

Introduction: Group Information Security

May 7th 2025 | Mauro Pianezzola - Volkswagen Group Information Security Management

Disclaimer

The following presentations as well as remarks/comments and explanations in this context contain forward-looking statements on the business development of the Volkswagen Group. These statements are based on assumptions relating to the development of the economic, political and legal environment in individual countries, economic regions and markets, and in particular for the automotive industry, which we have made on the basis of the information available to us and which we consider to be realistic at the time of going to press. The estimates given entail a degree of risk, and actual developments may differ from those forecast.

All figures are rounded, so minor discrepancies may arise from addition of these amounts.

Any changes in significant parameters relating to our key sales markets, or any significant shifts in exchange rates, energy and other commodities or the supply with parts relevant to the Volkswagen Group will have a corresponding effect on the development of our business. In addition, there may also be departures from our expected business development if the assessments of the factors influencing sustainable value enhancement and of risks and opportunities presented develop in a way other than we are currently expecting, or if additional risks and opportunities or other factors emerge that affect the development of our business.

We do not update forward-looking statements retrospectively. Such statements are valid on the date of publication and can be superseded.

This information does not constitute an offer to exchange or sell or an offer to exchange or buy any securities.

Agenda : Group Information Security

- 1 Our Challenge
- 2 The Group Information Security
- 3 ISMS / UNECE / CSMS

1. Our Challenge

Constantly new threat situations and increasingly aggressive approaches

APPROXIMATELY
394,000 NEW VARIANTS
OF VIRUSES, TROJANS
AND MALWARE
WORLDWIDE EVERY
DAY

APPROX. 36 BILLION
PHISHING E-MAILS PER
YEAR WORLDWIDE

>100 BILLION EUROS IN
DAMAGE P.A. IN
GERMANY

86% OF GERMAN
COMPANIES ARE
VICTIMS OF
CYBERCRIME

PASSWORDS CRACKED
WITHIN SECONDS

TARGETING DATA OF
ALL KINDS: FINANCIAL,
EMPLOYEE AND
CUSTOMER DATA

THE HUMAN FACTOR IS
A GATEWAY FOR
ATTACKS

RECREATIONAL
HACKERS ARE
BECOMING WELL-
EQUIPPED CYBER
GANGS

2. The Group Information Security

Projects & Fields of Action

**INDUSTRIAL
CYBER SECURITY (ICS)**

**SECURITY TOOLS &
PROCESSES**

CSMS

**IDENTITY & ACCESS
MANAGEMENT**

**VEHICLE SECURITY
OPERATIONS CENTER
(V-SOC)**

**INFORMATION
SECURITY SPECIALIST &
EXPERT CONFERENCE
(IS-SEC)**

**COMPUTER
EMERGENCYRESPONSE
TEAM
(CERT)**

**INFORMATION
SECURITY
MANAGEMENT SYSTEM
(ISMS)**

**INFORMATION
SECURITY
ASSESSMENTS**

**PKI
SERVICES**

...

**SICHER IST
+BESSER***
(*BETTER SAFE THAN SORRY)

The Group Information Security

Safely into the digital future with us.



The GISSC

Group Information Security Steering Committee

The highest corporate information security body

- Strategic Committee, implementation via GISP¹⁾
- All brands and regions represented
- Voting rights only if involved
- Six regular meetings per year



1) Group Information Security Program

Group Information Security Program

GISP

The program develops **business- and process-driven solutions** for new and growing business needs, **ensures synergies** as well as **Group-wide processes** and **standards** to increase the level of security maturity throughout the Group. The design of the program is based on the **information security strategy** adopted jointly with all brands and regions. GISP is divided into **5 clusters** and comprises about **50 projects**.



