

Best Risk Management Practices to Enforce a Strong Cyber Resilience

Jeff Primus

Principle Advisor & Accredited Trainer



- Implementer & Auditor for the ISO compliant Management Systems
  - in Governance, Cyber Security, Risk & Business Continuity
  - for the public sector and multinational companies in Switzerland, Europe and the Middle-East.
- Official & Accredited ISACA and PECB trainer since more than 20 years

ISO/IEC 27001 ISO/IEC 27005 ISO 31000 ISO 22301 ISO/IEC 20000 ISO 9001



- Former member of ISO SC27 Workgroup : defining the releases of the ISO/IEC 27001
- Lead lecturer at Sorbonne-Paris-1 & Switzerland Universities
- Performer as subject matter expert on radio and television shows.
- Former Board member of ISACA Switzerland

https://ch.linkedin.com/in/jeffprimus https://www.linkedin.com/company/actagis

© ACTAGIS Sarl – Ch. de la Résidence 3 – 1009 Pully – Switzerland
+41 21 353 03 30 www.actagis.ch team@actagis.ch

ACTAGIS – Consulting & Training Services



Logos used in this slide are licensed to ISC2 and ISACA

Cyber Resilience Steps



Cyber Security 2025 Landscape



- **Ransomware** – **91% of incurred losses** in H1 2025
  - (Axios, Sep 2025)
- **Infostealers** – **180% weekly increase** early 2025
  - (IBM X-Force 2025)
- **AI-driven phishing** – **+1,265%, 40% of email threats**
  - (SentinelOne, 2025)
- **India preparedness** – **Only 7% of orgs ready**
  - (Economic Times India, Mar 2025)
- **Major ransomware** (St. Paul) – **43 GB stolen, city systems shut down**
  - (Wikipedia, 2025)
- **Legacy vulnerabilities** – **32% of attacks exploit unpatched software**
  - (arXiv, May 2025)
- **Threat volume** – Amazon detects **750M threats/day (vs 100M months earlier)**
  - (WSJ, 2025)



Cyber Resiliance 2025 Landscape



- **Paul Ransomware Attack (July 2025, USA)**
  - Attackers (Interlock RaaS group) shut down city systems, blocking access to permits, billing, and police systems.
  - 43 GB of stolen data leaked after ransom refusal.
  - Business interruption: residents and companies couldn't access city services for days, forcing manual workarounds.
  - (Source: Wikipedia)



- **Change Healthcare Breach (Feb 2024, USA)**
  - A ransomware attack crippled one of the largest healthcare payment processors in the U.S.
  - Led to weeks-long outages in claims processing and pharmacy systems.
  - Financial disruption: over $1.6 billion in losses for hospitals and clinics due to interrupted revenue flow.
  - (Source: The Wall Street Journal)

Business Continuity Management Landscape



- **Lack of** historical **synergies** between ***BCM & CSRM frameworks***
  - But things are changing because of the rise of cyber threats
- The **synergies** are **essential** to implement an efficient BCM
- So, how can we enable the synergies between existing **frameworks ?**

