Vulnir

Deep Dive Session Security Controls – 40000-1-4

5 March 2026 - SURVEY

Angelo D'Amato
Founder

Meet your speaker

Angelo D'Amato
Founder / Cybersecurity Expert, Vulnir

Background

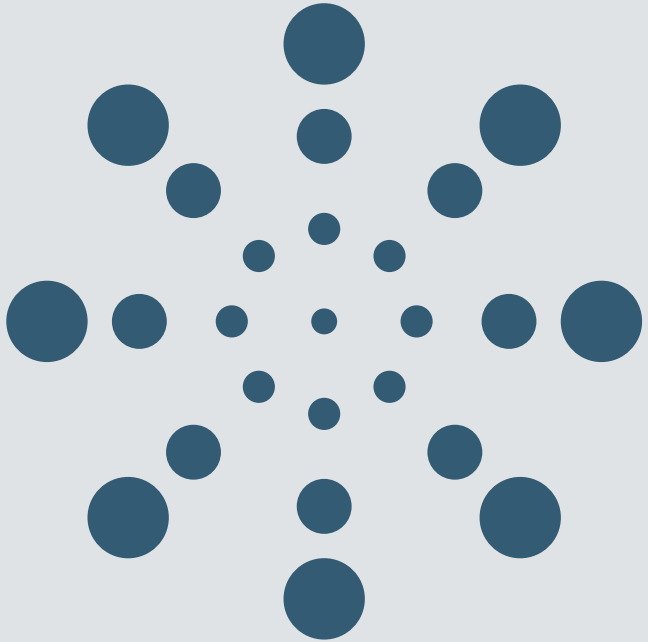
- With over fifteen years of experience, he is the subject matter expert for:
  - End-to-end cybersecurity assessments (Penetration testing, Security assessments)
  - Certifications and assessment (e.g., EN 303 645, Common Criteria, IEC 62443)
  - Regulatory compliance (e.g., Radio Equipment Directive, Cyber Resilience Act)
- I currently cover the role of rapporteur as a CEN contractor (*) within CEN/CLC/JTC 13/WG 9 for the following CRA standards:
  - PT2: Generic Security Requirements (prEN 40000-1-4)
  - PT3: Vulnerability handling requirements (prEN 40000-1-3)

* The European Union funds my activities within the STAN4CR project through the European Innovation Council and SMEs Executive Agency (EISMEA) under Grant Agreement No. 101196779.

CEN CENELEC EFTA European Commission

EVENT PAGE: https://www.stan4cra.eu/event-details/cra-standards-unlocked-deep-dive-session-security-controls-generic-security-requirements

