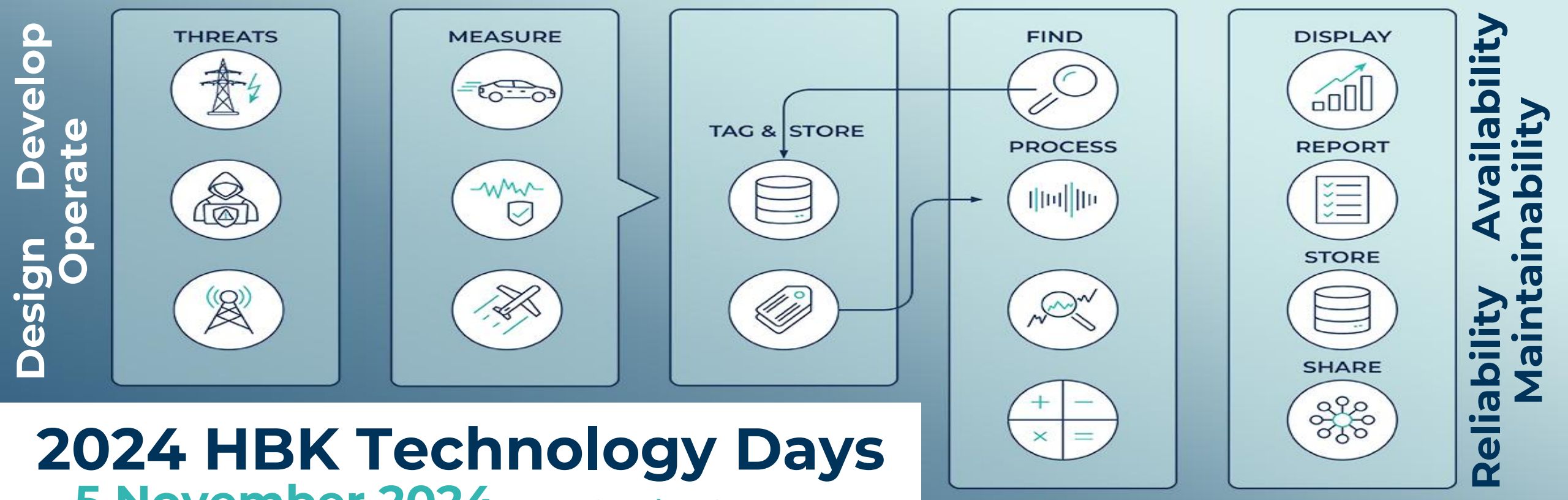




2024 HBK Technology Days

5 November 2024

Session 2: Minimising Cyber Threats to Sensors, Vehicles and Software

HBK Cyber Compliance

- ▲ CEP (Cyber Essentials Plus) certification.
 - It is an annual assessment of our cyber security health.
 - It is required to do business with UK Government & companies they work with.
- ▲ TISAX (Trusted Information Security Assessment Exchange)
 - Required by German Automotive companies
 - Covering all our German based products as well our VI-grade product range.
- ▲ DSCO (Deutsche Cyber-Sicherheitsorganisation).
 - Assessment for an automotive OEM for cloud measurement data.
 - This helps HBK reassure customers that our systems are safe to work with.

- Security regulations and compliance to minimise cyber threats from measurement sensors to software and AI

Tamlynn Deacon,
Director Cloud, Service & Cyber
HBK



Security regulations and compliance to minimise cyber threats from measurement sensors to software and AI

Abstract

- Security regulations and compliance aim to minimize cyber threats to measurement sensors, to software, and to AI by introducing and enforcing minimum standards. These include robust encryption, regular security audits, and adherence to industry-specific guidelines, to ensure secure data transmission, access controls, and continuous monitoring to help protect against vulnerabilities.
- In Europe, key regulations include the Cybersecurity Act, the NIS Directive, and the proposed Cyber Resilience Act. The Cybersecurity Act establishes a framework for cybersecurity certification of products, services, and processes. The NIS Directive focuses on improving the cybersecurity capabilities of critical infrastructure operators and digital service providers. The Cyber Resilience Act aims to ensure that digital products are secure throughout their lifecycle by mandating cybersecurity requirements for hardware and software. These regulations collectively enhance overall security and resilience against cyber threats, ensuring the integrity and confidentiality of sensitive information across all system components.