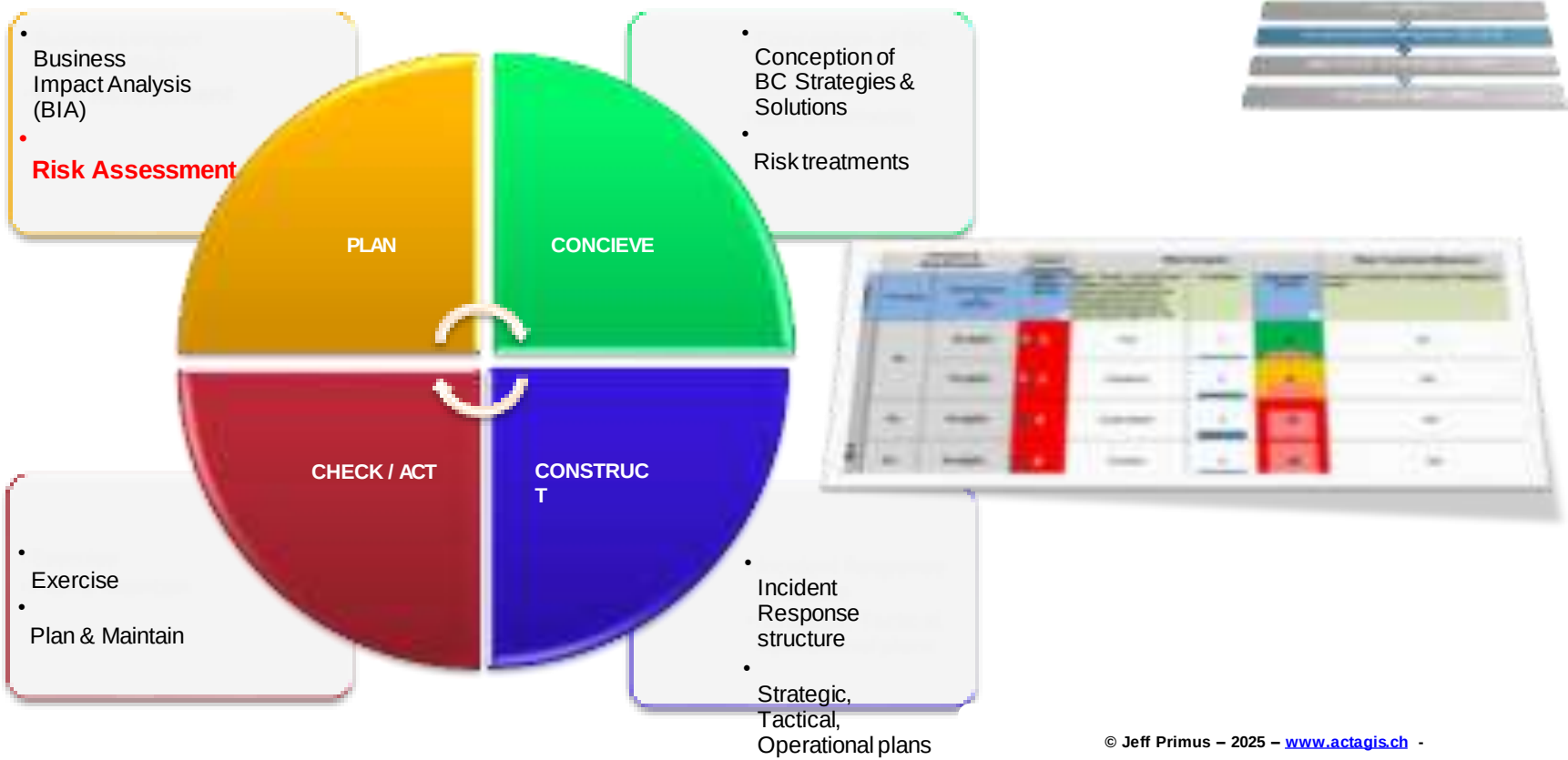


Business spans across multiple layers



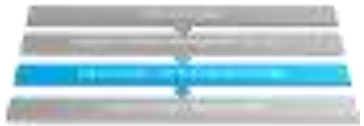
© Jeff Primus – 2025 – www.actagis.ch

Business Continuity
ISO 22301



© Jeff Primus – 2025 – www.actagis.ch -

Cyber Security Fundamentals
Requirements