GISSC
ALIGNED
PROTECTION



AUTHENTICATION
&
SECURITY
SOLUTIONS



GOVERNANCE
&
COMMUNICATION



IAM
SOLUTIONS



CSMS
GOV & OPS



3. Information Security Management System (ISMS) within Volkswagen AG

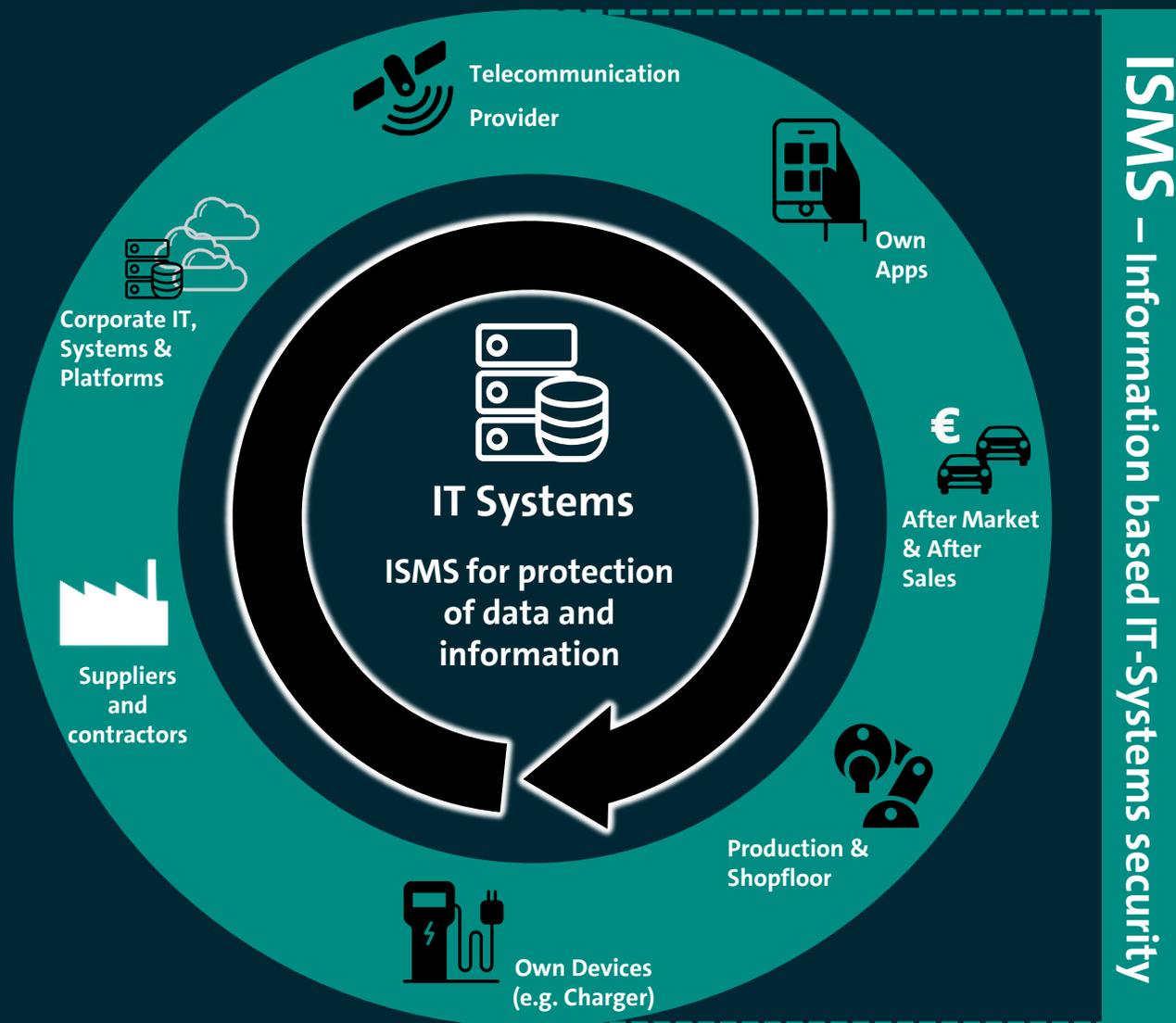
Responsibility through "Group Information Security" within Group and organizational policy

the ISMS has been defined and expanded by the Information Security Group .

Governance processes of the ISMS are ISO 27001 certified



VW IT Services is TISAX certified



Interface to UNECE Cyber Security Management System (CSMS)

Additional risk-assessment for IT-Systems within „Digital Ecosystem of Vehicle“ required

Cyber Security Management System

Threat analysis and risk-assessment

- Which kind of threat is the vehicle facing?
- What is the **gross risk** of it?

