



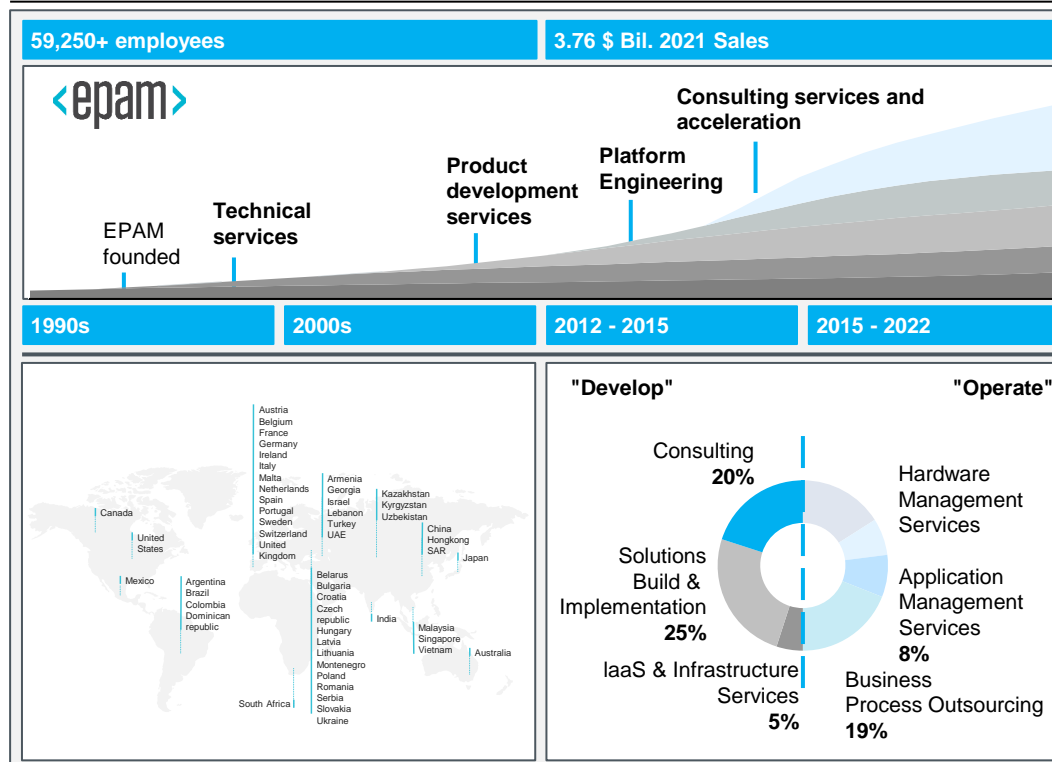
EU Cyber Regulation

CLDP - Central Asia Digital Trade & Cybersecurity
Conference

Almaty, 28/29 March 2023

Overview of EPAM facts and figures – 2022

Overview of the advantages of EPAM



EPAM results for 2022 incl. year-on-year comparisons

| | | | |
|---|---|---|--------------------------------------|
| Net sales, in million | | Outlook FY 2023, in million | |
| Sales \$4.825B +32.4% ↗ | | Sales in the range of \$5.250B +9% ↗ | |
| Sales by vertical industries, in million | | | |
| Travel & Consumer \$1.09B +47.4% ↗ | Financial Services \$1.03B +21.0% ↗ | Business Information & Media \$810M +21.4% ↗ | |
| Software & Hi-Tech \$793M +19.4% ↗ | Life Sciences & Healthcare \$507M +29.7% ↗ | Emerging \$595M +33.5% ↗ | |
| Sales by geography, in million | | | |
| AMERS ¹ \$2.89B 29.7% ↗ | EMEA ² \$1.74B +38.0% ↗ | APAC ³ \$120M +16.2% ↗ | CEE ⁴ \$79M -52.9% ↘ |
| Diluted earnings per share | | | |
| Gaap EPS ⁵ \$7.09 -13.0% ↘ | | Non-Gaap EPS \$10.90 +20.4% ↗ | |
| Employees & Locations | | | |
| 52,850+ Designers, Developer & Consultants | | 50+ Countries & Regions | |

Source: CORE | 1: AMERS = Americas, 2: EMEA = Europe, Middle East und Africa, 3: APAC = Asia Pacific, 4: CEE = Central East Asia, 5: EPS = Earnings per Share

EPAM is a strong, trusted partner for multinational enterprises and high-tech companies across many industries with Digital Product and Platform Engineering DNA

SELECTION OF PAST PROJECTS

| Financial Services | Business information & media | Retail & distribution | Life sciences & healthcare | Travel & Hospitality | Energy & utilities | Manufacturing & automotive | Insurance | |
|-----------------------------------|------------------------------|------------------------------|----------------------------|--------------------------|--------------------|----------------------------|------------------|--|
| REFINITIV | | | | | | | | |
| Born-digital Companies | | | | | | | | |
| Software companies | | | | Our purpose is people | | | | |
| | | | Be Limitless. | | | INNOVATION UNLEASHED | | |
| | | | | | | | | |

Brief introduction Dr Waldemar Grudzien



Dr Waldemar Grudzien

CORE SE, Expert Partner

Information security, Data privacy, Financial Oversight Audits

Director in the Banking Association BdB (2001 – 2016)