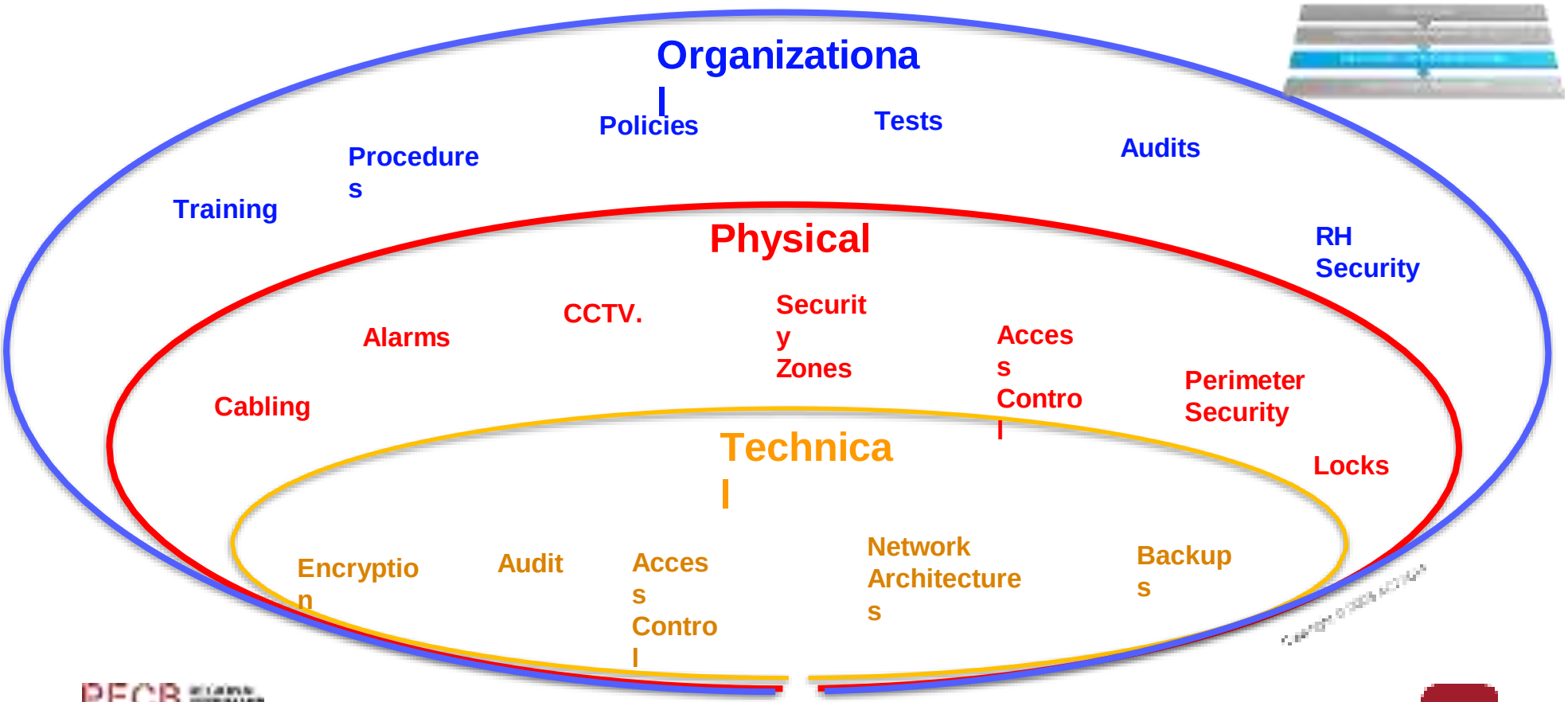
- Cyber Security concerns all information assets of the organization



Copyright © 2025 ACTAGIS

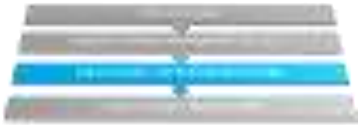
Cyber Security Fundamentals

Types of Measures



Cyber Security Risk Management (**CSRM**)

