



**ISA GLOBAL  
CYBERSECURITY  
ALLIANCE**

# ISA Webinar

All things automation and industrial cybersecurity

## Routes for Complying with the EU CRA & the Importance of Risk Assessments



**International Society of Automation**  
*Setting the Standard for Automation™*

15 October 2026

# ISA is the leading professional society for automation



Developer of 120+ consensus **standards** used around the world, including ISA/IEC 62443 for OT cybersecurity, ISA-95, ISA-18, ISA-112 and ISA-5



Globally recognized **training and certification** for OT cybersecurity, safety and automation professionals



Publications and **technical content** on ISA's media arm, Automation.com



**Industry consortia** and conformity assessment offerings for OT cybersecurity and wireless connectivity: ISA Global Cybersecurity Alliance, ISASecure and ISA100 Wireless



**Conferences**, exhibits and career development



**Mimo**®: the world's first LLM trained exclusively on automation content



# Presenter



## Michael Medoff, CFSE, CISA, CACE

Director of Certification  
**exida Certification LLC**  
**mmedoff@exida.com**



### About our Presenter

Michael Medoff is the Director of Certification for exida Certification LLC. His primary projects and special interested include:

- ✓ Helping product developer clients comply the functional safety and cybersecurity standards.
- ✓ TG Lead for the development of ISA/IEC 62443-4-1 Product Development Lifecycle Requirements 1st Edition.
- ✓ Co-lead of JT 62443-4-1 where they are working on the 2nd edition of ISA/IEC 62443-4-1.
- ✓ Mike is a member of JT -62443-07 who is reviewing and providing feedback on EN 62443.



# Overview

- CRA Introduction
- Product Categories
- Harmonized Standards
- Compliance Paths
- Exida Approach
- EN 62443
- Risk and Applicability Assessments
- Conclusions
- Questions

# European Union Cyber Resilience Act (CRA)

- CRA Applies to products with digital elements with a logical or physical data connection to a device or network
- A product with digital elements means a software or hardware product and its remote data processing solutions.
- Full compliance required for all new products with digital elements placed on the market in Europe after December 11, 2027
- Existing products are not retroactively required to meet the regulations unless they undergo substantial updates or modifications
  - Exception: Vulnerability and Incident Reporting

# Product Categories & Assessment Requirements

- **Critical** – 3<sup>rd</sup> party assessment required
- **Important Class II** – 3<sup>rd</sup> party assessment required
- **Important Class I** – self assessment to a harmonized standard
- **Default** – covers most devices, self assessment is sufficient

# Harmonized Standards

- Two types of Harmonized Standards
  - Horizontal – Applies broadly across product types and industries
  - Vertical – Applies to specific types of devices or industries
- Suppliers can choose which harmonized standards are used for their products
  - Compliance with a harmonized standard is not required
    - But compliance comes with **presumption of conformity** with the essential CRA requirements covered by that standard
  - You can also comply with CRA without complying with specific harmonized standards
  - It is usually easier to meet CRA by complying with harmonized standards

# Potential IACS Harmonized Standards

- From 62443 Family Base Standards
  - EN 62443-4-1 – Product Development Lifecycle (Draft available)
  - EN 62443-4-2 – Technical Security Requirements for ACS Components (Draft Available)
  - EN 62443-3-3 – Technical Security Requirements for ACS Systems (Planned)

# Potential Horizontal Harmonized Standards

| Deliverable                                                | Standard Number and Name                                 | Status                                                 |
|------------------------------------------------------------|----------------------------------------------------------|--------------------------------------------------------|
| <b>Vocabulary &amp; Definitions</b>                        | EN 40000-1-1: Cybersecurity requirements – Vocabulary    | Draft Available; Publication expected in November 2026 |
| <b>Principles of Cyber Resilience (Framework)</b>          | EN 40000-1-2: Cybersecurity principles & risk management | Draft Available; Publication expected in November 2026 |
| <b>Vulnerability Handling</b>                              | EN 40000-1-3: Vulnerability handling processes           | Draft Available                                        |
| <b>Generic Security Requirements</b>                       | EN 40000-1-4: Generic Security Requirements              | In Development                                         |
| <b>Technical Report on threats and security objectives</b> | TR 40000-1-5 Threats and Security Objectives             | In Development                                         |