New Damage- and risk-evaluation

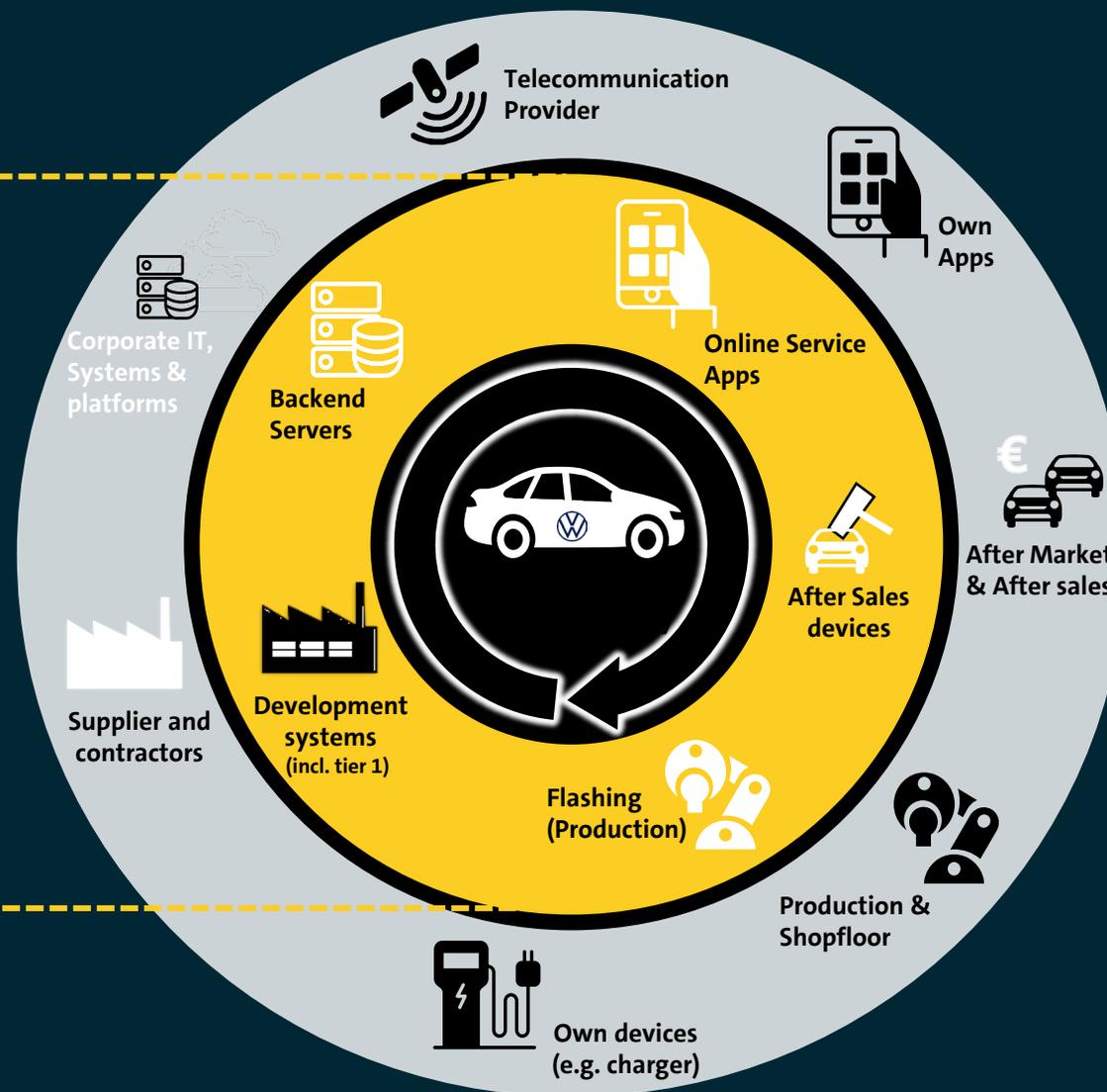
- Concerning already existing risks, what is the **net risk**?
- What kind of damage?
- Is it Safety-Relevant?

Mitigation and implementation of issues:

- Which issues mitigate the risk?
- Where to implement them?
- What is the timeline of implementation?
- Are there some risks left?

CSMS

On top cyber security for vehicle-relevant IT-Systems



ISMS – Information based IT-Systems security

Glossary

CERT	Computer Emergency Response Team
CSMS	Cyber Security Management System
CSMS Gov & Ops	CSMS Governance & Security Operations
GISP	Group Information Security Program
GISSC	Group Information Security Steering Committee
IAM	Identity and Access Management
ICS	Industrial Cyber Security
ISMS	Information Security Management System
ISO 27000	Information security standard - specifies the requirements for managing and improving ISMS
PKI	Public key infrastructure
TISAX	Trusted Information Security Assessment Exchange
UNECE	United Nations Economic Commission for Europe
SAM	South America
NAR	North America
APAC / ME	Asia and Pacific / Middle East