Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. – Project: 101190180.

EU Cloud Services Scheme (EUCS):

Regulation of Cloud Providers and Architectures under the Cyber Resilience Act

CRA training session
Understanding EUCS requirements and cloud architecture implications

Digital Innovation Hub Trakia

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

OSCRAT Open-Source Cyber Resilience Act Tools

About the Lecturer

- Lead Auditor for Management Systems (information security)
- Member of the **Institute for Artificial Intelligence** and founder of Safer.bg NGO.
- Managing director of **Zucchetti Bulgaria**
- Leading the Innovation ecosystem network of EDIH Trakia
- Assistant Professor at **UniBIT and Plovdiv university**:
  - ➢ Cybersecurity Standards
  - ➢ Cybersecurity fundamentals
  - ➢ ISO 42001:2023

What is EUCS?

Definition:

The EU Cloud Services Scheme (EUCS) is a comprehensive candidate cybersecurity certification framework specifically designed for cloud services operating within the European Union. It was established under the EU Cybersecurity Act (Regulation EU 2019/881) and developed by the European Union Agency for Cybersecurity (ENISA).

- Legal basis: EU Cybersecurity Act (Regulation 2019/881)
- Three assurance levels: Basic, Substantial, High
- Purpose: Harmonized security standards for cloud services across EU

EUCS - Purpose and Objectives

- Harmonization: Creates unified cybersecurity standards across all 27 EU member states, eliminating fragmentation of national certification schemes
- Trust Building: Enables cloud service providers (CSPs) to demonstrate their security capabilities through standardized, EU-wide recognized certification
- Market Access: Provides a single certification that is valid across the entire EU, reducing compliance costs and administrative burden for providers
- Risk Management: Addresses cybersecurity risks associated with cloud computing through structured evaluation processes

EUCS - Purpose and Objectives

- Harmonization: Creates unified cybersecurity standards across all 27 EU member states, eliminating fragmentation of national certification schemes
- Trust Building: Enables cloud service providers (CSPs) to demonstrate their security capabilities through standardized, EU-wide recognized certification
- Market Access: Provides a single certification that is valid across the entire EU, reducing compliance costs and administrative burden for providers
- Risk Management: Addresses cybersecurity risks associated with cloud computing through structured evaluation processes

EUCS - Legal Framework

- Primary Legislation: EU Cybersecurity Act (Regulation EU 2019/881)
- Development Authority: ENISA (European Union Agency for Cybersecurity)
- Enforcement: National cybersecurity certification authorities in each member state
- Market Impact: While certification is formally voluntary, other EU laws (NIS2 Directive, Data Act) may require EUCS certification for certain use cases
- a candidate cybersecurity certification scheme for cloud services under development by ENISA

EUCS - Three-Tier Assurance System

- Basic Level: Fundamental security controls for low-risk cloud services
- Substantial Level: Enhanced security measures for medium-risk applications
- High Level: State-of-the-art security requirements for critical infrastructure and high-risk scenarios
- Proposed High+ Level: Originally included sovereignty requirements (data localization, EU jurisdiction), currently under debate

EUCS - Scope of Coverage

SERVICE MODELS: INFRASTRUCTURE-AS-A-SERVICE (IAAS), PLATFORM-AS-A-SERVICE (PAAS), SOFTWARE-AS-A-SERVICE (SAAS)

CLOUD TYPES: PUBLIC, PRIVATE, HYBRID, AND MULTI-CLOUD ENVIRONMENTS

TECHNICAL STANDARDS: BASED ON ISO 27001/27002, C5:2020 (BSI), SECNUMCLOUD (ANSSI), AND OTHER INTERNATIONAL FRAMEWORKS

TRANSPARENCY REQUIREMENTS: MUST DISCLOSE DATA PROCESSING LOCATIONS, APPLICABLE LAWS, AND GOVERNANCE STRUCTURES

EUCS - Certification Process

Application: Cloud service providers apply to accredited certification bodies

Assessment: Third-party evaluation of security controls, documentation, and operational procedures

Duration: Three-year certification validity with ongoing monitoring requirements

Renewal: Periodic reassessment to maintain certification status

Recognition: Valid across all EU member states without additional national requirements

EUCS and CRA Connection

CRA covers "remote data processing" - cloud services essential for product function