Terms

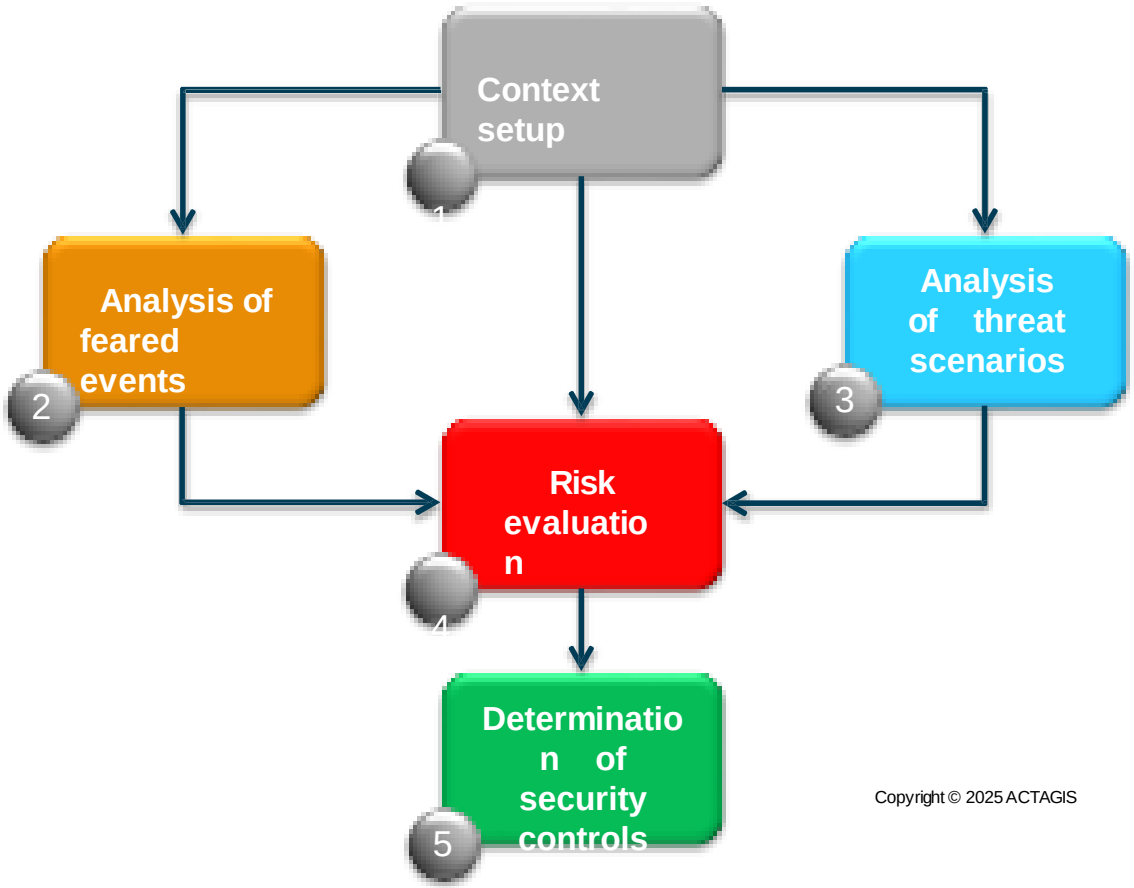


Term	Definition	Examples
Primary assets	**Information or processes** deemed **important** by the organization.	• Clients management • Payment process
Support assets	**Assets supporting primary assets**. We distinguish particularly computer systems and local organizations.	• ERP software • Servers and virtual machines • Buildings
Source of threats	Thing or person **at the origin of the threat**.	• Malicious collaborator with important knowledge and opportunities towards the information system
Feared events	**Generic event linked to a given impact level,** representing something that is feared by the organization.	• Corruption or alteration of customer management primary assets • Unavailability of payment management primary assets
Threat scenarios	**Scenario linked to a likelihood level,** describing a specific operating method	• Confidentiality breach on the ERP system

Copyright © 2025 ACTAGIS

Cyber Security Risk Management (**CSRM**)

ISO 27005 - Phases



Copyright © 2025 ACTAGIS

CSR M

Context setup - Assets

- Identifying Primary Assets (PA) and Supporting Assets (SA)



P1



P2

Primary Assets (PA)

Information assets or «intangible assets» that we want to protect

These may be activities or key processes for instance

Non-compliance of a PA with the security objectives (C, I, A, etc..) would cause harm to the company or to third parties

→ «**Severity**» oriented vision

Supporting Assets (SA)

- Information System Components (technical or non-technical assets)
- Support for the identified PA
- SA have **vulnerabilities** exploitable by threats, thus undermining PA's

