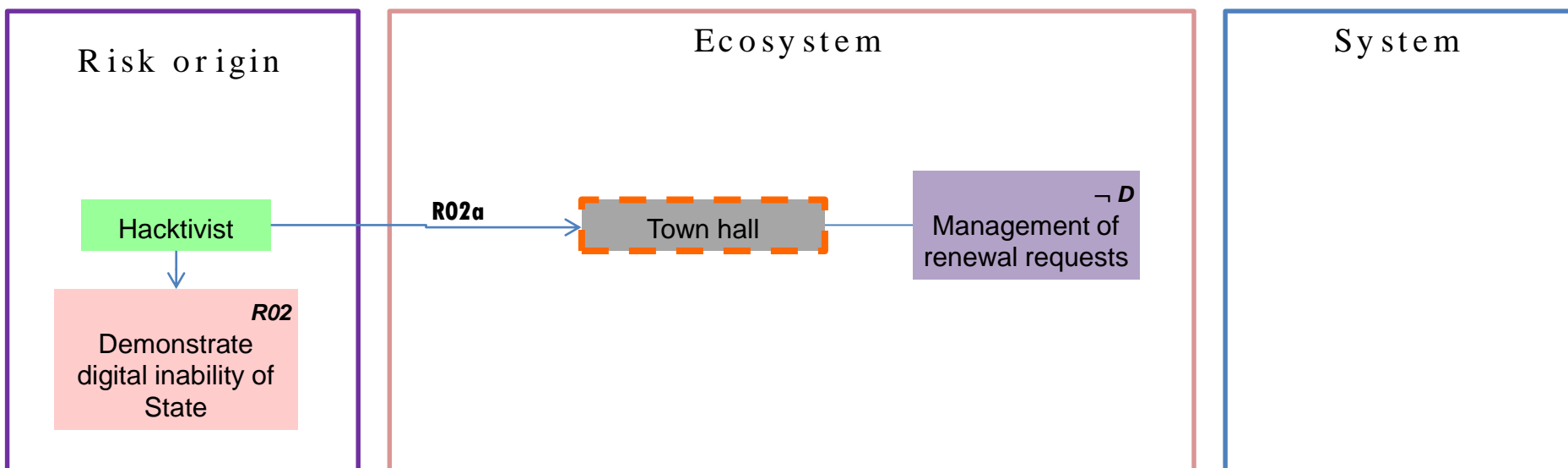
- ANSSI basic hygiene (standard)
- ANSSI basic hygiene (reinforced)
- ANSSI PSSIE
- CIS Controls
- ISA/IEC 62443-3-3 (SL1)
- ISA/IEC 62443-3-3 (SL2)
- ISA/IEC 62443-3-3 (SL3)
- ISA/IEC 62443-3-3 (SL4)
- ISO 27002
- NIST SP 800-53 (low)
- NIST SP 800-53 (moderate)
- NIST SP 800-53 (high)

It is suggested to implement all the incorrectly implemented or missing measures raised during the audits on the TAC, the Town hall and Heberweb (see top of slide 4).