PhD student, developer (1994 – 2001)

- **Founding member and head of the German blue chip CRITIS chapter (2008 - 2015)**
- **Co-author of German Cyber Sec Act, NIS Directive, PSD2 (RTS), BAIT**
- **Founding member of BaFin's "IT expert committee" in 2015**
- **Involved in ISO standards on biometrics and cryptography**
- **Chairman of the Bitkom Information Security Working Group since 05/21**

Legal acts of the EU digital legislation – Comparison

 following in depth

| Legal act | Name | In force/ applied since | Current Version | Draft Version | Main purposes | Affected | National Implementation | |
|-----------|------|--|---------------------------|------------------------------|----------------------------|--|---|-------------------------|
| 1 | GDPR | General Data Protection Act | 25.05.2016/ 25.05.2018 | 25.05.2016 | ... | Protection of individuals with regard to the processing of personal data | Person in charge, Processor | GDPR, BDSG, TTDSG, LDSG |
| 2 | DORA | Digital Operational Resilience Act | 17.01.2023/ 17.01.2025 | 14.12.2022 | ... | ICT risk management, ICT incident reporting, digital operational stability | Financial companies, Third-party ICT service provider | ... |
| 3 | CRA | Cyber Resilience Act | ... | ... | 16.09.2022 | Security of products with digital elements | Producers, importers, traders | ... |
| 4 | NIS | Network Information Security | 08.08.2016/ 29.06.2017 | <u>NIS 1.0</u> 08.08.2016 | <u>NIS 2</u> 16.12.2020 | Minimum level of protection and reporting of critical infrastructures | Critical infrastructures | IT-SIG 2.0 |
| 5 | AI | Artificial Intelligence Act | ... | ... | 21.04.2021 | Legal framework for artificial intelligence systems | AI systems | ... |
| 6 | CSA | Cyber Security Act 2019/881 | 27.06.2019/ 28.06.2022 | ... | 27.06.2019 | ... | ... | ... |
| 7 | CER | Directive on resilience of critical entities 2022/2557 | 17.01.2023 | 14.12.2022 | ... | ... | ... | ... |
| 8 | DSA | Digital Service Act | 16.11.2022/ 17.02.2024 | <u>19.10.2022</u> | 15.12.2020 | Uniform legal framework for the regulation of intermediary services | Intermediary services such as online platforms | ... |
| 9 | DMA | Digital Market Act | 01.11.2022/ 02.05.2023 | <u>14.09.2022</u> | 15.12.2020 | Regulation of dominant digital companies | Central online platforms | ... |

DORA (Digital Operational Resilience Act) entered into force on 16.01.2023 and becomes applicable on 17.01.2025

Transfer of national regulations into an overarching European legal framework

German Regulation

- I** Bank /
BAIT, MaRisk
- II** Payment-/E-money
institute
ZAIT, MaRisk
- III** Insurance company /
VAIT, MaGo
- IV** Investment firms /
BAIT, MaRisk
- V** Capital Management
Company /
KAIT, KAMaRisk

Content of the DORA

- 1** As a **new single EU regulatory framework**, DORA addresses **growing cyber risks** by **strengthening digital operational resilience in the financial sector**
- 2** DORA **combines** existing **regulations on security measures, reporting and verification of outsourcing** and **harmonises** them across Europe.
- 3** DORA addresses **20 types of financial companies and ICT third party service providers** (e.g. hyperscalers or corebanking providers) as suppliers to the financial industry and thus broadens monitoring frameworks to include
- 4** The EU Commission and the ESA want **DORA to replace national regulations, not to supplement** them.
- 5** **DORA requires** an Information Security Management System (**ISMS**) as well as **penetration tests** according to European standards (TIBER EU).
- 6** The financial industry will have to comply with **further reporting obligations and authorisation procedures**.