06 Security requirements: Deep Dive Survey



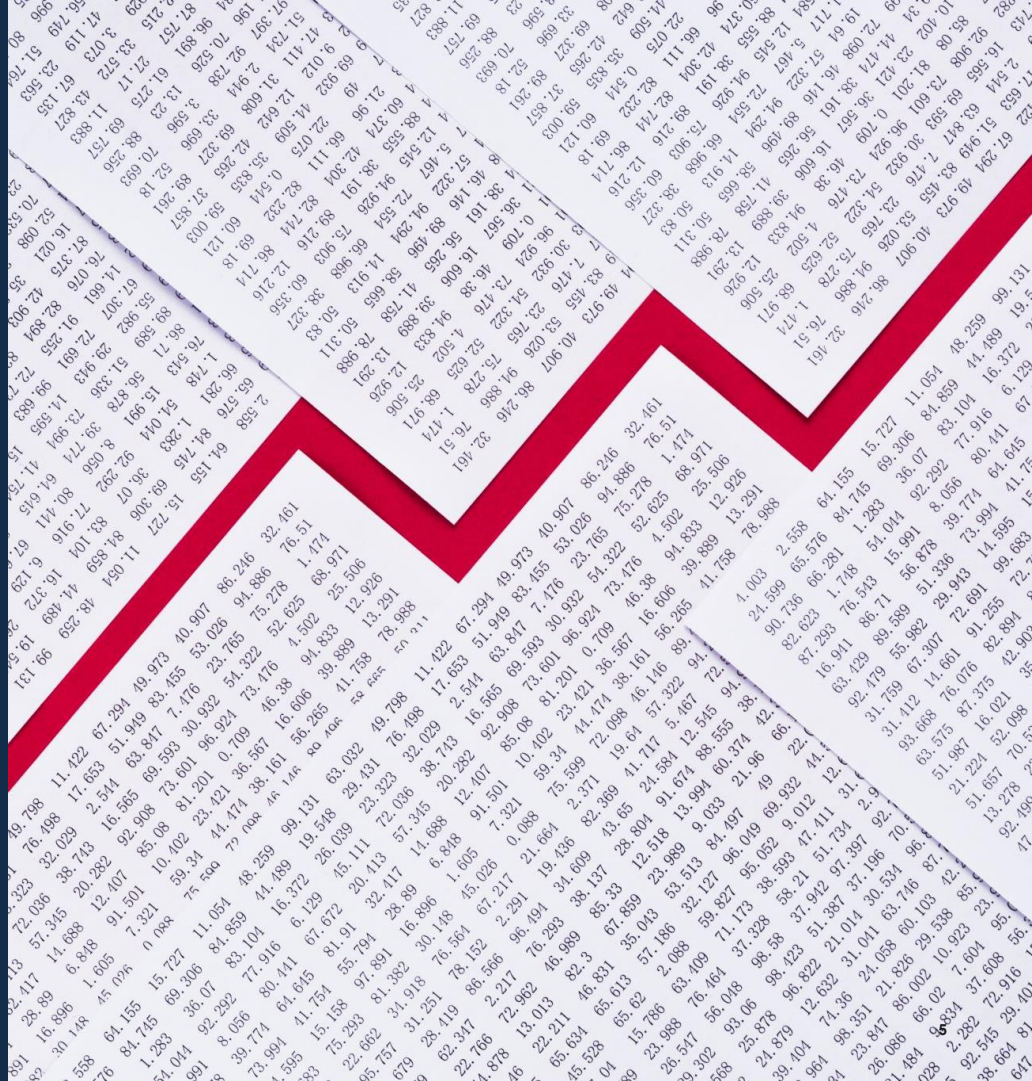
Survey participant overview

6.1	(a) - Vulnerability Assessment	3.98 Average Rating	115
6.2	(b) - Secure Configuration	4.16 Average Rating	87
6.3	(c) - Security Updates	4.12 Average Rating	58
6.4	(d) - Access Control	4.03 Average Rating	39
6.5	(e) - Confidentiality (Disclosure)	4.13 Average Rating	48
6.6	(f) - Integrity (Tampering)	4.20 Average Rating	30
6.7	(g) - Data Minimization	4.00 Average Rating	40
6.8	(h) - Availability	4.10 Average Rating	40
6.9	(i) – Minimize negative impact	4.25 Average Rating	32
6.10	(j) - Attack Surface Minimization	4.29 Average Rating	38
6.11	(k) – Reduce Impact of Incident	4.08 Average Rating	40
6.12	(l) - Monitoring and Logging	4.14 Average Rating	35
6.13	(m) - Data Deletion	4.28 Average Rating	36

7	Post-Workshop Survey: Cyber Resilience Act - Vulnerability Handling	4.38 Average Rating	26

6.1 (a) -

Vulnerability Assessment

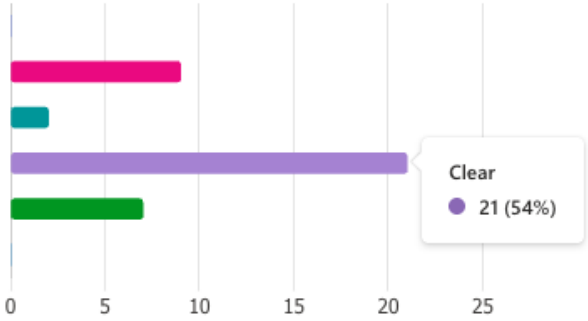


Vulnir

2. Clarity and Understandability: How clear and easy to understand is the proposed content for this section?

More details

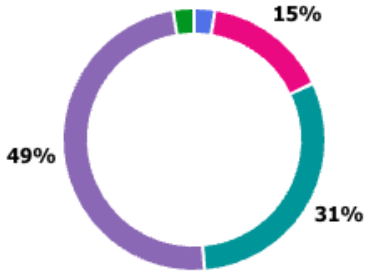
Not Clear	0
Somewhat clear	9
Neutral	2
Clear	21
Very Clear	7
Other	0



3. Practicality and Implementability: How practical and implementable do you find the requirements/guidance in this section for yo ur organization or typical stakeholders?

More details

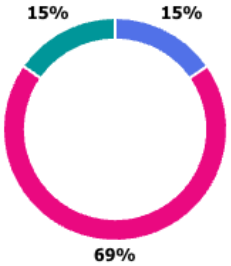
Not Practical	1
Somewhat practical	6
Neutral	12
Practical	19
Very Practical	1



4. Do you feel anything significant is missing from this section?

More details

Yes	6
No	27
Maybe	6



5. If you felt that something significant is missing please specify:

More details

8
Responses

Latest Responses
"physical control"
"Can the product delegate authentication to the OS of the PC it is installed on (e.g. ... "
...

3 respondents (50%) answered manufacturers for this question.

Update

5.If you felt that something significant is missing please specify:

1	more clarity on notification requirement
2	add information to FAQ for which product types certain mechanisms are probably not applicable
3	Great to see that the "applicability" requirements from EN18031 will be dropped and replaced by Risk Assessment.
4	In the standard, specify if access control apply to human and/or machine-to-machine access
5	Describe physical control as one of the authorized access controls

6. Suggestions for Improvement: What specific changes or additions would you recommend for this section?

More details

5

Responses

Latest Responses

"Describe physical control as one of the authorized access controls"

"In the standard, specify if access control apply to human and/or machine-to-machi..."

"Great to see that the "applicability" requirements from EN18031 will be dropped a... "

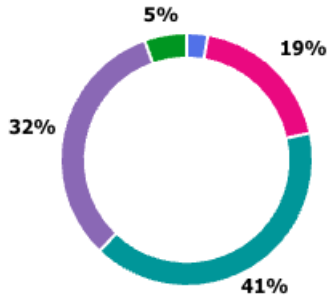
...

6.Suggestions for Improvement: What specific changes or additions would you recommend for this section?