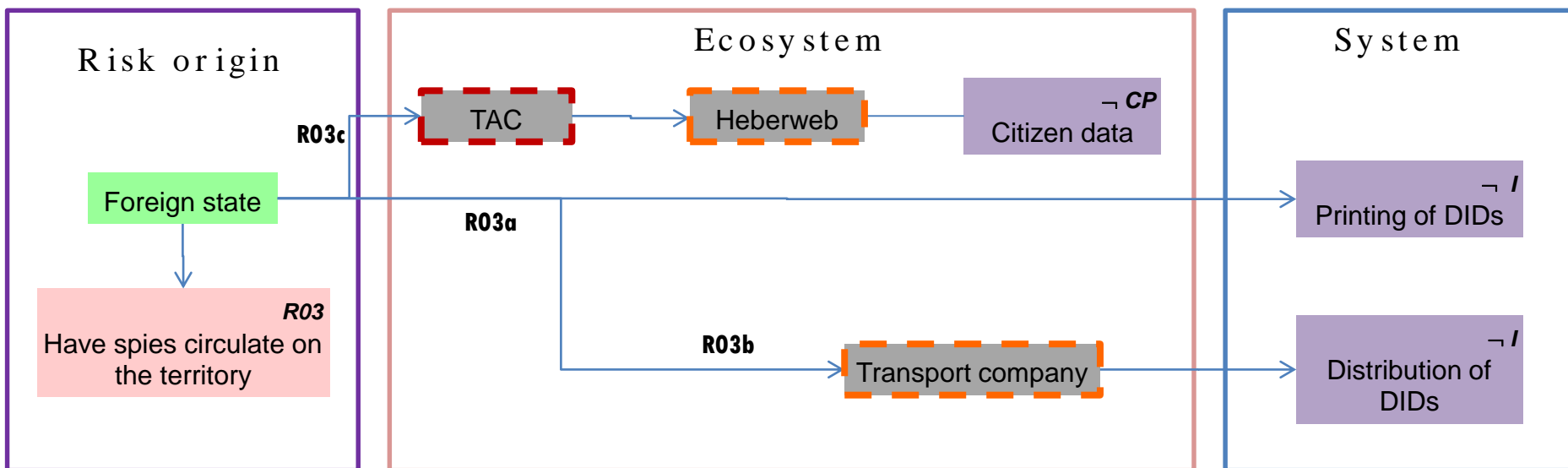
Severity: 4



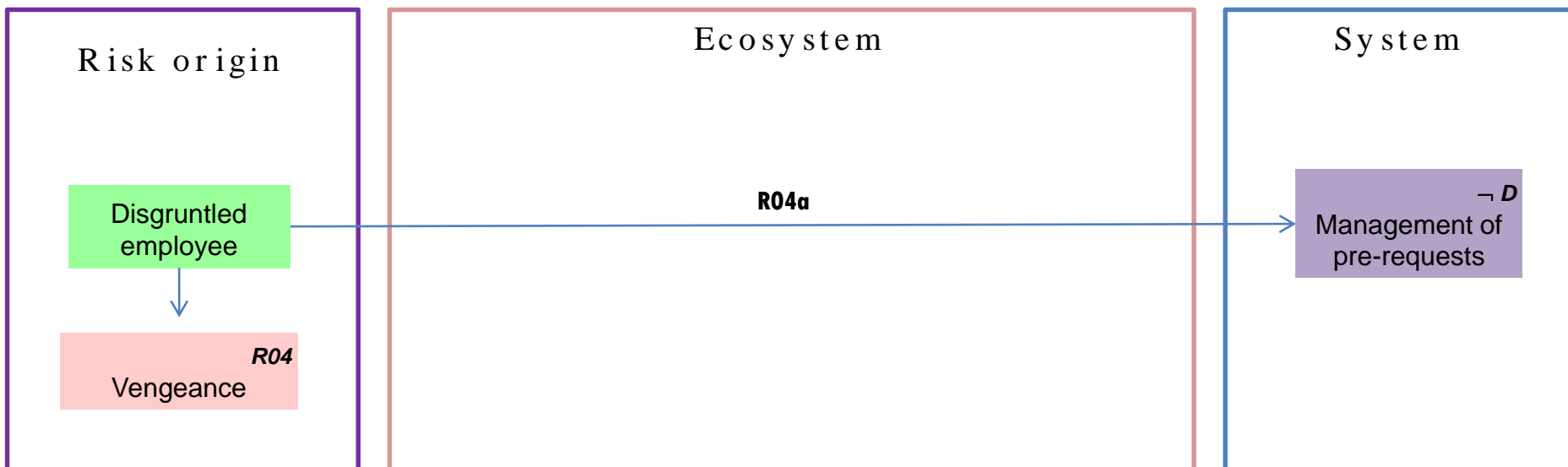
Severity: 3

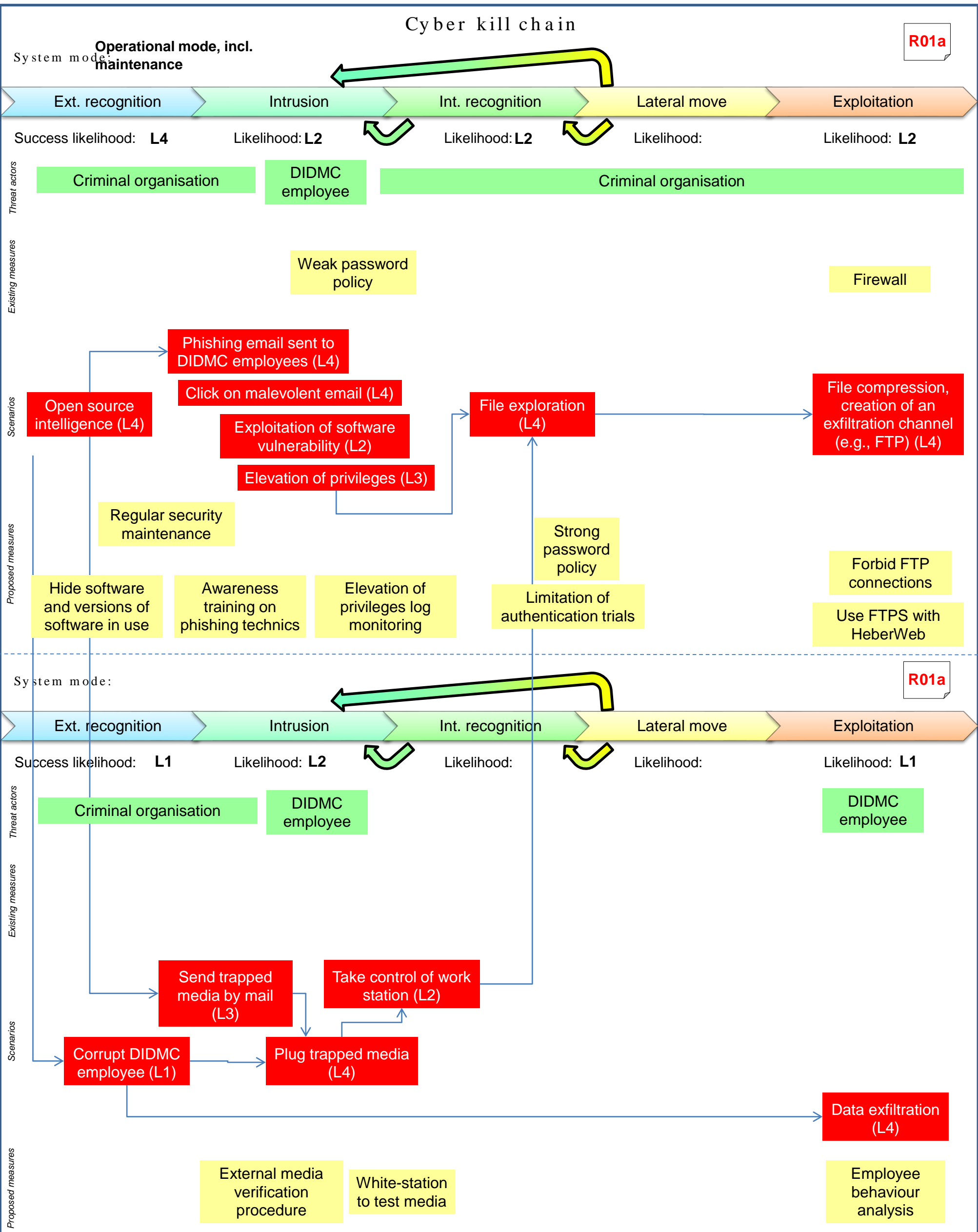


Severity: 4



Severity: 1





List of risks

(include at least threat source, business asset, feared event, impact, supporting asset, and possibly exploited vulnerability inside risk description – use colour coding for severity)