EU COM: 22,000 financial firms affected by DORA

BaFin supervisory objects New from DORA

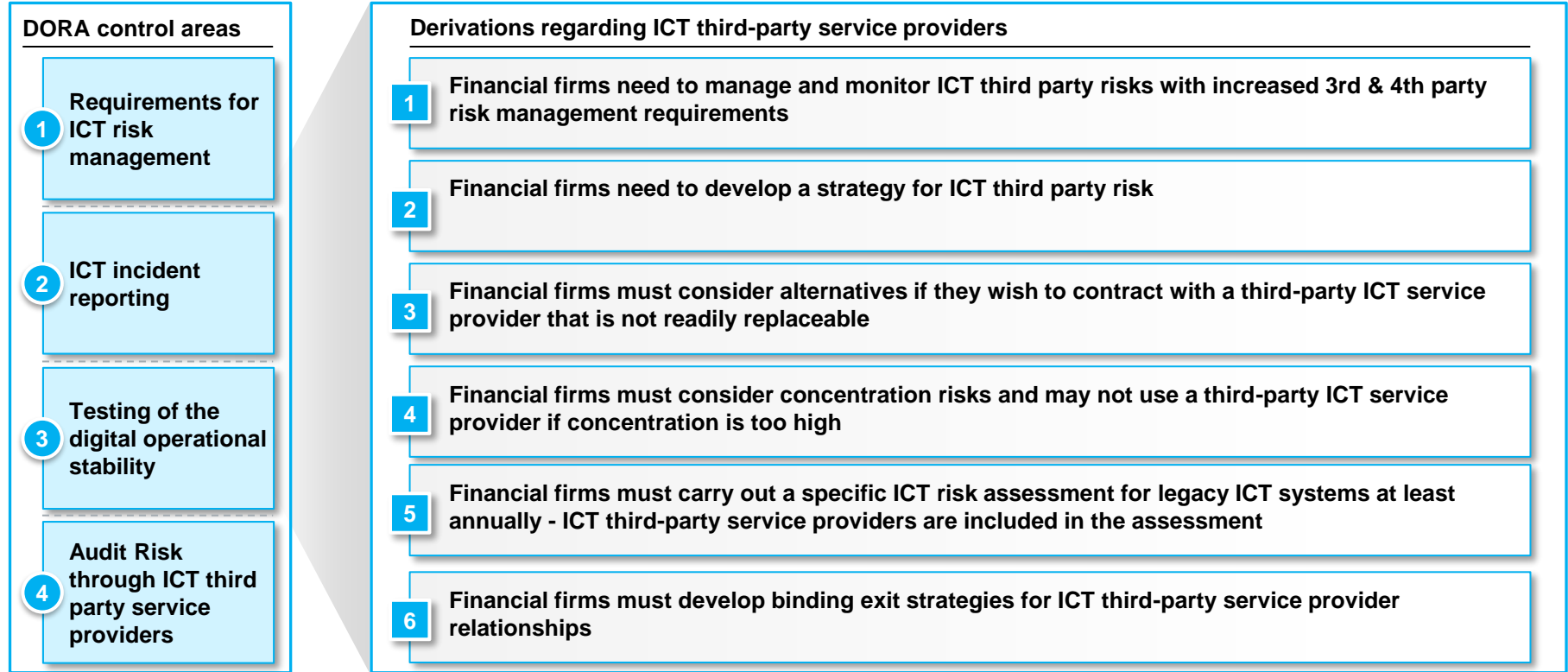
DORA extends BaFin/Bundesbank's supervisory framework to 20 types of financial companies and third-party ICT service providers



Quelle: CORE

DORA | Stand März 2023

Third-party ICT service providers to be supervised by financial supervisors as if they were a bank for the first time



DORA | Regulatory content Key topics

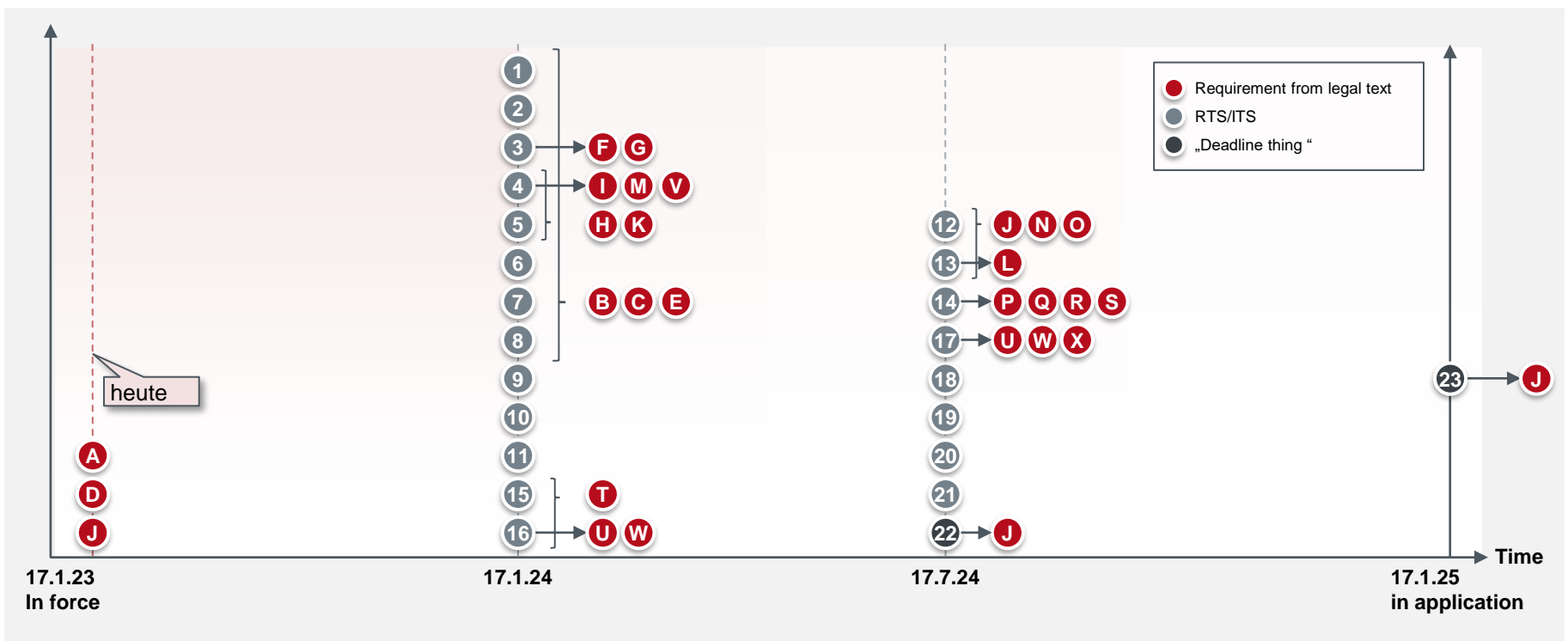
Regulatory content of the DORA in chapters, article groups and addressees

