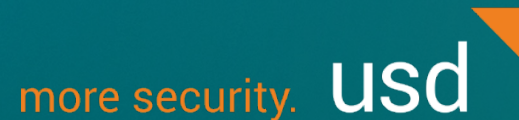


# How PCI DSS Can Help You Secure Your Critical Infrastructure

Christopher Kristes, Executive Board Member, usd AG  
Vinzent Ratermann, Managing Consultant, usd AG



# Agenda



## Our Central Questions for Today

How is critical infrastructure **protected in the EU**



What **challenges** are we facing



How can **PCI DSS** support you



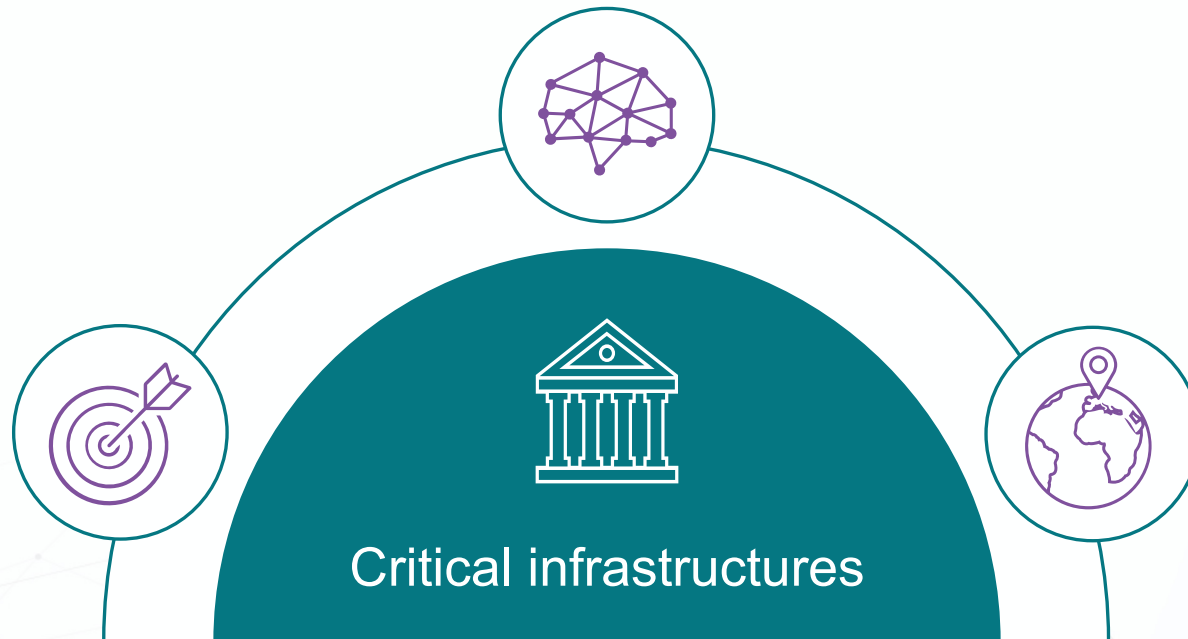
Worldline Case Study



# Critical Infrastructure Protection is Vital

Due to the high value of the target, attackers use very complex and elaborate attacks.

Particularly affected by digital threats.



Global political flashpoints are fueling the threat.

*"... are entities of importance for the state community whose failure would result in lasting supply bottlenecks, significant disruptions to public safety or other dramatic consequences."*

# Regulation in the EU

## EU NIS2

*Directive on Security of Network and Information Systems*

Goal: Regulates the information security of critical services to **reduce the impact of cyber attacks** and incidents to IT systems and networks.

Measures: Demands cyber security of company including:  
**policies and governance | incident and continuity management  
IT security in the supply chain | IT audits and tests | cryptography**

IT-Sicherheitsgesetz (2.0) /  
IT Security Act

German regulation

Piano nazionale per la  
protezione cibernetica e la  
sicurezza informatica

Italian regulation

Other member states  
regulations based on NIS2

Member states regulation

# What to Protect



Water

Nutrition



Health

Waste Management



## Finance and Insurance

Authorization

Clearing / Settlement

ATM

POS Terminal Operator

...



Transport & Traffic

IT & Telecom



Energy

SPIE



# Concept: Security Baseline (1/2)



## The Security Standard for Critical Infrastructure Assessments

*“... Critical Infrastructures must implement **adequate organizational and technical measures** to reduce the possibility of incidents to the availability, integrity, authenticity and confidentiality of the systems of the information technology ...”*

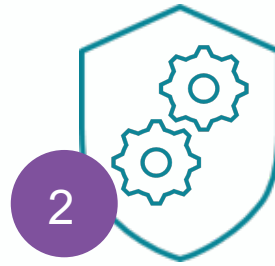
German Regulation (§8a BSI Law)