# Vertical Standards

- Vertical standards will exist for products defined as critical, important class I, and important class II
- These standards will apply the CRA essential requirements explicitly for each type of product
  - Examples include Routers, Modems, Switches, Microprocessors, ASICs, FPGAs, Operating Systems
  - Approximately 41 such standards are planned

# Compliance Paths

| Path                                         | Advantages                                                                                                                           | Disadvantages                                                                                                                      |
|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Vertical Standard                            | Tailored for product type                                                                                                            | Many not available in draft form yet                                                                                               |
| EN 62443 Path                                | Draft Available<br>Market may expect this for maker of industrial products<br>Good fit for products that are ISA/IEC 62443 compliant | -May be difficult to meet for field products which typically would have lower power and capabilities<br>-Still may undergo changes |
| EN 40000-1-x                                 | Unknown                                                                                                                              | Draft Not Available for 1-4 yet (Technical Reqs.)<br>Will probably have many non-applicable requirements                           |
| Directly against CRA Essential Requirements  | Available Now                                                                                                                        | Requirements are very high level<br>Self assessment only allowed for default products                                              |
| Combination (Essential Requirements + 62443) | Ensures that essential requirements are met even if 62443 changes                                                                    | May need to adjust approach as standards are finalized                                                                             |
| Wait                                         | Better decision can be made with more information                                                                                    | Hard deadline is coming up in Dec. 2027                                                                                            |

# Exida Approach

- Exida is focusing on EN 62443 standards for now
- However, we have been looking at EN 40000-1-2 and 3 for risk assessment and vulnerability response processes
- Will evaluate EN 40000-1-4 when available for lower end products
- Will certify against vertical standards as needed

# EN 62443 Current Status

- 2<sup>nd</sup> Draft of EN 62443-4-1 and 4-2 are currently available
- 3<sup>rd</sup> Draft expected in Q4 2026 – This should be the final draft
- EN 62443-3-3 (Systems) Planned, but not yet in draft format

# Differences between EN and ISA/IEC 62443-4-1

| Practice Number |         | Section Name                                 | # Major Requirement Changes | # Minor Requirement Changes | Requirements with no material change |
|-----------------|---------|----------------------------------------------|-----------------------------|-----------------------------|--------------------------------------|
| 2018 IEC        | 2026 EN |                                              |                             |                             |                                      |
| 1               | 1       | Security Management                          | 4                           | 7                           | 7                                    |
| N/A             | 2       | Security Risk Management                     | 4                           | 4                           | 1                                    |
| 2               | 3       | Specification of Security Requirements       | 2                           | 1                           | 2                                    |
| 3               | 4       | Secure by Design                             | 4                           | 0                           | 3                                    |
| 4               | 5       | Secure Implementation                        | 0                           | 1                           | 2                                    |
| 5               | 6       | Security Verification and Validation Testing | 2                           | 4                           | 3                                    |
| 6               | 7       | Management of Security Related Issues        | 2                           | 1                           | 4                                    |
| 7               | 8       | Security Update Management                   | 2                           | 0                           | 5                                    |
| 8               | 9       | Security Guidelines                          | 0                           | 2                           | 6                                    |

**20 Major Requirement Changes that must be met**

# Key Updates to EN 62443-4-1

- Security Support Period
  - Regular Product Security Reviews
  - Regular Security Testing
- Software Bill of Material (SBOM)
- Security Risk Assessment
- Product Intended Use
- Information Categorization and Data Minimization
- Secure by Default