Risk n°	Risk description	Risk owner	Comment
R01a	To make money, a criminal organization steals citizen data in the DIDMC IT system, by leveraging a phishing email, sending of a booby-trapped key and/or by corrupting DIDMC staff, and resells that data to support impersonation.	DIDMC	Severity: 4 Likelihood: 2
R01b	To make money, a criminal organisation steals citizen data within the town hall IT system, and resells that data to support impersonation.	DIDMC	Severity: 4 Likelihood: ?
R01c	To make money, a criminal organisation steals citizen data from dismantled HeberWeb equipment, and resells that data to support impersonation.	DIDMC	Severity: 4 Likelihood: ?
R02a	An hacktivist traps the DID renewal function on the PC of a town hall employee, rendering the service unusable, thus demonstrating the digital inability of the State.	DIDMC	Severity: 2-3 Likelihood: ?
R03a	A foreign state creates or modifies a DID renewal request in HerberWeb, exploiting the Team Viewer administration tool, in order to support impersonation for one of its spies.	DIDMC	Severity: 4 Likelihood: ?
R03b	A foreign state corrupts a DIDMC employee to have a false DID printed for one of its spies.	DIDMC	Severity: 4 Likelihood: ?
R03c	A foreign state steals DIDs during the transport, to support impersonation for its spies.	DIDMC	Severity: 4 Likelihood: ?
R04a	An internal DIDMC employee disrupts the DID manufacturing process by leveraging his access rights on the pre-request IT system, in order to lower the reputation of the organisation.	DIDMC	Severity: 1 Likelihood: ?