1	more clarity on notification requirement
2	add information to FAQ for which product types certain mechanisms are probably not applicable
3	Great to see that the "applicability" requirements from EN18031 will be dropped and replaced by Risk Assessment.
4	In the standard, specify if access control apply to human and/or machine-to-machine access
5	Describe physical control as one of the authorized access controls

7. In your opinion, is the proposed section proportionate to the cybersecurity risks it aims to address for organizations of all sizes, p articularly Small and Medium-sized Enterprises (SMEs)? More details

Not at all proportionate/Excessive burden	1
Somewhat disproportionate/Significant burden for SMEs	7
Neutral/Unsure	15
Somewhat proportionate/Manageable for most SMEs	12
Very proportionate/Well-adapted for SMEs	2



8. Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME: More details

3
Responses

Latest Responses
"The risk assessment process will make it hard for engineers without any knowledg... "
...

8.Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

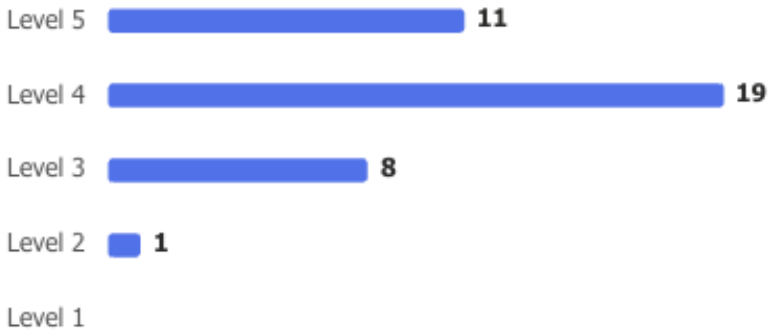
1	our products do not have architectures supporting such mechanisms. Still we have to do something. This causes likely a lot of redesign efforts.
2	Not clear if we can still make use of generic users to authenticate to a device
3	The risk assessment process will make it hard for engineers without any knowledge about security an risks. Hard requirements like the mentioned "applicable" requirements make it way easier but it resulted in a lot of problems for manufacturers to be compliant. Because in a lot of cases, they did not make sense! Really like it, thanks!