| Chapter | Description / Article | Addressees |
|----------------|---|--|
| 1 Chapter I | <ul style="list-style-type: none"> General provisions article 1 to article 4 | <ul style="list-style-type: none"> 19 types of financial companies + ICT third-party service providers; management body must have ICT expertise |
| 2 Chapter II | <ul style="list-style-type: none"> ICT risk management <ul style="list-style-type: none"> section I: article 5 section II article 6 to 16 | <ul style="list-style-type: none"> Financial company Management body must have ICT know-how |
| 3 Chapter III | <ul style="list-style-type: none"> ICT-related incident management, classification and reporting article 17 to 23 | <ul style="list-style-type: none"> Financial companies (17-19, 23), competent authority (20 - 22) |
| 4 Chapter IV | <ul style="list-style-type: none"> Digital operational resilience testing article 24 to 27 | <ul style="list-style-type: none"> Financial companies (24 - 26), Tester (27) |
| 5 Chapter V | <ul style="list-style-type: none"> Managing of ICT third-party risk article 28 to 30, section I: Key principles for a sound management of ICT third-party risk; article 31 to 44, section II: Oversight Framework of critical ICT third-party service providers | <ul style="list-style-type: none"> Financial companies und ICT third-party service provider |
| 6 Chapter VI | <ul style="list-style-type: none"> Information-sharing arrangements article 45 | <ul style="list-style-type: none"> Financial companies |
| 7 Chapter VII | <ul style="list-style-type: none"> Competent authorities article 46 to article 56 | <ul style="list-style-type: none"> ESA, competent authority |
| 8 Chapter VIII | <ul style="list-style-type: none"> Delegated acts article 57 | <ul style="list-style-type: none"> European Commission |
| 9 Chapter IX | <ul style="list-style-type: none"> Transitional and final provisions article 58, section I <ul style="list-style-type: none"> article 59 to 64, section II: Änderungen | <ul style="list-style-type: none"> European Commission, ESA, ESRB¹ |

¹ European Systemic Risk Board

Merging the requirements from the ordinance text and RTS/ITS across the timeline - work can be bundled together

Merging the requirements from the ordinance text and RTS/ITS across the timeline



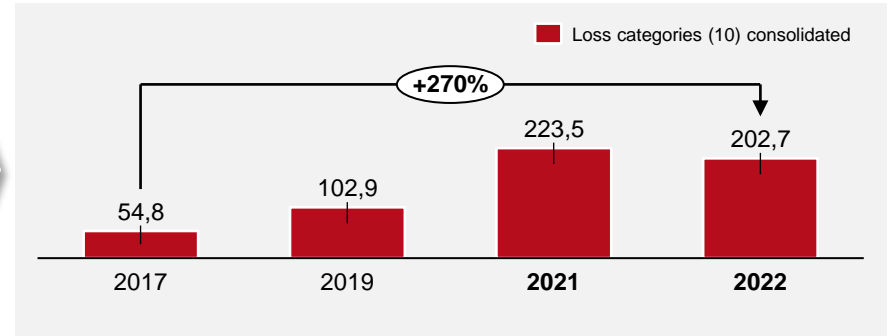
Quelle: CORE 2023

Cyber Resilience Act pursues four specific objectives

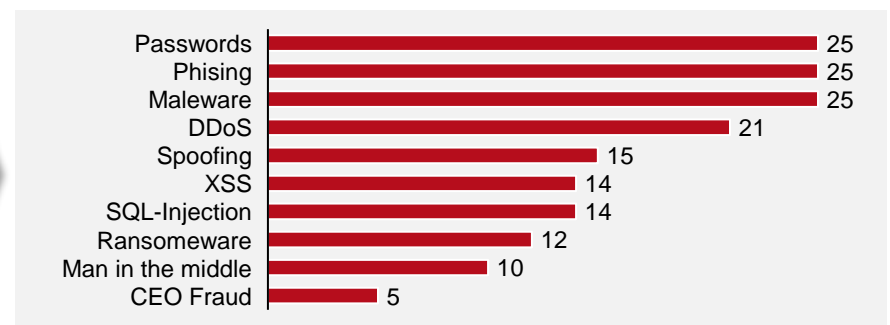
Four goals counteract damage from cyberattacks

| | | |
|---|---|--|
| 1 | Product safety in the life cycle | Ensure that manufacturers improve the safety of products with digital elements from the design and development phase and throughout the life cycle |
| 2 | Cyber security framework | Ensure a coherent cybersecurity framework that facilitates compliance for hardware and software manufacturers |
| 3 | Transparency | Increasing the transparency of the security features of products with digital elements; and |
| 4 | Safe use | Empowering businesses and consumers to use products with digital elements safely. |