About the presenter, Tamlynn Deacon, Director Cloud, Service & Cyber, HBK

Minimizing Cyber Threats to Sensors, Vehicles and Software

SECURITY REGULATIONS AND COMPLIANCE TO MINIMISE CYBER THREATS FROM MEASUREMENT SENSORS TO SOFTWARE AND AI

Tamlynn Deacon
Director of Cloud, Service and
Cyber Security

Agenda

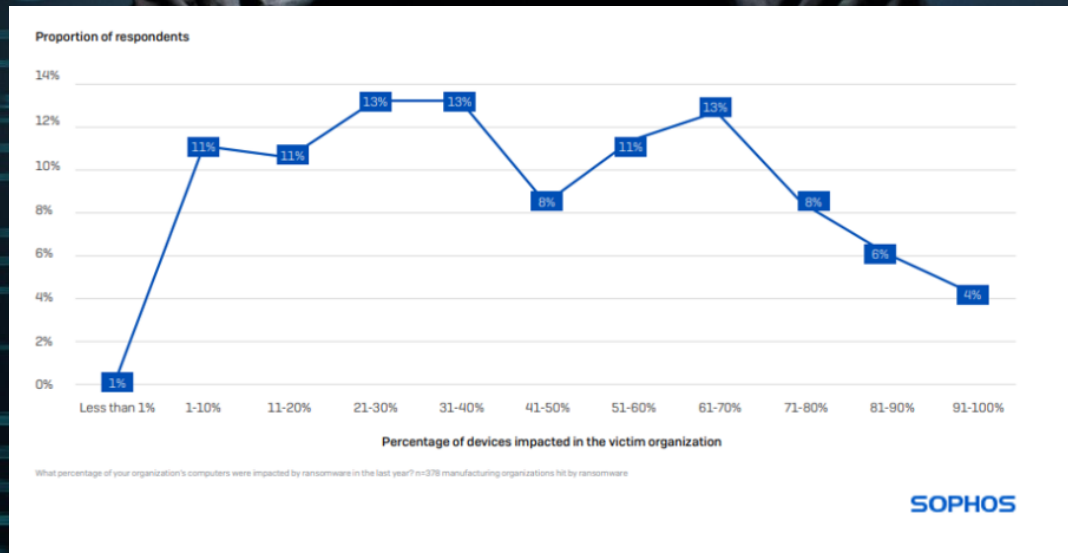
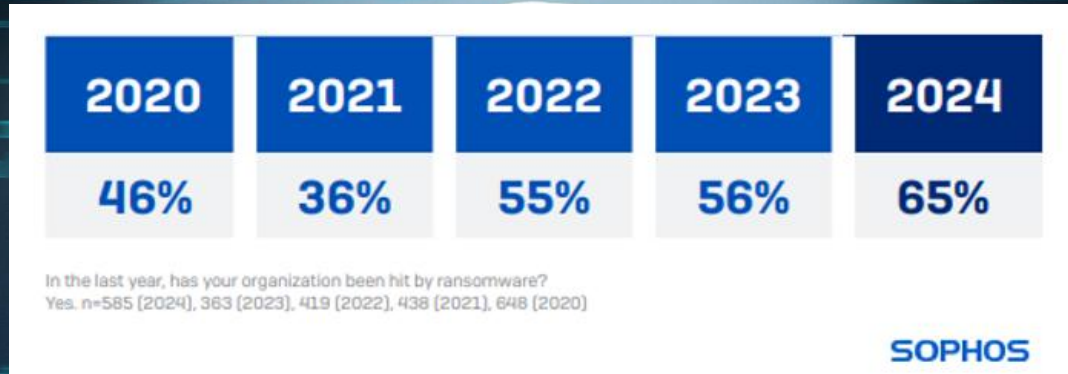
1. Speaker Introduction
2. Why is Cyber Security Important?
3. HBK Cyber Compliance
4. Existing Cyber Regulations (CSA, CRA, NIS2)
5. Scheduled AI Regulation (EU AI Act)
6. Summary

Tamlynn Deacon – Cyber Career



Why is Cyber Security Important?