# Key Updates to EN 62443-4-2

- Eliminated Device Types
  - Software Application
  - Host Device
  - Embedded Device
  - Network Device
- Device types have different requirements subsets in the current IEC 62443-4-2
- Replaced by the applicability assessment
  - E.g. networking specific requirements will not be applicable to components without networking capability
- A security evaluation methodology has been added
  - This does not change any requirements, but provides insight as to how the requirements will be evaluated
- Acceptance Criteria Specifically documented for each requirement
  - Provides clear guidance for the evaluator
- Some technical requirements removed

# No security-level threshold

- EN 62443-4-2 does not specify what security level must be met to meet CRA requirements
- Previous analysis by exida and others determined meeting SL-2 would meet most CRA Requirements
- EN 62443-4-2 maps the CRA essential requirements to 4-2 requirements
  - SL-3 and SL-4 requirements must be considered
  - Start with this list of requirements and then cull down the list based on applicability and risk assessment

# SL-3 and SL-4 Requirements

| Security Level | FR 1 | FR 2 | FR 3 | FR 4 | FR 5 | FR 6 | FR 7 |
|----------------|------|------|------|------|------|------|------|
| SL-1           | 9    | 9    | 5    | 2    | 2    | 1    | 7    |
| SL-2           | 5    | 5    | 8    | 2    | 1    | 1    | 2    |
| SL-3           | 4    | 6    | 4    | 2    | 2    | 1    | 1    |
| SL-4           | 1    | 1    | 0    | 0    | 0    | 0    | 0    |
| Totals         | 19   | 21   | 17   | 6    | 5    | 3    | 10   |

**22 SL-3 and SL-4 Requirements**

**Table 1: Number of EN 62443 4-2 Requirements that must be considered**

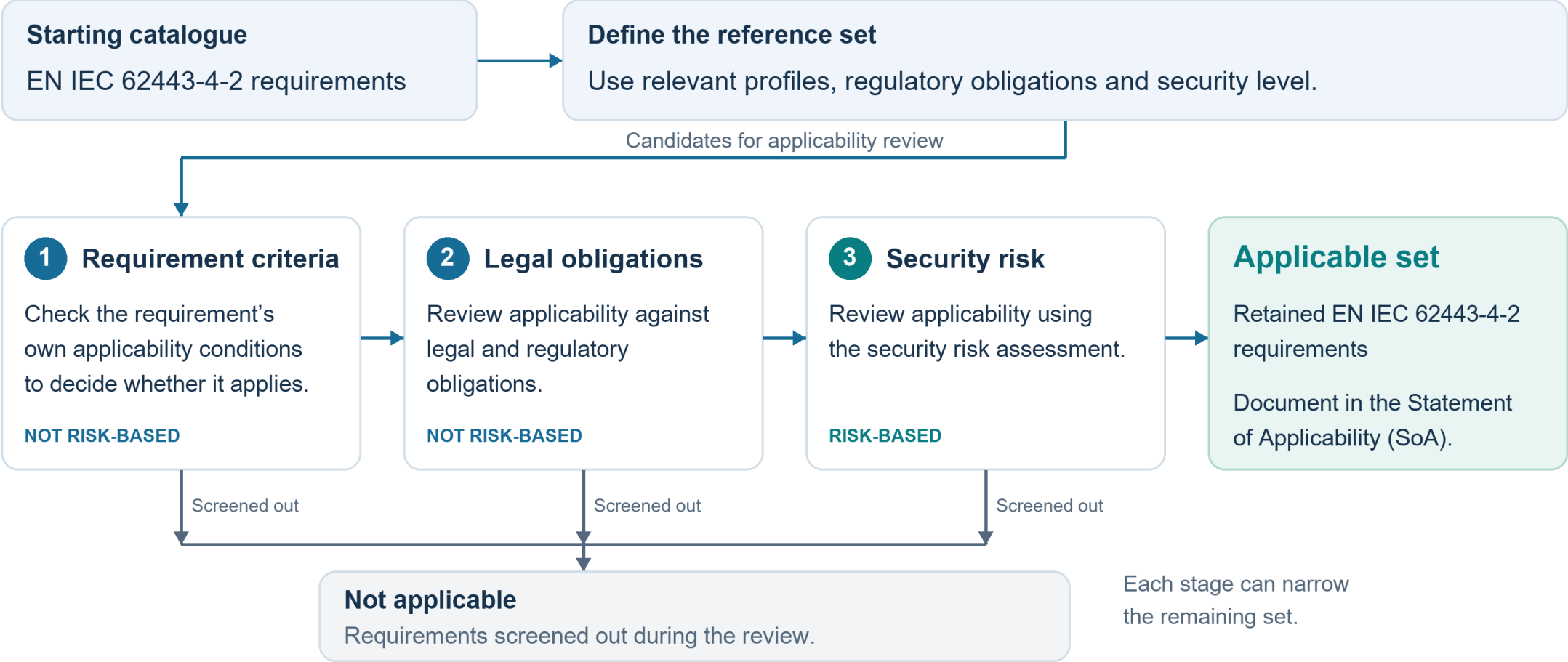
- Products Targeting SL-1 and SL-2 may still require higher level security requirements
- Requirements may be excluded due to:
  - Non-applicability
  - Regulatory conflicts
  - Security risk assessment
- Not every SL-3 or SL-4 requirement must be implemented-but each must be evaluated