→ «**Likelihood**» oriented vision



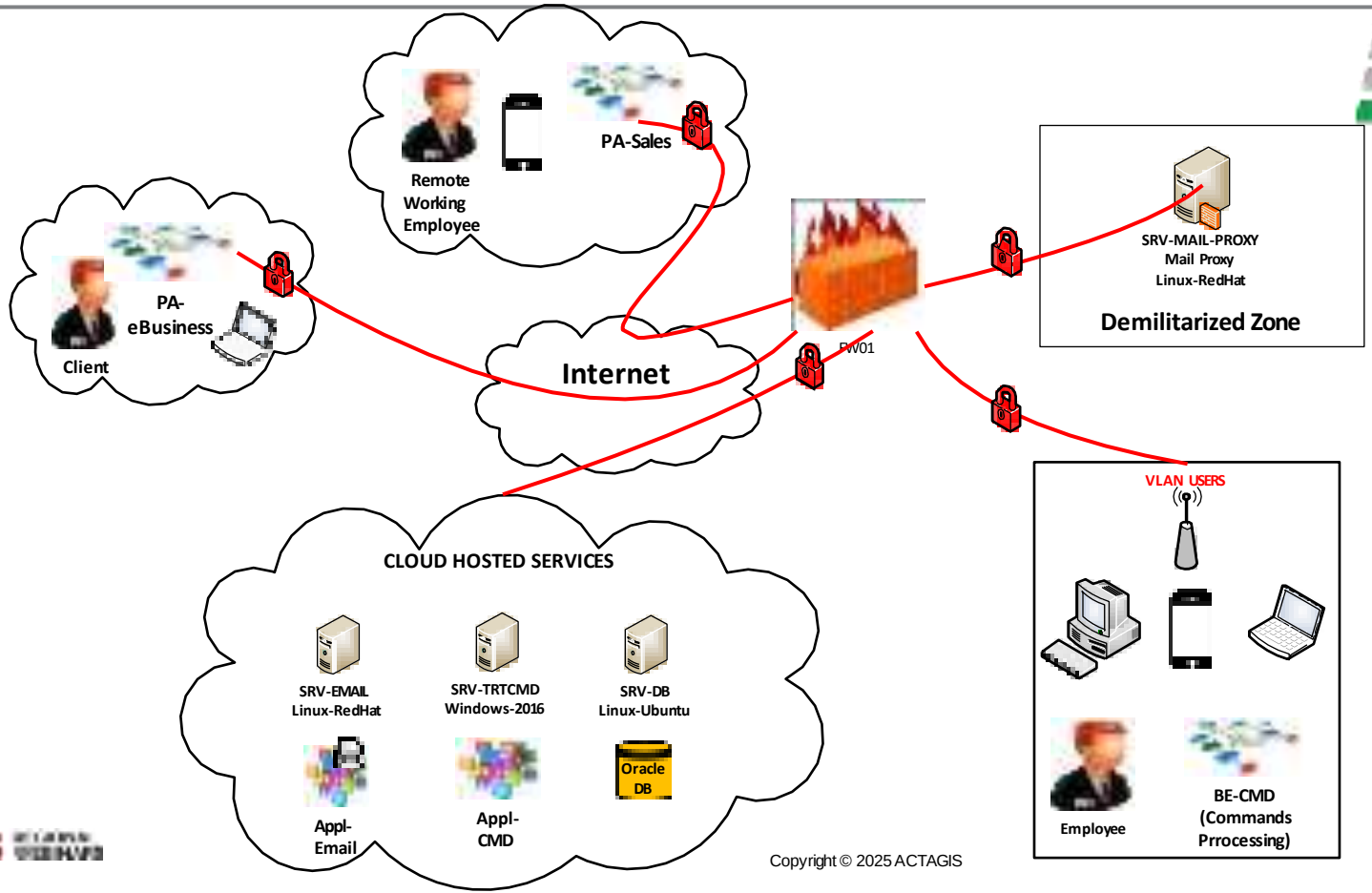




Copyright © 2025 ACTAGIS

CSRM

Context setup - Architecture



Copyright © 2025 ACTAGIS

CSRM
Context setup - Threats

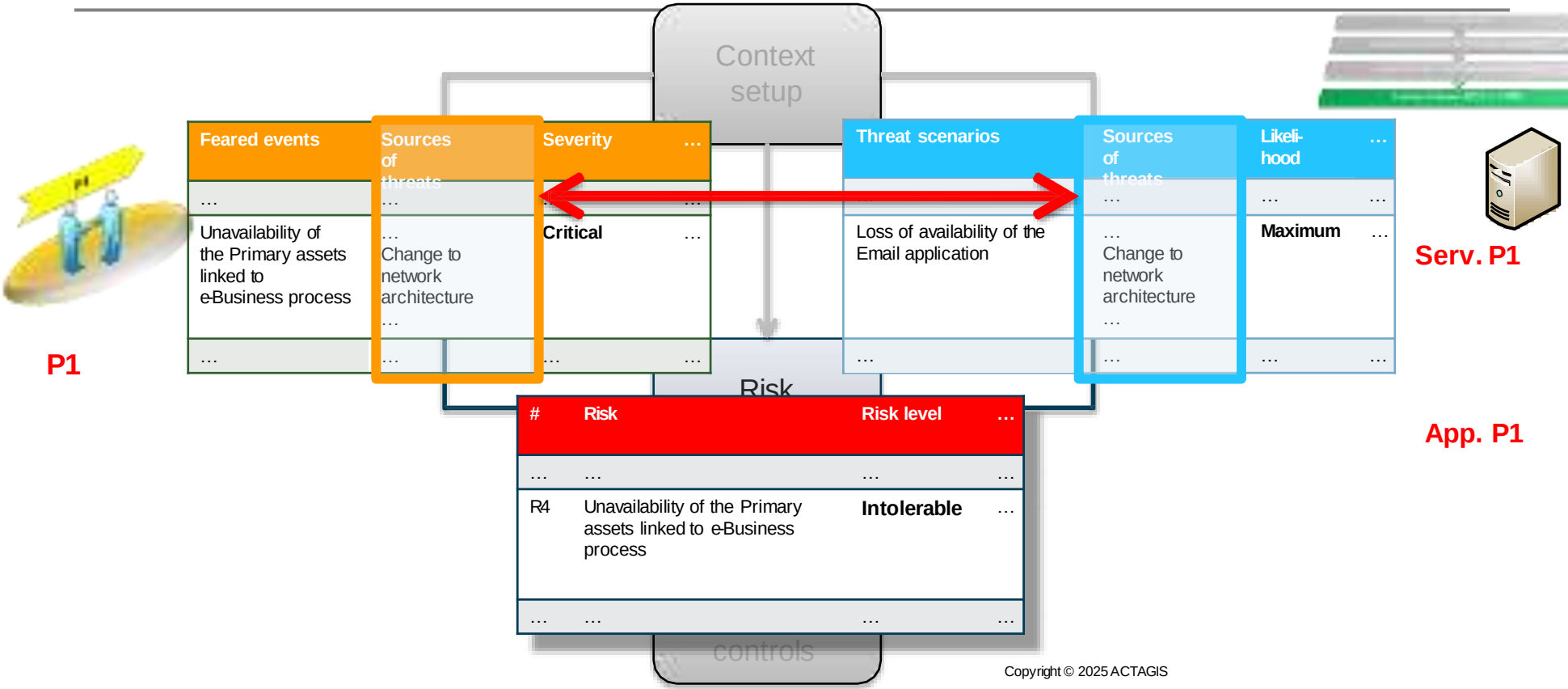
- Extract of a source of threats table

#	Threat source categories	Applicable ?	Examples of occurrence
Human sources acting deliberately			
1	Human source, internal, malevolent, with limited resources	yes	1. Disgruntled fired employee or willing to take revenge on the employer or his/her colleagues
2	Human source, internal, malevolent, with important resources	yes	1. Fired manager willing to take revenge on the employer or his/her colleagues 2. Developer acting for fun or to satisfy his/her ego
3	Human source, internal, malevolent, with unlimited resources	yes	1. System administrator
4	Human source, external, malevolent, with limited resources	yes	1. Act of vandalism 2. Script-kiddie
5	Human source, external, malevolent, with important resources	yes	1. Person politically engaged acting for ideological or political reasons, committed hacker
…	…	…	• …