- ▲ Increase in Cyber attacks in industry.
- ▲ Increase of ransomware attacks by 80% since 2021.
- ▲ Protected vs unprotected devices.
 - Average of 44% of manufacturing and production computers are impacted by ransomware.
 - Main cause for entry point is unprotected devices.
 - Only 50% of companies have more than half of their devices protected.





Why is Cyber Security Important?

- ▲ Examples of potential threat to products.
 - Firmware attacks
 - Data Integrity attacks
 - IoT device vulnerability
 - Supply chain attacks
 - Ransomware

**Regulations and Directives
are needed to
govern and reduce threats.**



Why is Cyber Security Important?

- ▲ To protect confidential information.
- ▲ To protect business continuity.
- ▲ To protect HBK.
- ▲ To protect HBK customers using HBK products and services.
- ▲ HBK customers have increasing cyber security requirements.

Cyber certification has become a purchasing quality requirement.

HBK Cyber Compliance

- ✓ HBK is highly focused on maintaining cyber security in line with our business objectives to Empower the Innovators
- ✓ Utilising Information Security management system aligned to ISO27K controls and NIST series as well as regulations
- ✓ 24/7 SOC team
- ✓ Threat intelligence
- ✓ Focused red teaming
- ✓ Monthly Executive Cyber security updates
- ✓ Industry led certifications / risk rating



HBK Cyber Compliance

- ▲ CEP (Cyber Essentials Plus) certification.
 - It is an annual assessment of our cyber security health.
 - It is required to do business with UK Government & companies they work with.
- ▲ TISAX (Trusted Information Security Assessment Exchange)
 - Required by German Automotive companies
 - Covering all our German based products as well our VI-grade product range.
- ▲ DSCO (Deutsche Cyber-Sicherheitsorganisation).
 - Assessment for an automotive OEM for cloud measurement data.
 - This helps HBK reassure customers that our systems are safe to work with.



HBK Cyber Compliance

▲ BITSIGHT

- Security performance management
- External real time validation of our Cyber Posture covering all HBK
- Consistently maintaining 'Advanced' rating

▲ Cybersecurity certifications are becoming the norm internationally.

- CMMC (Cybersecurity Maturity Model Certification) to work with US DoD has recently been finalised
- We will be discussing the latest EU regulations

▲ HBK can meet your cybersecurity requirements.

- With collaboration between Information and Cyber Security, Hardware and Software Development, Legal and Compliance teams.



CSA – Cyber Security Act

▲ Aim

- To achieve a high level of cybersecurity, cyber resilience, and trust within the EU.
- By establishing a comprehensive framework for cybersecurity certification.
- Through the EU Agency for Cybersecurity (ENISA).

▲ Scope

- Applies to Information and Communication Technology (ICT) products, services, and processes.
- Introduces an EU-wide cybersecurity certification framework.
- To ensure certified products and services are recognized across all EU member states.

▲ CSA came into force in June 2019.



CYBER RESILIENCE

CRA – Cyber Resilience Act

Introduces uniform cybersecurity standards for the design, development, production, and market availability of hardware and software products.

- ▲ Scope
 - Applies to all products connected directly or indirectly to another device or network, including IoT devices.
- ▲ CE Marking:
 - Products will bear the CE marking to indicate compliance with the regulation's cybersecurity requirements.



CYBER RESILIENCE

CRA – Cyber Resilience Act

- ▲ Lifecycle Responsibility
 - Manufacturers are responsible for the cybersecurity of their products throughout their **entire lifecycle**.
- ▲ Consumer Awareness
 - To make it easier for consumers to identify products with proper cybersecurity features, enhancing transparency and informed decision-making.
- ▲ Exceptions
 - Certain products, such as medical devices and aeronautical products, are exempt if they are covered by existing EU rules.
- ▲ CRA came into force 30 October 2024.