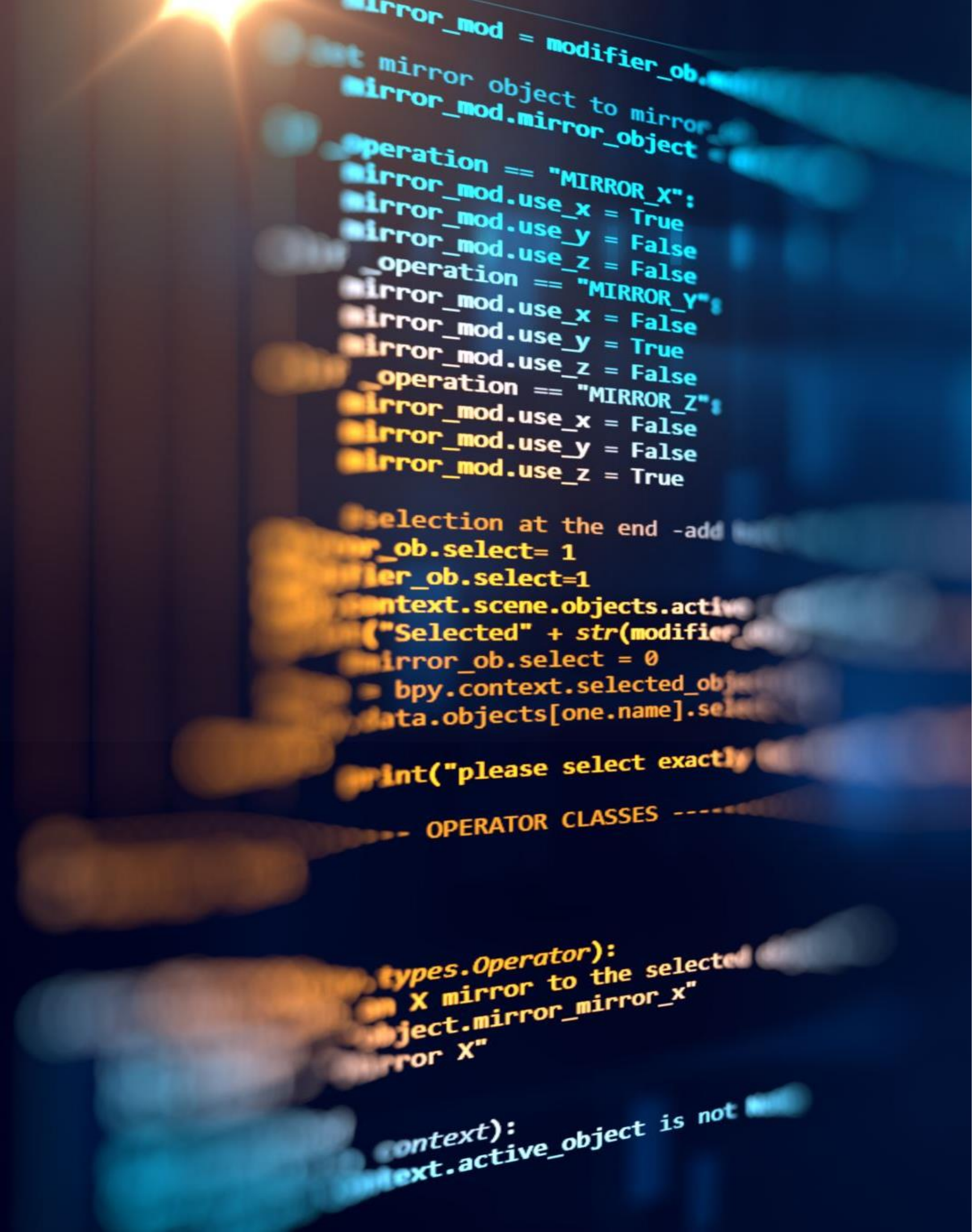
When EUCS applies: Cloud service designed by/for manufacturer and essential for product operation

Compliance requirement: Products with digital elements may require EUCS-certified cloud backend

Risk-based approach: Higher risk products need higher assurance levels

Cloud Architecture Types and Regulatory Impact

Cloud Type	EUCS Approach	Key Considerations
Public Cloud	Horizontal scheme applies	Shared infrastructure, stronger isolation requirements
Private Cloud	Horizontal scheme applies	Dedicated infrastructure, meets same EUCS criteria
Hybrid/Community	Horizontal scheme applies	All integrated environments covered; must document controls
Multi-tenancy	Isolation requirements	Ensure separation of physical/virtual resources between tenants
Subservices	Explicit assessment needed	Evaluate and document all dependent subservice organizations
Capability Types	Defined per draft	Infrastructure, Platform, Application; not just IaaS/PaaS/SaaS