Copyright © 2025 ACTAGIS

CSRM

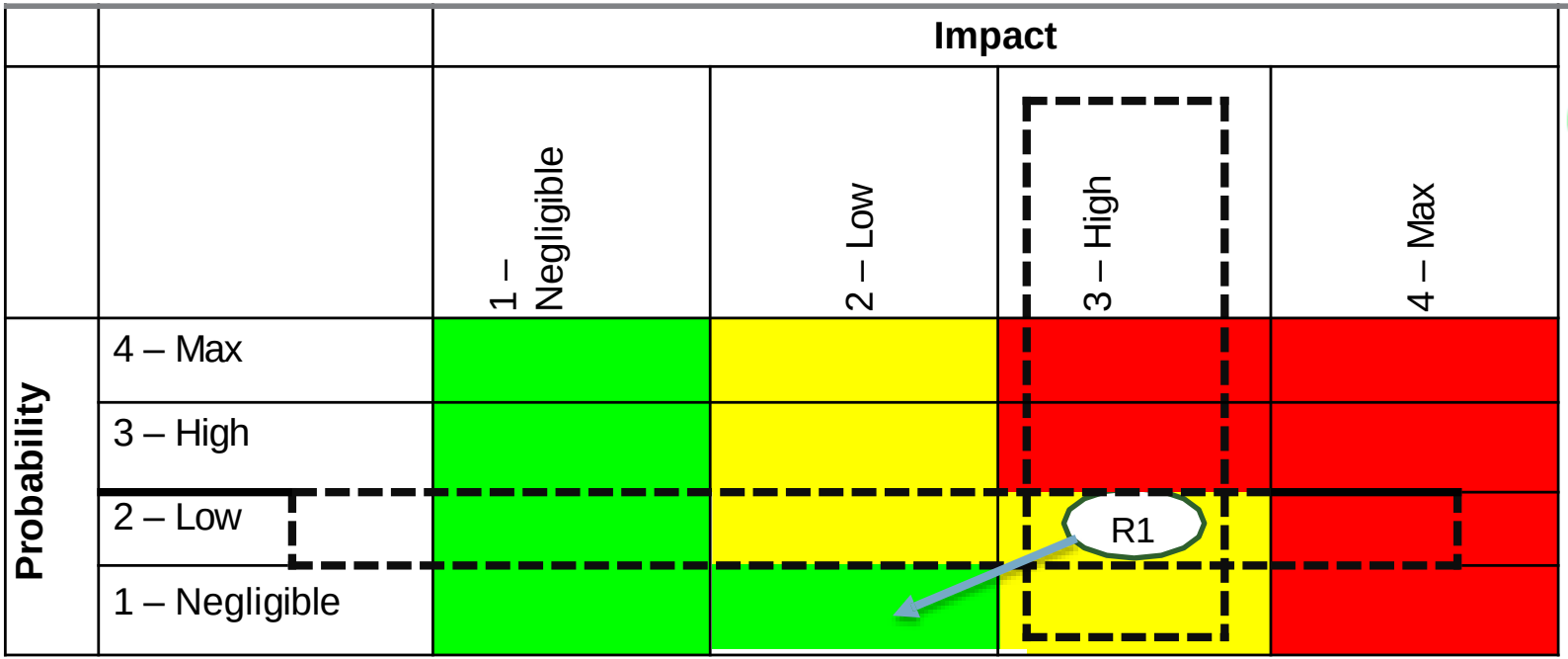
Risk evaluation - Example



Copyright © 2025 ACTAGIS

CSRM

Risk evaluation - Example



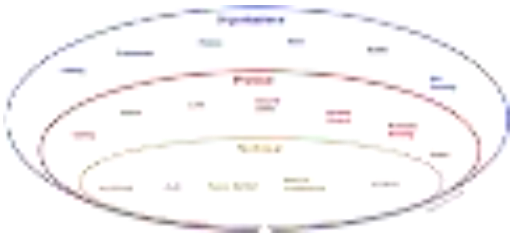
Acceptable risks: Can be ignored	Significant risks: To be monitored	Intolerable risks: To be reduced

Copyright © 2025 ACTAGIS

CSR
Selection of security controls
M

- **Organizational**
  - Access control Policy
- **Technical**
  - Network hardening
  - System hardening
  - Secure Development Lifecycle
- **Examples**
  - **N-factor authentication**
  - **Encryption of data transfer**





Copyright © 2025 ACTAGIS

Q&A Session



Do you have questions

We can help you !

Scan the QR code to get in touch for further advice

© ACTAGIS Sàrl – Ch. de la Résidence 3 – 1009 Pully – Switzerland
+41 21 353 03 30 www.actagis.ch team@actagis.ch

All the content and the images in this presentation are licensed to / owned by ACTAGIS unless otherwise stated
(and the PECB logo and the 1st slide's background image provided by PECB)