# CRA Supports Requirement Reduction

1. Start with some required subset of requirements (e.g. EN 62443-4-2 SL-4) or Security Firewall Profile (based on EN 62443-4-2)
2. Filter Out Requirements based on:
  - Requirement Specific applicability criteria
  - Requirements prohibited by legal or regulatory obligations
  - Risk Assessment
    - Not applicable due to intended use or security context
    - Not applicable based on security risk acceptance criteria
    - Use threat model
    - Handling different concepts of acceptable risk
      - Must document non-applicable requirements + justification
      - Customers/end users can decide if they meet their risk assessment criteria

# Selecting applicable security requirements

Scope the requirement set, then review applicability in three stages.



# Risk Assessments

- Products are not overburdened by irrelevant or non-important cybersecurity requirements
- Risk assessments should be documented and justified
- Justifications should be based on well known guidelines or standards
  - Vertical Harmonized standards will provide guidance
  - Use case are needed because it hard to analyze risk out of context
  - Risk Assessments should be conservative and defensible given legal aspects
  - Third party review of risk assessments can help reduce risk

# Commission Guidance on Risk Assessment

- Risk assessments must consider the products application and intended purpose/ reasonably foreseeable use
- Manufacturers can not use their own risk tolerance, but must consider the operational environment
- The manufacturer cannot by their discretion accept all/ any residual risks
- Cybersecurity risk and responsibility cannot be transferred to the user, but documentation provided to users and restrictions on intended use can be taken into account
- Cost and commercial feasibility cannot be the justification for leaving risks untreated
- Cybersecurity Risks must be sufficiently addressed

*The guidance helps identify what not to do for a risk assessment, but there is limited guidance on what can be done for a successful risk assessment.*

# If the manufacturer's risk criteria can't be used, what criteria can be used?

*exida recommended approach, leverage industry guidelines to develop a reasonable matrix for typical users. (e.g., leveraging IEC 61511 informative guidance for process industry for asset and safety values)*