Obligations for Cloud Providers

- Security by design throughout lifecycle
- Application document per **Annex F** (detailed controls, scope, subservices)
- Manage and assess all subservice organizations and dependencies
- Publish supplementary cybersecurity info (Article 55)
- Specify Complementary Customer Controls (CCCs)
- Incident and vulnerability management process (rapid response + notification)
- Maintenance: regular change management & periodic reassessment

Annex F it is not enough

Annex	Purpose
A	Security objectives & requirements
B	Assessment methodology & subservice dependencies
C	Assessment for Substantial/High levels
D	Assessment for Basic level
E	CAB competence requirements
F	Document content requirements
G	Certification lifecycle & maintenance
H	Peer assessment procedures
I	Terminology & definitions

EUCS Annexes: Description and Impact for Cloud Service Providers

Annex A: Security Objectives and Requirements

- Description: Lists all the technical and organizational security requirements (controls) that a CSP must implement, organized by assurance level (Basic, Substantial, High).
- Impact: *Core compliance task*. The CSP must assess their own environment against every requirement in Annex A, identify gaps, and align security measures to these controls. Non-compliance or weak implementation means failing certification.

EUCS Annexes: Description and Impact for Cloud Service Providers

Annex B: Assessment Methodology & Subservice Dependencies

- Description: Describes how to carry out security assessments, focusing on how subservices or external providers affect assurance, and how existing certified controls can be reused.
- Impact: CSPs must document all subservice dependencies and show how risks are managed end-to-end. Failure to map dependencies or rely on uncertified subservices can prevent certification or downgrade assurance level.

Annex C: Assessment for Substantial and High

- Description: Sets the audit procedures, documentation, and reporting standards for CSPs seeking Substantial or High assurance.
- Impact: CSPs at these levels must undergo thorough (often resource-intensive) third-party audits and produce detailed technical evidence, which means greater preparation, cost, and ongoing resource commitment.

EUCS Annexes: Description and Impact for Cloud Service Providers

Annex D: Assessment for Basic

- Description: Provides streamlined, self-assessment-focused requirements and checklists for Basic-level certification, including review by a conformity assessment body (CAB).
- Impact: Easier process for low-risk cloud offerings, but CSPs must still be vigilant as self-assessments are subject to CAB checks and possible escalation if issues emerge.

Annex E: CAB Competence Requirements

- Description: Defines expected qualifications and procedures for CABs.
- Impact: CSPs must select CABs meeting these standards—working with non-qualified CABs invalidates the process or delays market entry.

EUCS Annexes: Description and Impact for Cloud Service Providers

Annex F: Documentation Content Requirements

- Description: Explains how CSPs must structure and submit documentation for certification: including the application, evidence, and mapping to all controls.
- Impact: *Documentation burden is high*. CSPs must submit comprehensive and well-structured records—poor documentation can directly lead to rejection or extended

EUCS Annexes: Description and Impact for Cloud Service Providers

Annex G: Certification Lifecycle and Maintenance

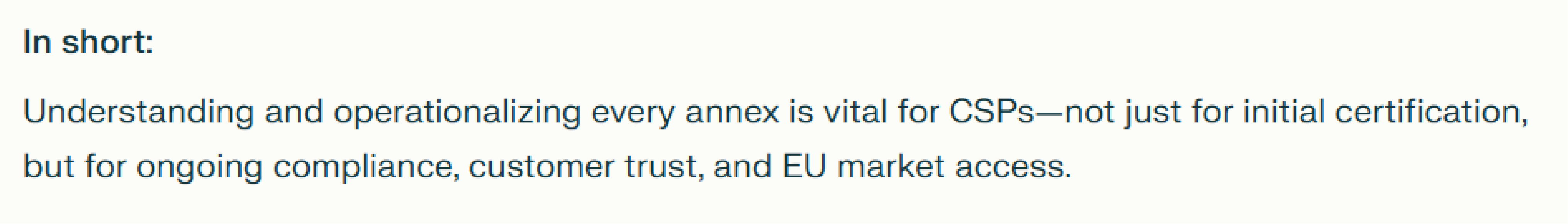
- Description: Lays out requirements for the duration, renewal, change management, and continued assurance for certificates.
- Impact: CSPs are obligated to maintain their security posture and update their compliance evidence over time—certification is not a one-time effort, but an ongoing process.