9. Overall, how satisfied are you with this section?

More details

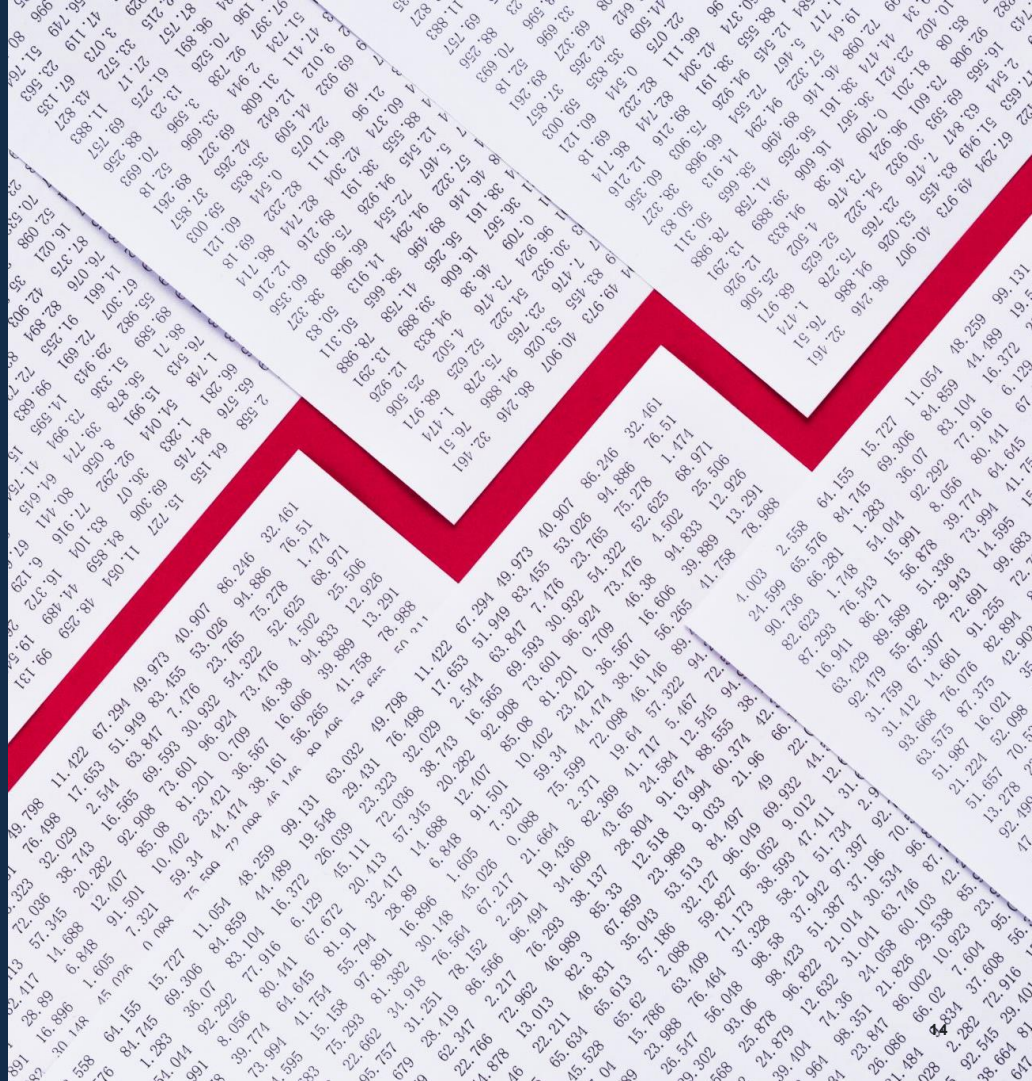
4.03

Average Rating



6.2 (b) -

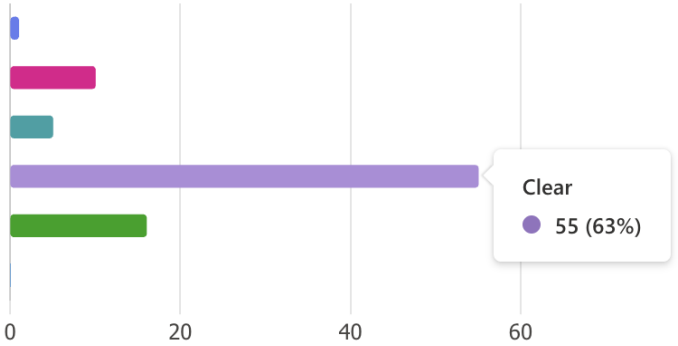
Secure Configuration



2. Clarity and Understandability: How clear and easy to understand is the proposed content for this section?

More details

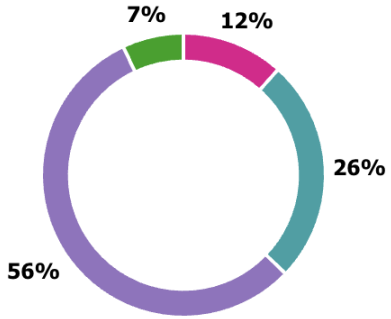
Not Clear	1
Somewhat clear	10
Neutral	5
Clear	55
Very Clear	16
Other	0



3. Practicality and Implementability: How practical and implementable do you find the requirements/guidance in this section for your organization or typical stakeholders?

More details

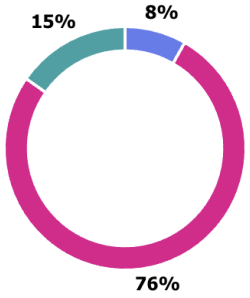
Not Practical	0
Somewhat practical	10
Neutral	22
Practical	48
Very Practical	6



4. Do you feel anything significant is missing from this section?

More details

Yes	7
No	65
Maybe	13



5. If you felt that something significant is missing please specify:

More details

7
Responses

Latest Responses
...

3 respondents (43%) answered products for this question.

5.If you felt that something significant is missing please specify:

1	Applicability to industrial products, power plants for instances
2	Better distinguishing between secure configuration and implemented security controls
3	Up-to-date implementation guidance
4	How to handle security by default in products that are to be integrated in host devices (i.e. radio modules, chip sets)
5	Difference between product, equipment and remote data processing equipment and the scope of the requirement.
6	How to demonstrate evidence of these different controls?
7	The structure of the slides is very clear and understandable, however going a bit deeper to what we can expect in 40000-1-4 with regard to the respective requirement would be very helpful. At the moment it looks like we see the different inputs.

6. Suggestions for Improvement: What specific changes or additions would you recommend for this section?

More details

6
Responses

Latest Responses

"Secure deletion may need a technical clarification; it may be easier said than... "

...

1 respondents (20%) answered Password Handling for this question.

Update

webinar Best Practices data processing
root Password Handling industrial environment
comment in chat initial Password offered regularly

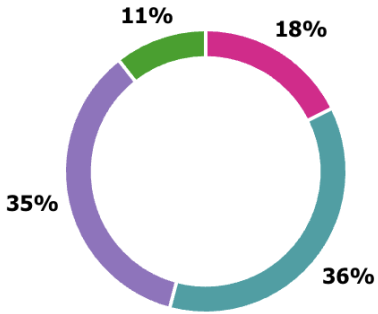
6.Suggestions for Improvement: What specific changes or additions would you recommend for this section?

1	I hope courses like this can be offered regularly.
2	Address the remote data processing.
3	I liked the comment in chat to "not run everything as root" - this is the level that implementors understand.
4	Guideance for Best Practices, e.g. initial Password Handling in industrial environment.
5	Hope to allow more audiences in the next webinar.
6	Secure deletion may need a technical clarification; it may be easier said than done with some products (cf. disks/storage, etc.).

7. In your opinion, is the proposed section proportionate to the cybersecurity risks it aims to address for organizations of all sizes, particularly Small and Medium-sized Enterprises (SMEs)?

More details

Not at all proportionate/Excessive burden	0
Somewhat disproportionate/Significant burden for SMEs	15
Neutral/Unsure	31
Somewhat proportionate/Manageable for most SMEs	30
Very proportionate/Well-adapted for SMEs	9



8. Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

More details

7
Responses

Latest Responses

"I'd argue that these are really fundamental things that have been a part of g... "

. . .