Damage in EUR billion (incl. theft, espionage, sabotage)



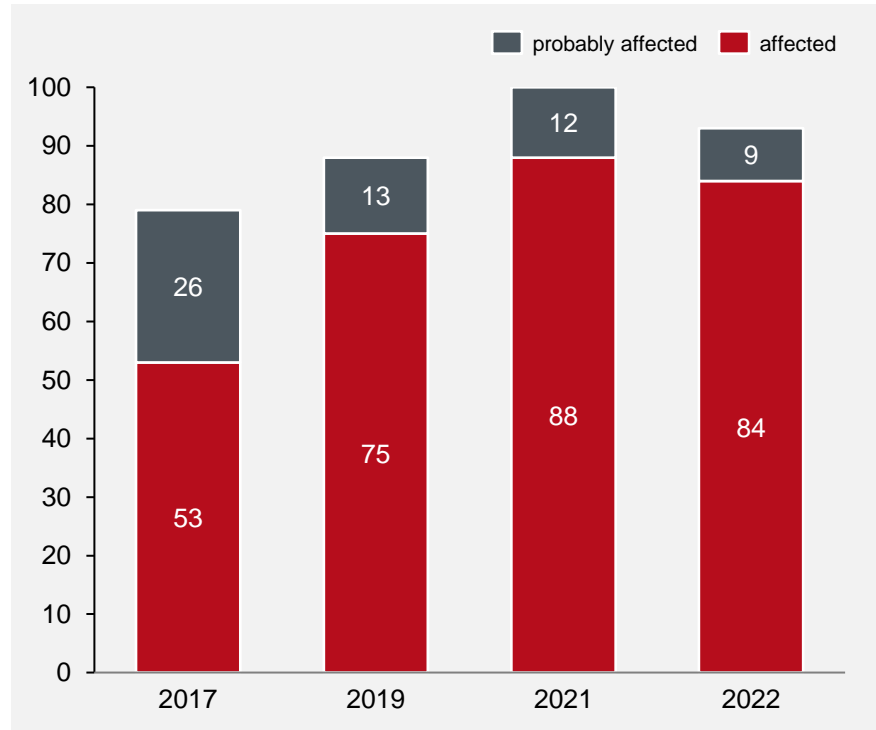
Types of damage from cyber attacks¹ (in %)



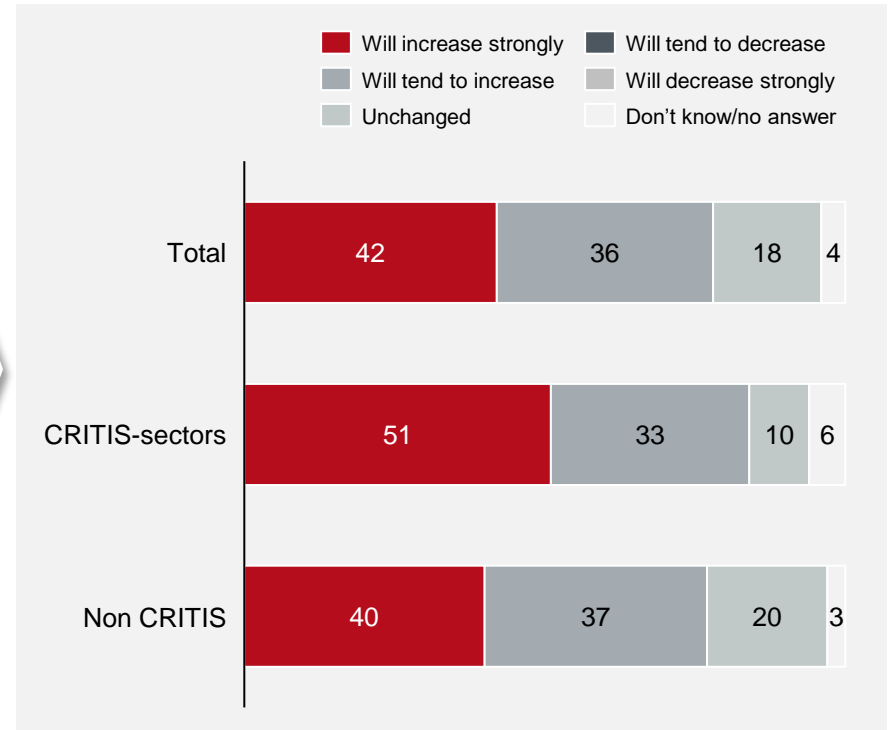
Source: Bitkom | Economic Protection 2022; 1: "Which of the following types of cyberattacks have caused damage in your company within the last 12 months?"