Annex H: Peer Assessment

- Description: Sets rules for reviewing CABs’ performance and consistency.
- Impact: *Indirect* but critical; helps ensure fairness and universality so CSPs face the same expectations across Europe.

Annex I: Terminology

- Description: Glossary of all important terms and references used in the scheme.
- Impact: Ensures CSPs properly interpret requirements, reducing ambiguity and errors during assessment.



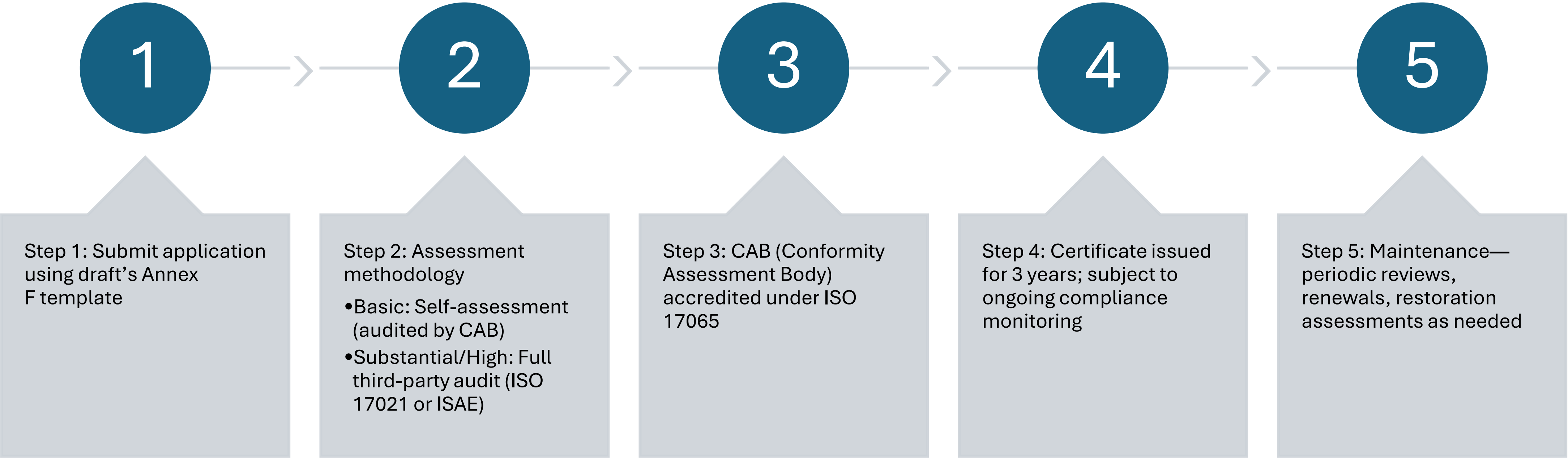
In short:

Understanding and operationalizing every annex is vital for CSPs—not just for initial certification, but for ongoing compliance, customer trust, and EU market access.

Manufacturer Responsibilities in Cloud Integration

- Select cloud providers certified under required EUCS level
- Include all relevant cloud controls and capabilities in technical documentation
- Align device support periods with certified cloud service
- Coordinate on vulnerability/incident handling and user notification
- Ensure complete system CE marking (device + cloud backend)
- Document customer responsibility including CCCs (Complementary Customer Control - mf)

EUCS Certification Process Steps



Step 1: Submit application using draft’s Annex F template

Step 2: Assessment methodology

- Basic: Self-assessment (audited by CAB)
- Substantial/High: Full third-party audit (ISO 17021 or ISAE)

Step 3: CAB (Conformity Assessment Body) accredited under ISO 17065

Step 4: Certificate issued for 3 years; subject to ongoing compliance monitoring

Step 5: Maintenance—periodic reviews, renewals, restoration assessments as needed

CAB stands for Conformity Assessment Body.

A CAB is the “official auditor” and certifier for cloud services aiming to be EUCS certified, ensuring trust, quality, and harmonized standards across the EU.A CAB is a Conformity Assessment Body. In the context of EUCS and other certification schemes, a CAB is:

- An accredited, independent organization (such as a certification or auditing company) responsible for evaluating whether a cloud service provider (CSP) meets all security and compliance requirements set by the scheme.
- CABs carry out assessments, audits, and reviews of CSP documentation, technical controls, processes, and ongoing maintenance, and ultimately issue certifications if all criteria are satisfied.
- For EUCS certification (especially for Substantial and High assurance levels), only CABs meeting strict qualification and competence criteria (see Annex E) can conduct these assessments.