| Level | Severity                                                                    |                                                                                       |                                                                                                     |                                                                     |
|-------|-----------------------------------------------------------------------------|---------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|
|       | Confidentiality                                                             | Integrity                                                                             | Availability                                                                                        | Safety                                                              |
| S1    | Unauthorized access to restricted data with no business impact              | Loss of non-critical system data                                                      | Loss of availability leading to system downtime of less than 12 hours or less than \$10k in loss    | Personal nuisance with little to no physical harm (ex. first aid)   |
| S2    | Unauthorized access to restricted data with limited business impact         | Loss of system data with limited business impact                                      | Loss of availability leading to system downtime of more than 1 day days or less than \$100k in loss | Minor injuries requiring medical treatment                          |
| S3    | Unauthorized access to restricted data with moderate business impact        | Loss of system data with moderate business impact or regulatory penalties             | Loss of availability leading to system downtime of less than 10 days or less than \$1M in loss      | Several injuries resulting in loss time                             |
| S4    | Unauthorized access to highly restricted data with moderate business impact | Loss of system data with significant business impact or moderate regulatory penalties | Loss of availability leading to system downtime of less than 1 month or less than \$10M in loss     | One on-site fatality or one or more long term disabilities.         |
|       |                                                                             | Loss of system data with critical business impact or significant regulatory penalties | Loss of availability leading to system downtime of more than one month or more than \$10M in loss   | Multiple fatalities or an off-site fatality or long term disability |

| Likelihood | Severity   |            |            |             |             |
|------------|------------|------------|------------|-------------|-------------|
|            | S1         | S2         | S3         | S4          | S5          |
| Very High  | - Moderate | - Medium   | - High     | - Very High | - Very High |
| High       | - Low      | - Moderate | - Medium   | - High      | - Very High |
| Med        | - Very Low | - Low      | - Moderate | - Medium    | - High      |
| Low        | - Very Low | - Very Low | - Low      | - Moderate  | - Medium    |
| Very Low   | - Very Low | - Very Low | - Very Low | - Low       | - Moderate  |

*Screenshots from exSILentia CRA Software*

# What level of residual risk is tolerable?

- Leverage existing risk assessment methods (e.g., ISA/IEC 62443-3-2) to lead risk assessment process
- Reduce the likelihood of successful compromise by taking credit for cybersecurity protections designed into the product based on relevant standards (e.g., EN 62443-4-2 Draft)
- Document any application restrictions in user documentation
- Credit in risk assessment should be conservative and defensible

| Likelihood | Severity   |            |            |             |             |
|------------|------------|------------|------------|-------------|-------------|
|            | S1         | S2         | S3         | S4          | S5          |
| Very High  | - Moderate | - Medium   | - High     | - Very High | - Very High |
| High       | - Low      | - Moderate | - Medium   | - High      | - Very High |
| Med        | - Very Low | - Low      | - Moderate | - Medium    | - High      |
| Low        | - Very Low | - Very Low | - Low      | - Moderate  | - Medium    |
| Very Low   | - Very Low | - Very Low | - Very Low | - Low       | - Moderate  |

| Name      | User Defined Action                                                    | Color       |
|-----------|------------------------------------------------------------------------|-------------|
| Very Low  | No Action Required                                                     | Green       |
| Low       | No Action Required                                                     | Light Green |
| Moderate  | No product changes required, consider customer documentation           | Yellow      |
| Medium    | Consider implementing additional cybersecurity requirements in product | Orange      |
| High      | Cybersecurity requirements must be added for product                   | Red         |
| Very High | Cybersecurity requirements must be added for product                   | Dark Red    |