NIS2 – Network and Information Security Directive 2

An updated European Union regulation aimed at enhancing cybersecurity across member states.

▲ Scope

- Applies to a broader range of sectors and services compared to its predecessor, the original NIS Directive.
- It includes critical sectors like energy, transport, health, and digital infrastructure.

▲ Security Requirements

- Sets stricter security measures and incident reporting requirements for companies considered a part of critical infrastructure.



NIS2 – Network and Information Security Directive 2

▲ Supply Chain Security

- NIS2 addresses the security of supply chains.
- To ensure that all entities involved in the supply chain adhere to robust cybersecurity practices.

▲ Harmonised Sanctions

- Introduces harmonised sanctions across the EU.
- To ensure consistent enforcement and compliance.

▲ Implementation Timeline

- NIS2 came into force in January 2023.
- Member states had until October 2024 to transpose its measures into national law.



EU AI Act – European Union Artificial Intelligence Act

▲ Aim

- To ensure that AI systems used in the EU are safe, respect fundamental rights, and adhere to ethical principles.
- To foster trustworthy AI by addressing the risks associated with AI technologies.

▲ Scope

- Applies to all AI systems used within the EU, regardless of where developed.
- It categorizes AI applications into different risk levels:
 - Prohibited / Unacceptable Risk
 - High-Risk
 - Limited Risk
 - Minimal Risk

EU AI Act – European Union Artificial Intelligence Act

Classification	Description	Examples
Prohibited / Unacceptable Risk	AI systems that pose unacceptable risks and are banned.	AI that exploits vulnerabilities, pose a clear threat to safety, livelihoods, and rights, such as social scoring by governments
High-Risk	AI systems that significantly impact safety or fundamental rights. Subject to strict requirements.	AI in critical infrastructure, healthcare, education, employment, law enforcement
Limited Risk	AI systems with specific transparency obligations.	Chatbots, deepfakes
Minimal Risk	AI systems with minimal or no risk. Subject to minimal regulation.	AI-enabled video games, spam filters