Scales

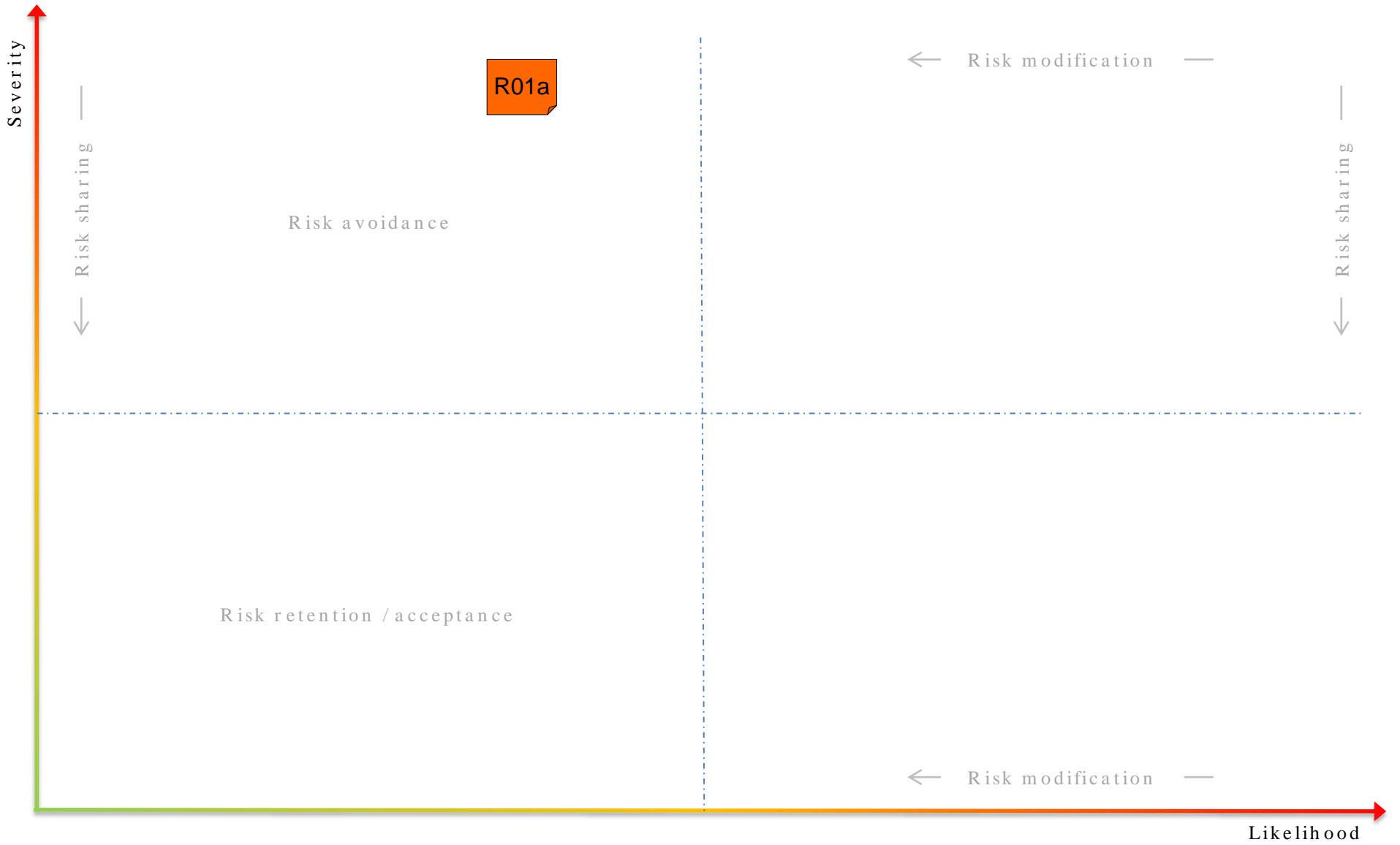
SEVERITY SCALE
G4 – CRITICAL
G3 – SERIOUS
G2 – SIGNIFICANT
G1 – MINOR

LIKELIHOOD SCALE
L4 – CERTAIN OR ALREADY OCCURRED
L3 – VERY LIKELY
L2 – LIKELY
L1 – RATHER UNLIKELY

RISK LEVEL SCALE
HIGH
MODERATE
LOW

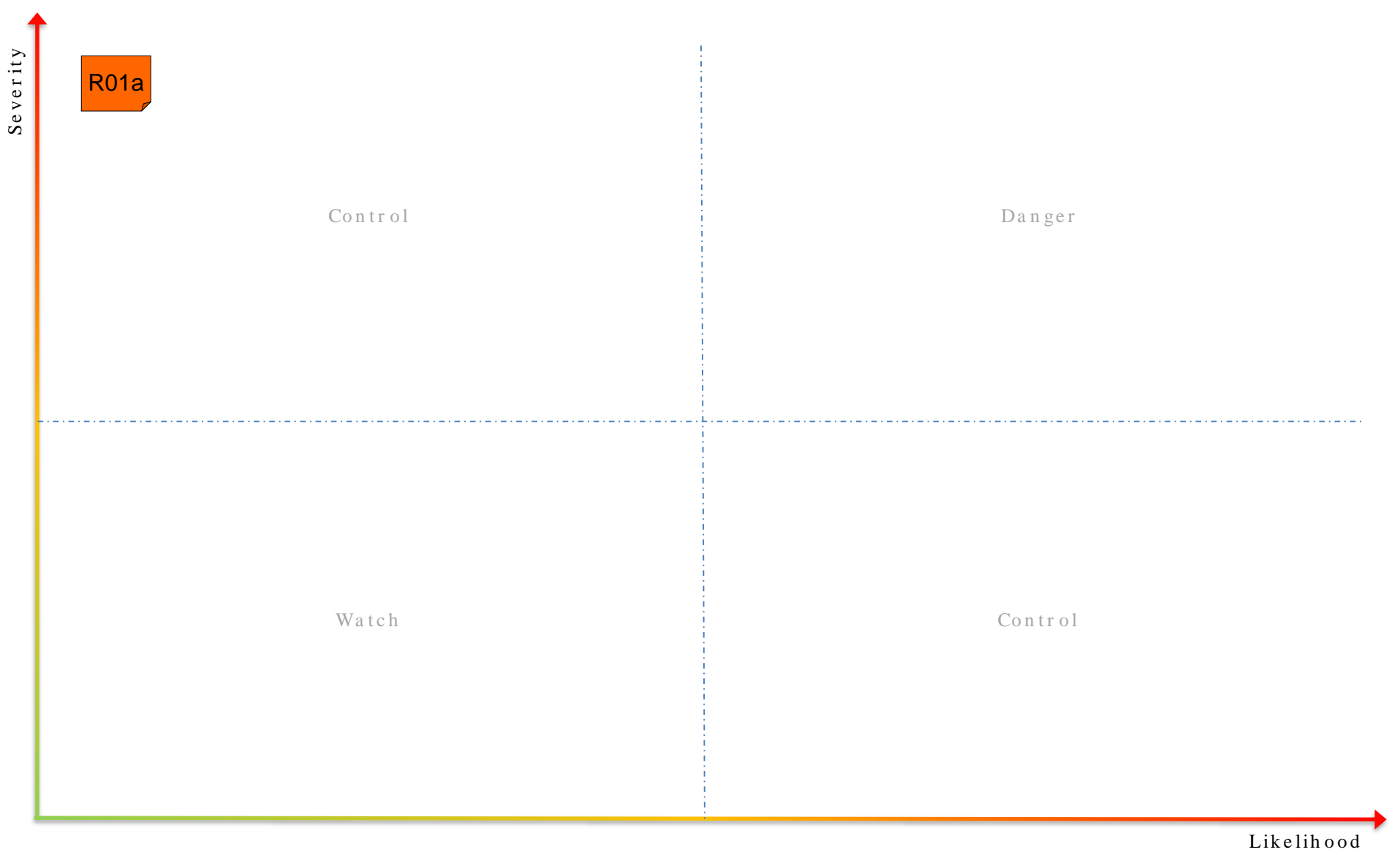
Synthesis of inherent / initial risks

1



Synthesis of residual risks

3



Security objectives

(i.e., ISO risk treatment options)

Risk retention / acceptance:

Risk modification:

Risk avoidance:

Risk sharing:

R01a Hide software and versions of software in use Regular security maintenance

Awareness training on phishing techniques Elevation of privileges log monitoring

Limitation of authentication trials Strong password policy

Use FTPS with HeberWeb Forbid FTP connections

External media verification procedure White-station to test media

- The objective of this study is a risk assessment to support the accreditation of the Digital Identity Document (DID) renewal system.
- Seven business assets have been identified. Of most importance, the printing and distribution of the DIDs, which need to be of-integrity, and the citizen data and the DIDs themselves, which need to be confidential. The violation of the security needs on these assets may lead to fraud and impersonation, of critical severity. Then come the management of the renewal requests, the DID ready notification service and the management of the pre-requests. All these functions need to be available, ranging respectively from high availability to best effort. The violation of the security needs on these assets may lead to significant up to serious consequences, including delays, investigation costs and the activation of back-up solutions. Finally, there are also some privacy concerns related to the citizen data.
- Our hypothesis is that the sole role of the DID Management Company (DIDMC) is to renew DIDs. With that hypothesis, the following three DIDMC IT systems make up the core of the system-under-study: the office automation IT system, the pre-request management IT system, and the production / printing IT system. In addition, we can make the hypothesis that DIDMC provided the DID renewal software, which is hosted at HeberWeb, and accessed via internet by the town hall employees. Beyond the IT supporting assets, it is possible to identify the DIDMC employees and the DIDMC premises as human and infrastructural supporting assets.