8.Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

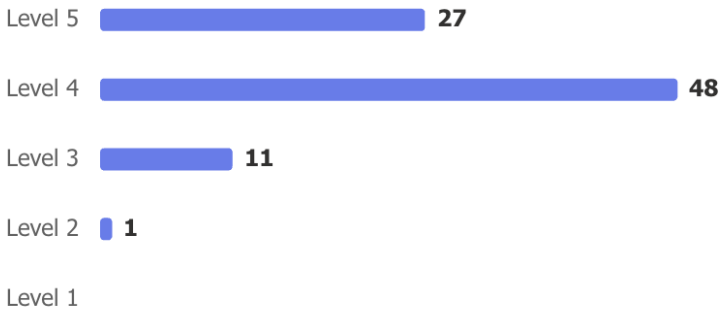
1	This section doesn't have anything that I think would add undue burden to SMEs
2	SME's have already done the EN 18031 work, continuing with the same labeling and requirements reduces the burden.
3	too much complexity, too many aspects, processes and understanding do not always exist to the extent that we would like to have. How to you intend to implement Article 10 (education) for this? Teaching e-learnings for developers would be nice.
4	Vulnerability analysis on smart objects is still being stabilized via OWASP and NIST. It will be interesting to understand how to manage this, including in terms of resets.
5	Overall, an "interactive" tool that guides through processes (and end-product standards) would be helpful.
6	The CRA aldo applies to very small software houses. These companies may find it very complicated to address formal requirements for non-vertical products with low risk and a limited market, so more specific guidance for these cases and lightweight implementation would be useful
7	I'd argue that these are really fundamental things that have been a part of good practices already for the past 30 years or so.