# Concept: Security Baseline (2/2)



Sector-Specific Security  
Standard (B3S)

defined by experts  
per sector



ISO 27001  
(BSI Grundschutz)

in combination with adequate  
sector-specific requirements



ISO 27001  
(BSI Grundschutz)

might also be acceptable  
standalone

# Example: Sector Finance and Insurance



## B3S Electronic Cash Network Operators



Scope



Requirements

### Critical Service

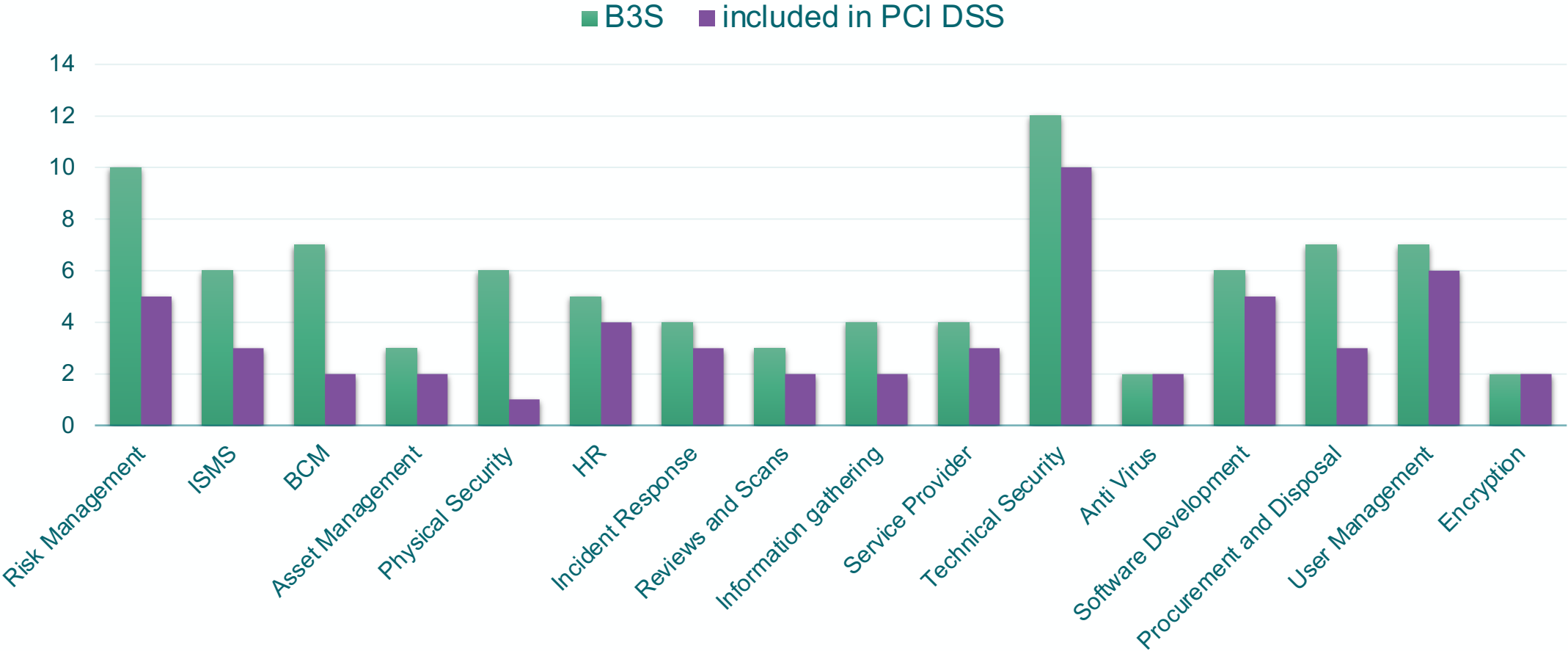
Systems that receive card data from POS terminals and systems that process that data.

### PCI DSS

The core systems are the same if credit card payments are allowed.

B3S relies heavily on PCI DSS 3.2.1, but only for the PCI DSS scope.

# B3S Electronic Cash Network Operators vs. PCI DSS



# Case Study

## Worldline Germany GmbH



# Case Study: Assessment Approach



Scoping



PCI DSS  
Assessment



Critical Infrastructure  
Assessment



Reporting

# Case Study: Scoping

Define the Scope for PCI DSS and the Critical Service



Scoping

## Critical Infrastructure Scope



### PCI DSS Scope

- Cardholder Data Environment
- Connected To Systems
- Security Impacting Systems



### Non-PCI DSS Scope

- Additional systems of the critical infrastructure  
e.g. systems working with tokens
- Management Systems



# Case Study: Assessment



## PCI DSS Assessment Followed by the Critical Infrastructure Assessment

Perform PCI DSS testing for PCI DSS compliance

Verify that all non-compliances are remediated



Perform KRITIS testing in PCI DSS scope

Perform KRITIS testing and PCI DSS testing in non-PCI DSS scope

# Case Study: Reporting



## Write and Submit Reports



PCI DSS Scope

Report on Compliance

Attestation on Compliance



Critical Infrastructure

Assessment Report

List of non-Compliances

4



Reporting

# Key Take-Aways

## PCI DSS Can Help You Secure Your Critical Infrastructure



Securing critical infrastructure will be one of the major IT security issues for the next years.



PCI DSS overlaps with sector-specific security standards or can even be a baseline by itself.



Advantages for the PCI DSS and critical infrastructure assessment due to synergy effects between both scopes and the clarity of DSS requirements.



Use PCI DSS not only in the credit card environment.