German economy affected by attacks across the board and expects increased cyber attacks

Affected by theft, industrial espionage or sabotage



Development of the number of cyberattacks



1: Basis: All companies surveyed (n=1,066) | Source: Bitkom Research 2022

CRA regulatory content

Cyber Security Act Com (2022) 454 - Regulatory content

| Chapter | Title | Article |
|----------------|---|----------------------------|
| 1 Chapter I | General provisions | ➤ Article 1 to Article 9 |
| 2 Chapter II | Obligations of economic operators | ➤ Article 10 to Article 17 |
| 3 Chapter III | Conformity of the product with digital elements | ➤ Article 18 to Article 24 |
| 4 Chapter IV | Notification of conformity assessment bodies | ➤ Article 25 to Article 40 |
| 5 Chapter V | Market surveillance and enforcement | ➤ Article 41 to Article 49 |
| 6 Chapter VI | Delegated powers and committee procedures | ➤ Article 50 to Article 51 |
| 7 Chapter VII | Confidentiality and sanctions | ➤ Article 52 to Article 53 |
| 8 Chapter VIII | Transitional and final provisions | ➤ Article 54 to Article 57 |

Security requirements for products with digital elements

Security requirements for products with digital elements

1 Production risk-aware to cyber security



2 Product features



3 Delivery without known vulnerabilities



a **Security by Default:** Delivery in standard configuration, with the option of a reset to the delivery status.

b **IAM:** Protection against unauthorised access such as authentication, identity or access management systems.

c **CIA protection Confidentiality of** processed data, e.g. through encryption of data at rest/motion

d **CIA protection Integrity of** processed data/ commands/ programmes/ configurations, notification of violation

e **Data economy:** process personal or other data adequate/relevant to the purpose.

f **CIA protection Availability of** essential functions, including denial-of-service attacks

g **Security by design:** minimising one's own negative impact on the availability of services of others

h **Security by design:** limiting attack surfaces, including external interfaces

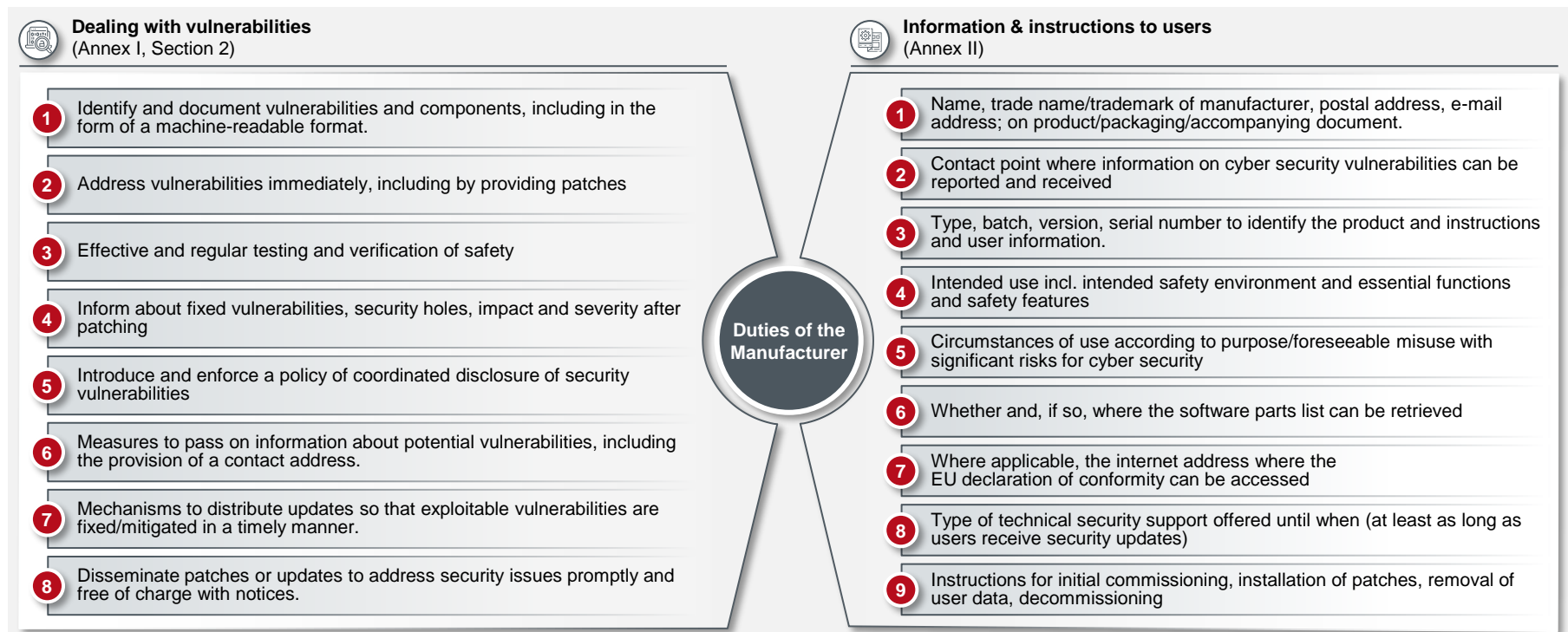
i **Security by design:** Reducing the impact of a security incident

j **Logging/monitoring:** Provision of security-relevant information including accesses

k **Security updates:** Provision of security updates, automatic or notification

Obligations of manufacturers

Obligations of the manufacturers



ISMS is the answer to the „Ultimate Question of Life, the Universe, and Everything “: The contents of ISO 27001 and DORA show many overlaps, an ISMS is indispensable



ISO 27001 Content

Illustration in DORA


Match?