EU AI Act – European Union Artificial Intelligence Act

▲ Focus

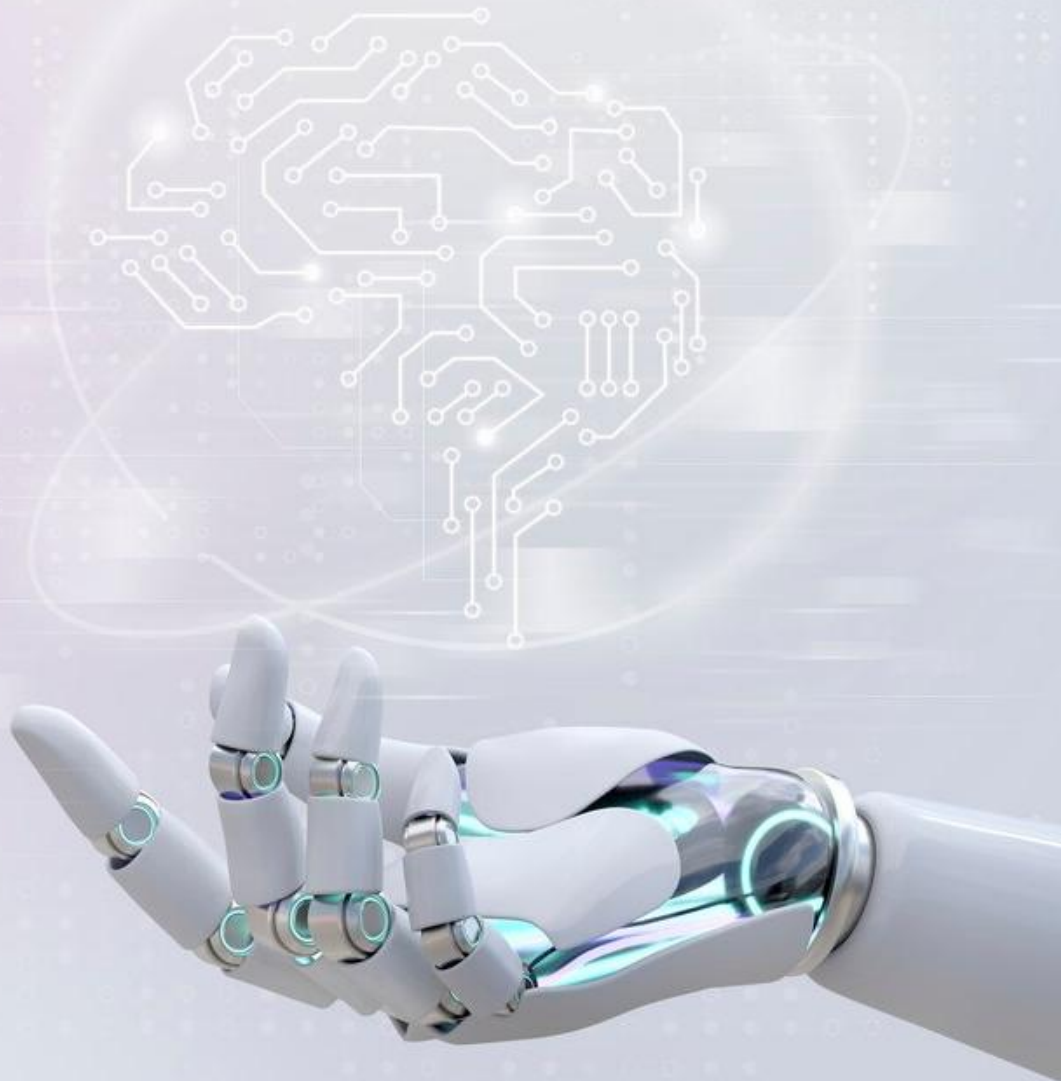
- To create a risk-based framework that ensures AI systems are used responsibly.
- To emphasize transparency, accountability, and human oversight to mitigate potential harm.

▲ Requirements:

- Risk Management, Data Governance, Transparency, Human Oversight, Robustness, and Accuracy.
- To ensure AI systems are reliable and perform accurately.

▲ Implementation Timeline

- From February 2025 to December 2030



ACT / Directive Comparison

ACT	CSA	CRA	NIS2 Directive	EU AI Act
Aim	Enhanced Cyber Security by creating a certification framework across ICT products	Enhanced Cyber Security across the entire lifecycle of digital products	Enhance the cybersecurity of network and information systems	Regulate the development, deployment, and use of artificial intelligence (AI) within the EU to ensure it is safe, transparent, and respects fundamental rights
Scope	Primarily focuses on establishing a framework for cybersecurity certification of ICT products, services, and processes	Applies to all products with digital elements, including hardware and software, that are connected directly or indirectly to another device or network	Covers a wide range of sectors, including energy, transport, health, and digital infrastructure. It applies to both public and private entities that meet specific criteria	Applies to all AI systems used within the EU, with specific provisions for high-risk AI applications, such as those used in critical infrastructure, education, employment, and law enforcement
Focus	Enhances trust and security in the digital single market by providing EU-wide certification schemes	Ensures products are secure throughout their lifecycle, from design to obsolescence	Critical infrastructure and essential services, with an emphasis on risk management, incident reporting, and supply chain security	Establishing a risk-based framework for AI, with different requirements based on the level of risk associated with the AI application
Requirements	Sets up a certification framework to ensure that ICT products and services meet specified cybersecurity standards	Introduces EU-wide cybersecurity standards for the design, development, production, and market availability of digital products	Manage cybersecurity risks, ensure corporate accountability, establish incident reporting processes, and plan for business continuity	High-risk AI systems must meet strict requirements, including risk management, data governance, transparency, human oversight, and robustness
Consumer Impact	Helps consumers and businesses make informed choices about the security properties of ICT products and services	Aims to make it easier for consumers to identify products with proper cybersecurity features	Creating secure environment by ensuring essential and digital services are better protected against cyberattacks	Aims to protect consumers by ensuring AI systems are safe, transparent, and respect fundamental rights, thereby fostering trust in AI technologies