- The audits performed on HeberWeb, the Technical Administration Company (TAC), the town halls and DIDMC showed that a number of security measures are already in place, but that there are significant residual vulnerabilities, mainly related to improper security policies, poor configuration and some obsolete technical solutions (e.g., FTP, SSL v3.0).
- Three risk sources have a high likelihood of attacking the system-under-study: a criminal organisation may see a lucrative opportunity (R01), a foreign state may want to provide false DIDs for its spies (R03) and an hacktivist may want to disrupt the manufacturing of DIDs for ideological reasons (R02). We have also retained a disgruntled employee as potential risk origin due to the high privileges that this insider has on the system (R04).
- The interconnections of the system-under-study are quite numerous, directly with the citizens and HeberWeb, and indirectly with the town halls and the TAC. The analysis of the ecosystem shows that the TAC is in the danger zone, essentially due to poor equipment security maintenance and configuration. All the other interested parties are in the control zone, with a particular concern for HeberWeb, essentially due to poor end-of-life management of the IT equipment.
- We assume that the criminal organisation or the foreign state may attack the system-under-study directly (R01a, R03a) or it may proceed via the town hall (R01b, R03b), or via HeberWeb (R01c, R03c). By contrast, we assume that the hacktivist would rather attack via the town halls (R02a), whilst of course, the insider would only attack the system directly (R04a). Considering these strategic scenarios, it is recommended to apply all of the audit recommendations. The corrections suggested in the audits should significantly improve the cybersecurity status of TAC, HeberWeb and the town halls.
- The analysis of the criminal organisation direct attack path (R01a) shows that the DIDMC is vulnerable to phishing, malware on mobile media, and, in a lesser measure, to corruption. It was assessed likely that malware could leverage the poor security maintenance practices to exploit some software vulnerability, thus allowing the criminal organisation to gain privileges and egress sensitive data. Many low-cost security measures were proposed to modify the risk, including awareness training, improved maintenance and better security policies. With these measures, R01a should become rather unlikely.
- ...