Conclusion

| | ISO 27001 Content | Illustration in DORA | Match? | | |
|-----------------|--|---|--|---------------|---|
| ISO 27001 - HLS | 4 | Context of the organisation | Article 1 (1), Governance & Control Framework | ✓ | |
| | 5 | Leadership | Article 4 (2), Governing Body... supervised... | ✓ | |
| | 6 | Planning | Article 5, ICT Risk Management Framework | ✓ | |
| | 7 | Support | Article 1 (2f), adequate budgetary resources | ✓ | |
| | 8 | Operation | Article 4, Article 5 (1) | ✓ | |
| | 9 | Performance evaluation | Article 5 (5) | ✓ | |
| | 10 | Improvement | Article 5 (6), framework continuously improved | ✓ | |
| | ISO 27001 Security Controls | A.5 | Information Security Policy | Article 8 (2) | ✓ |
| | | A.6 | Organisation of information security | Article 4 (1) | ✓ |
| | | A.7 | Staff security | - | ✗ |
| A.8 | | Value management | Article 7 (1) | ✓ | |
| A.9 | | Access control | Article 8 (3b) | ✓ | |
| A.10 | | Cryptography | Article 8 (3a) | ✓ | |
| A.11 | | Physical and environmental security | Article 7 (4) | ✓ | |
| A.12 | | Operational safety | Article 8 (1), Article 21 to Article 24 | ✓ | |
| A.13 | | Communication security | - | ✗ | |
| A.14 | | Acquisition, development & maintenance of systems | Article 8 (4e,f) | ✓ | |
| A.15 | Supplier relations | Article 25 to Article 27 | ✓ | | |
| A.16 | Information security incident handling | Article 15 to Article 20 | ✓ | | |
| A.17 | IS aspects of business continuity management | Article 10, Article 11 | ✓ | | |
| A.18 | Compliance | Data protection: Article 26 (2) | ! | | |

- DORA focuses on
 - Risk management
 - Reporting of serious ICT incidents
 - Digital operational stability and its testing through threat-oriented penetration tests
 - Control of ICT third party providers
- These are essential elements of an ISMS that require preparatory and complementary work for their implementation
- These additional works are, for example, cryptography and physical security and are also components of an ISMS.

In practice, DORA requires an implemented ISMS



2013 version is reflected in 2022 version

| 5. Organizational Controls | | 5. Organizational Controls | | 7. Physical Controls | | 8 Technological Controls | |
|----------------------------|------------------------|----------------------------|------------------------|--------------------------|-------------------------------|--------------------------|-----------------------------|
| New assignment | Old allocation | New assignment | Old allocation | New assignment | Old allocation | New assignment | Old allocation |
| 5.1 | 05.1.1, 05.1.2 | 5.29 | 17.1.1, 17.1.2, 17.1.3 | 7.8 | 11.2.1 | 8.20 | 13.1.1 |
| 5.2 | 06.1.1 | 5.30 | New | 7.9 | 11.2.6 | 8.21 | 13.1.2 |
| 5.3 | 06.1.2 | 5.31 | 18.1.1,18.1.5 | 7.10 | 08.3.1, 08.3.2, 08.3.3,11.2.5 | 8.22 | 13.1.3 |
| 5.4 | 07.2.1 | 5.32 | 18.1.2 | 7.11 | 11.2.2 | 8.23 | New |
| 5.5 | 06.1.3 | 5.33 | 18.1.3 | 7.12 | 11.2.3 | 8.24 | 10.1.1,10.1.2 |
| 5.6 | 06.1.4 | 5.34 | 18.1.4 | 7.13 | 11.2.4 | 8.27 | 14.2.5 |
| 5.7 | New | 5.35 | 18.2.1 | 7.14 | 11.2.7 | 8.28 | New |
| 5.8 | 06.1.5,14.1.1 | 5.36 | 18.2.2,18.2.3 | 8 Technological Controls | | 8.29 | 14.2.8,14.1.3 |
| 5.9 | 08.1.1, 08.1.2 | 5.37 | 12.1.1 | New assignment | Old allocation | 8.30 | 14.2.7 |
| 5.10 | 08.1.3, 08.2.3 | 6. People Controls | | 8.1 | 06.2.1,11.2.8 | 8.31 | 12.1.4,14.2.5 |
| 5.11 | 08.1.4 | New assignment | Old allocation | 8.2 | 09.2.3 | 8.32 | 12.1.2,14.2.2,14.2.3,14.2.3 |
| 5.12 | 08.2.1 | 6.1 | 07.1.1 | 8.3 | 09.4.1 | 8.33 | 14.3.1 |
| 5.13 | 08.2.2 | 6.2 | 07.1.2 | 8.4 | 09.4.5 | 8.34 | 12.7.1 |
| 5.14 | 13.2.1,13.2.2,13.2.3 | 6.3 | 07.2.2 | 8.5 | 09.4.2 | | |
| 5.15 | 09.1.1, 09.1.2 | 6.4 | 07.2.3 | 8.6 | 12.1.3 | | |
| 5.16 | 09.2.1 | 6.5 | 07.3.1 | 8.7 | 12.2.1 | | |
| 5.17 | 09.2.4, 09.3.1, 09.4.3 | 6.6 | 13.2.4 | 8.8 | 12.6.1,18.2.3 | | |
| 5.18 | 09.2.2,09.2.5, 09.2.6 | 6.7 | 06.2.2 | 8.9 | New | | |
| 5.19 | 15.1.1 | 6.8 | 16.1.2,16.1.3 | 8.10 | New | | |
| 5.20 | 15.1.2 | 7. Physical Controls | | 8.11 | New | | |
| 5.21 | 15.1.3 | New assignment | Old allocation | 8.12 | New | | |
| 5.22 | 15.2.1,15.2.2 | 7.1 | 11.1.1 | 8.13 | 12.3.1 | | |
| 5.23 | New | 7.2 | 11.1.2,11.1.6 | 8.14 | 17.2.1 | | |
| 5.24 | 16.1.1 | 7.3 | 11.1.3 | 8.15 | 12.4.1, 12.4.2,12.4.3 | | |
| 5.25 | 16.1.4 | 7.4 | New | 8.16 | New | | |
| 5.26 | 16.1.5 | 7.5 | 11.1.4 | 8.17 | 12.4.4 | | |
| 5.27 | 16.1.6 | 7.6 | 11.1.5 | 8.18 | 09.4.4 | | |
| 5.28 | 16.1.7 | 7.7 | 11.2.9 | 8.19 | 12.5.1,12.6.2 | | |