9. Overall, how satisfied are you with this section?

More details

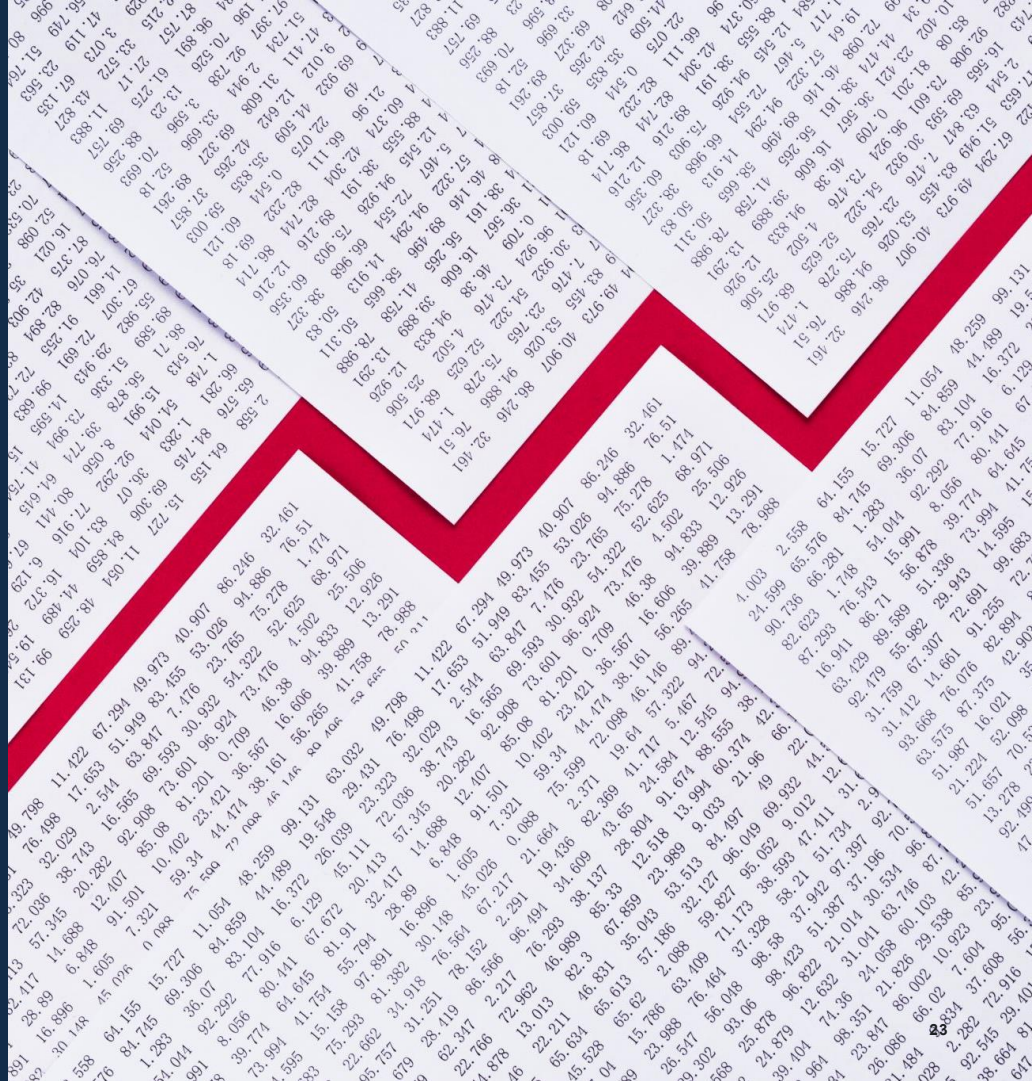
4.16

Average Rating



6.3 (c) -

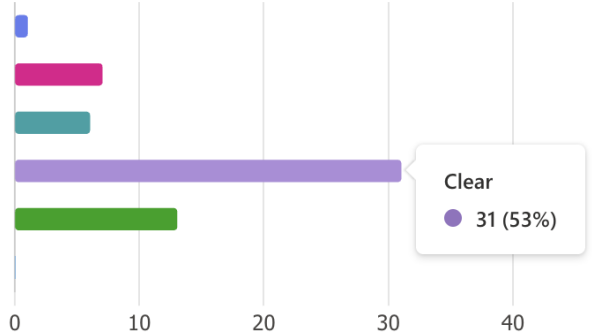
Secure Updates



2. Clarity and Understandability: How clear and easy to understand is the proposed content for this section?

More details

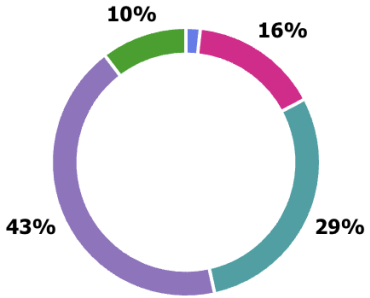
Not Clear	1
Somewhat clear	7
Neutral	6
Clear	31
Very Clear	13
Other	0



3. Practicality and Implementability: How practical and implementable do you find the requirements/guidance in this section for your organization or typical stakeholders?

More details

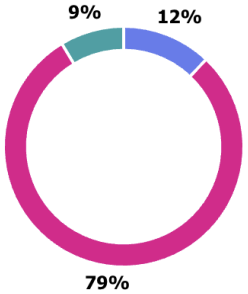
Not Practical	1
Somewhat practical	9
Neutral	17
Practical	25
Very Practical	6



4. Do you feel anything significant is missing from this section?

More details

Yes	7
No	46
Maybe	5



5. If you felt that something significant is missing please specify:

More details

8
Responses

Latest Responses

"For these requirements which will very specific to „some" products, (but not ... "

...

5 respondents (63%) answered Update for this question.

5.If you felt that something significant is missing please specify:

1	Not all products in the scope of the CRA are accessable e.g. via internet for notification. Detailed definition of how to notify user (information only on manufacturer's homepage, actively via App, direct contact to user, newsletter, social media, ...). Is a direct contact needed or is general communication sufficient?
2	Indeed silent patching of the cloud component needs to be properly covered.
3	Security Update for Offline Products
4	What about embedded products wihtout connectivity: automatic update is not possible. Moreover, in industrial context, automatic update is out of question and can be dangerous (from safety point of view) Eventually, if the secure update must be verified by the product itself or the SW in charge for the update (e.g. an embedded products with update sent by an updater via USB)
5	Examples and definition of "where applicable" for updates. Industry has lots of such cases.
6	An approach for shipping security vulnerability fixing updates to users which decide to opt out

5.If you felt that something significant is missing please specify:

7	Two things need clarifications. The first was raised also during the talk; the so-called "silent patching" practice needs clarifications; preferably, it should not be allowed without appropriate documentation. The second is the separation of security updates from functional updates. This point is important! Functional updates also may contradict other essential requirements; they often enlarge attack surfaces and bring new vulnerabilities!
8	For these requirements which will very specific to „some“ products, (but not for all) it would be great to have differentiated a little bit on really essential requirements for all products with digital elements and those which maybe need „lighter requirement“ I know that the threat model/risk assessment will provide that information, but still something to consider. Hope that the decision tree structure for harmonized standards will easily clarify such doubts.

6. Suggestions for Improvement: What specific changes or additions would you recommend for this section?

More details

4

Responses

Latest Responses

...

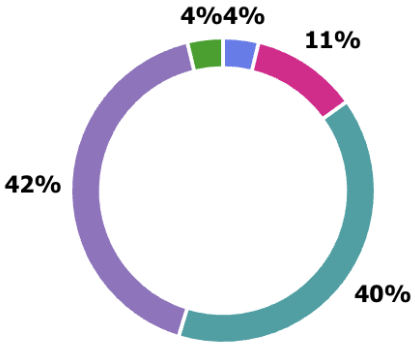
6.Suggestions for Improvement: What specific changes or additions would you recommend for this section?

1	Explanation of why SUM-4 may be required, and why SUM-3 doesn't adequately cover this already (e.g. an update scheduled under human approval)
2	I hope courses like this can be offered regularly.
3	Overview of the relatioonships of all mentioned standards
4	Does the where appropriate limit for automatic updates also cover the notification requirements?

7. In your opinion, is the proposed section proportionate to the cybersecurity risks it aims to address for organizations of all sizes, particularly Small and Medium-sized Enterprises (SMEs)?

More details

Not at all proportionate/Excessive burden	2
Somewhat disproportionate/Significant burden for SMEs	6
Neutral/Unsure	21
Somewhat proportionate/Manageable for most SMEs	22
Very proportionate/Well-adapted for SMEs	2



8. Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

More details

4

Responses

Latest Responses

...