Summary

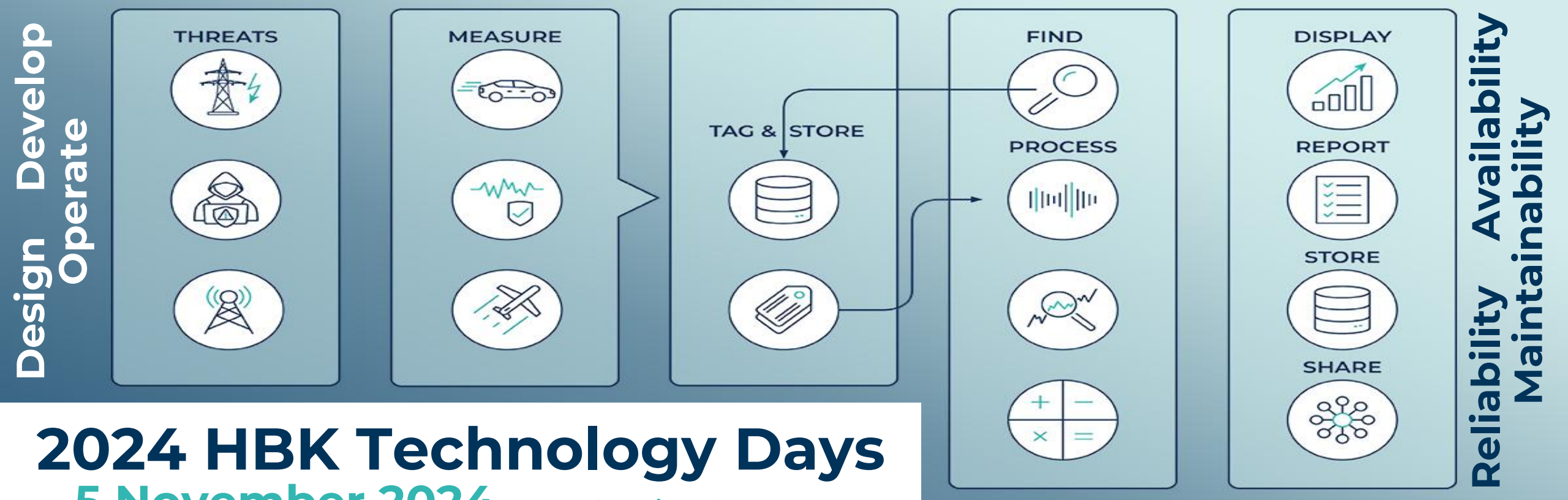
These regulations collectively contribute to a more secure and resilient digital environment in the EU, each addressing different aspects of cybersecurity and product security.

They will help us align and ultimately create more secure and future proofed products by ensuring:

- ▲ We have enhanced security measures across the entirety of our product lifecycle.
- ▲ We focus on risk management practices to mitigate potential security threats.
- ▲ We adhere to uniform compliance requirements for organizations to follow,, removing the doubt
- ▲ We continue to protect our consumers by ensuring that products and services meet stringent security standards.

Contact us to enable HBK to meet your hardware & software security requirements.

www.hbkworld.com



2024 HBK Technology Days

5 November 2024

Session 2: Minimising Cyber Threats to Sensors, Vehicles and Software

HBK Cyber Compliance

- ▲ CEP (Cyber Essentials Plus) certification.
 - It is an annual assessment of our cyber security health.
 - It is required to do business with UK Government & companies they work with.
- ▲ TISAX (Trusted Information Security Assessment Exchange)
 - Required by German Automotive companies
 - Covering all our German based products as well our VI-grade product range.
- ▲ DSCO (Deutsche Cyber-Sicherheitsorganisation).
 - Assessment for an automotive OEM for cloud measurement data.
 - This helps HBK reassure customers that our systems are safe to work with.

- Security regulations and compliance to minimise cyber threats from measurement sensors to software and AI

Tamlynn Deacon,
Director Cloud, Service & Cyber
HBK