Integrating EUCS with CRA Product Compliance

- Cloud essential for product: triggers EUCS requirement under CRA
- Documentation and certificate support technical file for product
- Vulnerability and incident management: coordinated process between manufacturer and cloud provider
- National authorities monitor compliance for both products and cloud services

Key Takeaways

- EUCS is a candidate scheme—requirements subject to finalization
- Horizontal approach covers all cloud types & capability categories
- Subservice assessment and CCCs central to compliance
- Timely maintenance and change management are mandatory
- Integration with CRA is essential for products relying on cloud services

Case Study: Applying EUCS to a Smart IoT Device (to be continue)

Scenario: Smart thermostat with analytics platform in the cloud

- Define scope: Infrastructure + Application capabilities
- Assess and document all cloud subservices
- Complete application per Annex F (controls, responsibilities)
- Coordinate with CAB for audit/assessment
- Document CCCs and user guidance
- Maintain compliance through updates and periodic reassessment

Case Study: Smart Thermostat with Cloud Analytics

Business Context

- **Manufacturer:** SmartHome Tech Ltd.
- **Product:** Intelligent thermostat with predictive heating/cooling
- **Cloud Service:** Real-time analytics platform for energy optimization
- **Market:** EU residential and small commercial buildings

Key Challenge

- Product relies on cloud for core functionality (remote control, analytics, AI predictions)
- CRA requires compliance for both device AND essential cloud services
- EUCS certification needed for cloud platform to support CRA compliance

Documentation and Assessment Process

Complete Annex F Application

- **Service Description:** Analytics platform capabilities and boundaries
- **Control Mapping:** Each Annex A requirement mapped to implemented controls
- **Subservice Controls (CSOCs):** Document inherited controls from AWS/Azure/etc.
- **Customer Controls (CCCs):** What thermostat users must configure
- **Evidence:** Policies, procedures, technical configurations, audit logs

CAB Coordination

- **Select Accredited CAB:** Choose based on cloud expertise and EUCS accreditation
- **Assessment Level:** Substantial (medium-risk IoT application)
- **Timeline:** 3-6 months from application to certificate
- **Audit Process:** Document review, technical testing, on-site assessment

Customer Responsibilities and Maintenance

Document CCCs (Examples)

- **User Account Security:** Strong passwords, MFA setup
- **Network Configuration:** Secure home WiFi settings
- **Privacy Settings:** Data sharing preferences and consent
- **Device Updates:** Installing firmware updates when available

User Guidance Provided

> - Setup wizard with security best practices
> - Regular security reminders via app notifications
> - Clear documentation on shared security responsibilities
> - Support channels for security-related questions

Maintain Compliance

- **Quarterly Reviews:** Monitor subservice compliance status
- **Annual Reassessment:** Formal CAB review of changes
- **Incident Response:** Coordinated handling of security issues
- **Certificate Renewal:** 3-year cycle with ongoing maintenance

(Case: How CRA Will Affect Smart IoT Device Manufacturers)

CRA Requirements for Manufacturer

- **Risk Assessment:** Comprehensive cybersecurity risk analysis for device + cloud
- **Technical Documentation:** Detailed security measures for entire system
- **CE Marking:** Demonstrate compliance for complete product (hardware + software + cloud)
- **Support Period:** Minimum 5 years of security updates for both device and cloud platform
- **Vulnerability Management:** Coordinated disclosure process with cloud provider

New Obligations

- **Essential Requirements:** Must meet Annex I cybersecurity requirements
- **Conformity Assessment:** May require third-party assessment for critical products
- **Incident Reporting:** Report exploited vulnerabilities to ENISA
- **Documentation:** Maintain comprehensive technical files throughout product lifecycle

Practical Implementation Roadmap

Phase 1 (Months 1-3): Preparation

- Gap analysis against CRA and EUCS requirements
- Select and engage CAB for EUCS certification
- Begin Annex F documentation

Phase 2 (Months 4-9): Certification

- Complete EUCS assessment and certification
- Finalize CRA technical documentation
- Prepare for conformity assessment

Phase 3 (Month 10+): Market Launch

- Product launch with CE marking
- Ongoing compliance monitoring
- Customer education and support

Key Challenges

- **Coordination:** Aligning device and cloud security measures
- **Documentation:** Comprehensive technical files and evidence
- **Ongoing Costs:** Maintaining certifications and compliance
- **Customer Education:** Ensuring users implement required CCCs

Thank you!

Yasen Tanev

+359 887 311 230

yasen.tanev@dihtrakia.org