# Risk Assessment Workflow



| Threat |    |                                                                                                                                                                                                                                                         |          |            | Consequence |    |                                                                                            |            |          |                                        | Mitigation                               |                        |                                        |                |                        |         | Consequence |   |  |
|--------|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|------------|-------------|----|--------------------------------------------------------------------------------------------|------------|----------|----------------------------------------|------------------------------------------|------------------------|----------------------------------------|----------------|------------------------|---------|-------------|---|--|
| #      | ID | Name                                                                                                                                                                                                                                                    | Category | Likelihood | #           | ID | Name                                                                                       | Category   | Severity | Risk                                   | #                                        | ID                     | Name                                   | Security Level | Comments               | L w/Mit | R w/Mit     |   |  |
| 1      | 1  | User Spoofing- Network Sniffing: An unauthorized individual uses a network sniffing attack to acquire access credential information to subsequently perform unauthorized access to the IACS via user spoofing. IEC62443-4-2 FR1 – ID and Authentication | L        | Very High  | 1           | 1  | Manipulation of operational data leading to potential loss of control and equipment damage | Confide... | S1       | 3                                      | 1p                                       | 22                     | CR 1.9C Strength of certificate-bas... | SL-2           | Not currently in place | High    | C...        | 2 |  |
|        |    |                                                                                                                                                                                                                                                         |          |            | Integrity   | S1 |                                                                                            | 3          | 2p       | 21                                     | CR 1.9B Strength of certificate-bas...   | SL-2                   | Not currently in place                 | I...           | 2                      |         |             |   |  |
|        |    |                                                                                                                                                                                                                                                         |          |            | Availab...  | S3 |                                                                                            | 5          | 3p       | 20                                     | CR 1.9A Strength of certificate-bas...   | SL-2                   | Not currently in place                 | A...           | 4                      |         |             |   |  |
|        |    |                                                                                                                                                                                                                                                         |          |            | Safety      | S3 |                                                                                            | 5          | 4p       | 19                                     | CR 1.8 Public key infrastructure cert... | SL-2                   | Not currently in place                 | S...           | 4                      |         |             |   |  |
|        |    |                                                                                                                                                                                                                                                         |          |            |             |    |                                                                                            | 5p         | 18       | CR 1.7 RE (2) Password lifetime res... | SL-4                                     | Not currently in place |                                        |                |                        |         |             |   |  |
|        |    |                                                                                                                                                                                                                                                         |          |            |             |    |                                                                                            | 6p         | 17       | CR 1.7 RE (1) Password generation...   | SL-3                                     | Not currently in place |                                        |                |                        |         |             |   |  |
|        |    |                                                                                                                                                                                                                                                         |          |            |             |    |                                                                                            | 7p         | 16       | CR 1.7 Strength of password-base...    | SL-1                                     | Implemented            |                                        |                |                        |         |             |   |  |
|        |    |                                                                                                                                                                                                                                                         |          |            |             |    |                                                                                            | 8p         | 15       | CR 1.6 RE (1) Unique Identification... | SL-2                                     | Not currently in place |                                        |                |                        |         |             |   |  |
|        |    |                                                                                                                                                                                                                                                         |          |            |             |    |                                                                                            | 9p         | 14       | CR 1.6 Wireless access management      | SL-1                                     | Implemented            |                                        |                |                        |         |             |   |  |
|        |    |                                                                                                                                                                                                                                                         |          |            |             |    |                                                                                            | 10p        | 13       | CR 1.5 RE (1) Hardware security for... | SL-3                                     | Not currently in place |                                        |                |                        |         |             |   |  |
|        |    |                                                                                                                                                                                                                                                         |          |            |             |    |                                                                                            | 11p        | 12       | CR 1.5D Authenticator Management       | SL-1                                     | Implemented            |                                        |                |                        |         |             |   |  |
|        |    |                                                                                                                                                                                                                                                         |          |            |             |    |                                                                                            | 12p        | 11       | CR 1.5C Authenticator Management       | SL-1                                     | Implemented            |                                        |                |                        |         |             |   |  |
|        |    |                                                                                                                                                                                                                                                         |          |            |             |    |                                                                                            | 13p        | 10       | CR 1.5B Authenticator Management       | SL-1                                     | Implemented            |                                        |                |                        |         |             |   |  |
|        |    |                                                                                                                                                                                                                                                         |          |            |             |    |                                                                                            | 14p        | 9        | CR 1.5A Authenticator Management       | SL-1                                     | Implemented            |                                        |                |                        |         |             |   |  |



# Conclusions

- Harmonized standards provide presumption of conformity for CRA requirements they cover
  - But all are still in development
- Choices of harmonized standards exist
- Use “candidate” harmonized standards + CRA Essential Requirements
- Evaluate all relevant CRA-mapped requirements using applicably and security risk assessment
  - This will determine set of requirements that must be met
- Revisit analysis as standards become harmonized
- Document exclusions and risk treatment, and maintain the assessment throughout the support period

# Questions?