8.Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

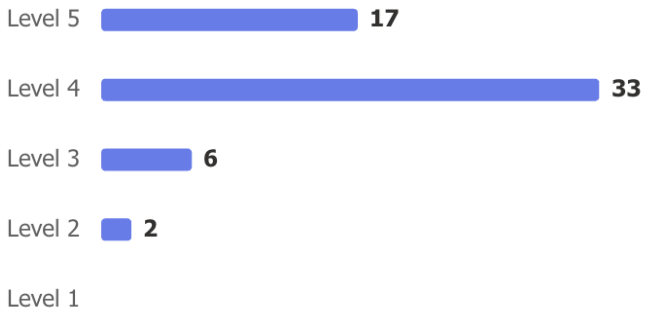
1	the amount of mechanisms are till today not so necessary for our customer domain.
2	Problems with the definition of "notification" that will cause a burden and a rebuild of a product, and there is no time from the date of the standard to be able to rebuild in time.
3	Retention of software up to 10 years requires excessive infrastructure
4	Again, already having been a part of good practices for the past twenty years or so. That said, the wide scope of the CRA may cause problems in some sectors and specialized products.

9. Overall, how satisfied are you with this section?

More details

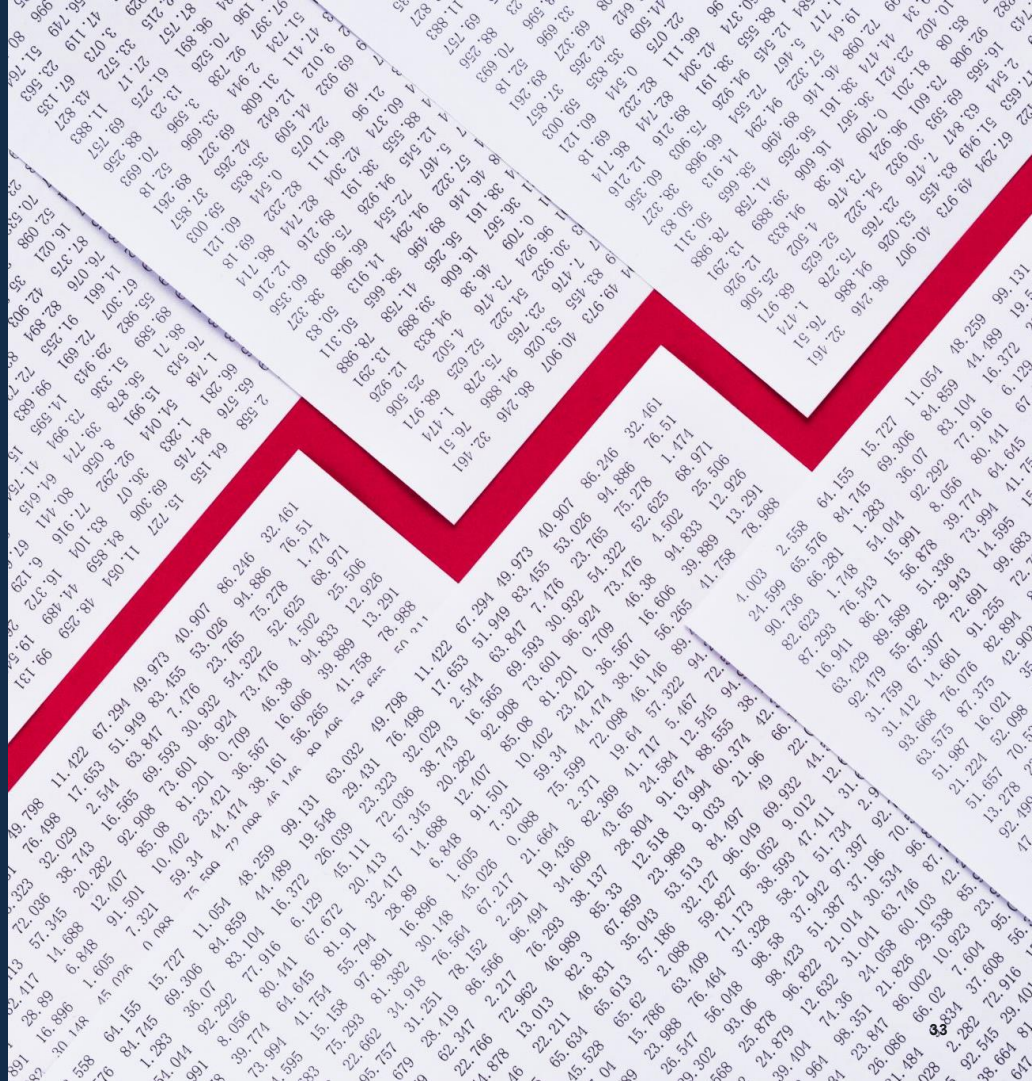
4.12

Average Rating



6.4 (d) -

Authorized access

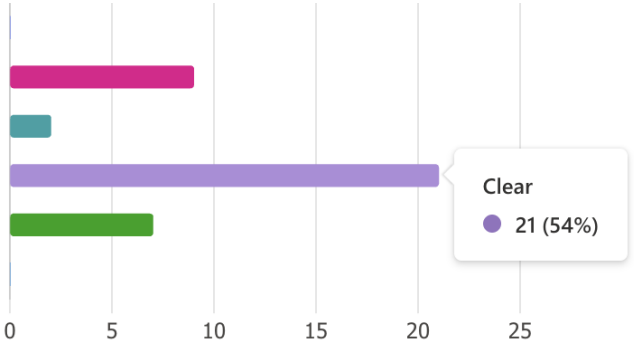


Vulnir

2. Clarity and Understandability: How clear and easy to understand is the proposed content for this section?

More details

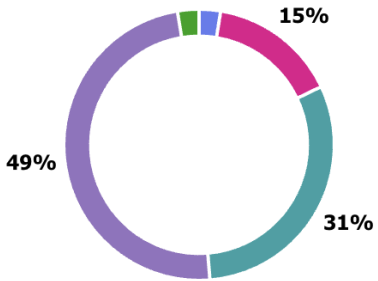
Not Clear	0
Somewhat clear	9
Neutral	2
Clear	21
Very Clear	7
Other	0



3. Practicality and Implementability: How practical and implementable do you find the requirements/guidance in this section for your organization or typical stakeholders?