Source: ISO/IEC 27002:2022

Comparison of ISO 27002:2022 to :2013 shows radical structural changes as well as emphasis on technology, TOM approach and data protection

| 5. Organizational Controls | 6. People Controls | 7. Physical Controls | 8 Technological Controls |
|----------------------------|--------------------|----------------------|--------------------------|
| 5.1 | 6.1 | 7.1 | 8.1 |
| 5.2 | 6.2 | 7.2 | 8.2 |
| 5.3 | 6.3 | 7.3 | 8.3 |
| 5.4 | 6.4 | 7.4 | 8.4 |
| 5.5 | 6.5 | 7.5 | 8.5 |
| 5.6 | 6.6 | 7.6 | 8.6 |
| 5.7 | 6.7 | 7.7 | 8.7 |
| 5.8 | 6.8 | 7.8 | 8.8 |
| 5.9 | | 7.9 | 8.9 |
| 5.10 | | 7.10 | 8.10 |
| 5.11 | | 7.11 | 8.11 |
| 5.12 | | 7.12 | 8.12 |
| 5.13 | | 7.13 | 8.13 |
| 5.14 | | 7.14 | 8.14 |
| 5.15 | 5.26 | | 8.15 |
| 5.16 | 5.27 | | 8.16 |
| 5.17 | 5.28 | | 8.17 |
| 5.18 | 5.29 | | 8.18 |
| 5.19 | 5.30 | | 8.19 |
| 5.20 | 5.31 | | 8.20 |
| 5.21 | 5.32 | | 8.21 |
| 5.22 | 5.33 | | 8.22 |
| 5.23 | 5.34 | | 8.23 |
| 5.24 | 5.35 | | 8.24 |
| 5.25 | 5.36 | | 8.25 |
| | 5.37 | | 8.26 |
| | | | 8.27 |
| | | | 8.28 |
| | | | 8.29 |
| | | | 8.30 |
| | | | 8.31 |
| | | | 8.32 |
| | | | 8.33 |
| | | | 8.34 |



- Main domains reduced from 14 to 4:
 - Organizational
 - People
 - Physical
 - Technological
- controls reduced from 114 to 93 - many controls were merged
- 11 new controls

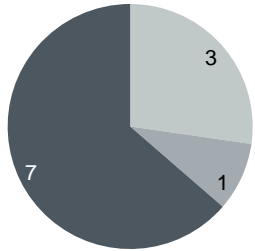
- Greater consideration of
 - Data protection
 - Cloud
 - Threats
 - modern coding
- Better structuring in domains

ISO 27002 is an appropriate adaptation to the modern age.



11 new controls in ISO 27002:2022 - strengthening data protection, cloud, threat analysis and modern development methods

- Organization
- Physical
- Technological



| Control | Description |
|---|---|
| 5.7 Threat Intelligence | Collect and analyse information on information security threats to produce threat analyses. |
| 5.23 IS for use of cloud services | The procedures for acquiring, using, managing and exiting cloud services should be established in accordance with the organisation's information security requirements. |
| 5.30 ICT readiness for business continuity | ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements. |
| 7.4 Physical security monitoring | Premises should be constantly monitored for unauthorised access. |
| 8.9 Configuration management | Configurations, including security configurations, of hardware, software, services and networks should be defined, documented, implemented, monitored and verified. |
| 8.10 Information deletion | Information stored in information systems, devices or on other storage media should be deleted when it is no longer needed. |
| 8.11 Data masking | Data masking should be done in accordance with access control and business requirements. |
| 8.12 Data leakage prevention | Data leakage prevention measures should be applied to systems, networks and other devices that process, store or transmit sensitive information. |
| 8.16 Monitoring activities | Networks, systems and applications should be monitored for anomalous behaviour and appropriate measures taken to assess potential information security incidents. |
| 8.23 Web filtering | Access to external websites should be managed to reduce exposure to malicious content. |
| 8.28 Secure coding | The principles of safe programming should be applied in software development. |