More details

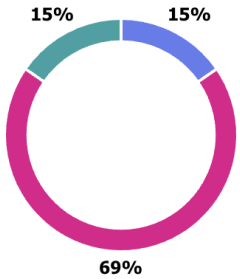
Not Practical	1
Somewhat practical	6
Neutral	12
Practical	19
Very Practical	1



4. Do you feel anything significant is missing from this section?

More details

Yes	6
No	27
Maybe	6



5. If you felt that something significant is missing please specify:

More details

8
Responses

Latest Responses
"physical control"
"Can the product delegate authentication to the OS of the PC it is installed o... "
...

3 respondents (50%) answered manufacturers for this question.

Update

5.If you felt that something significant is missing please specify:

1	more clarity on notification requirement
2	The topic is huge! In general, I'd hope to see whether the guidance is geared toward the MAC-side instead of the DAC-side.
3	Define what is meant by "Void" with regards to manufacturers that have already implemented requirements under RED and EN 18031 and now they are "void"? Is there anything to replace them?
4	You mentioned that the 18031 applicability will not be included in EN 40000-1-4. Is that not a problem with HAS since the outcome of the risk assessment will be dependant on the person
5	Clear answer on whether "report" for newly added GEC-13 is targeted at user of the product, or at the manufacturer of the product
6	Report to who? The user or the manufacturer? I see a risk that reporting only to the user can fall into the weeds. But how can a product report to the manufacturer if it’s not online?

5.If you felt that something significant is missing please specify:

7	Can the product delegate authentication to the OS of the PC it is installed on (e.g. Windows login)
8	physical control

6. Suggestions for Improvement: What specific changes or additions would you recommend for this section? More details

5
Responses

Latest Responses

"Describe physical control as one of the authorized access controls"

"In the standard, specify if access control apply to human and/or machine-to-..."

"Great to see that the "applicability" requirements from EN18031 will be drop..."

...

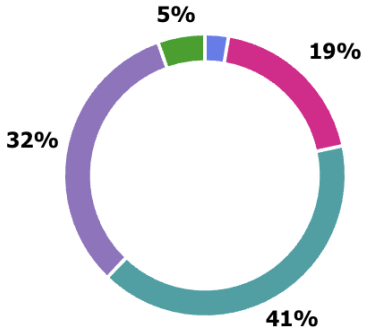
6.Suggestions for Improvement: What specific changes or additions would you recommend for this section?

1	more clarity on notification requirement
2	add information to FAQ for which product types certain mechanisms are probably not applicable
3	Great to see that the "applicability" requirements from EN18031 will be dropped and replaced by Risk Assessment.
4	In the standard, specify if access control apply to human and/or machine-to-machine access
5	Describe physical control as one of the authorized access controls

7. In your opinion, is the proposed section proportionate to the cybersecurity risks it aims to address for organizations of all sizes, particularly Small and Medium-sized Enterprises (SMEs)?

More details

Not at all proportionate/Excessive burden	1
Somewhat disproportionate/Significant burden for SMEs	7
Neutral/Unsure	15
Somewhat proportionate/Manageable for most SMEs	12
Very proportionate/Well-adapted for SMEs	2



8. Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

More details

3

Responses

Latest Responses

"The risk assessment process will make it hard for engineers without any kno... "

8.Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

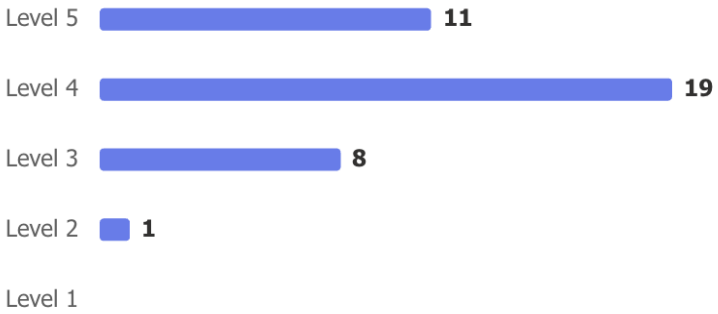
1	our products do not have architectures supporting such mechanisms. Still we have to do something. This causes likely a lot of redesign efforts.
2	Not clear if we can still make use of generic users to authenticate to a device
3	The risk assessment process will make it hard for engineers without any knowledge about security an risks. Hard requirements like the mentioned "applicable" requirements make it way easier but it resulted in a lot of problems for manufacturers to be compliant. Because in a lot of cases, they did not make sense! Really like it, thanks!

9. Overall, how satisfied are you with this section?

More details

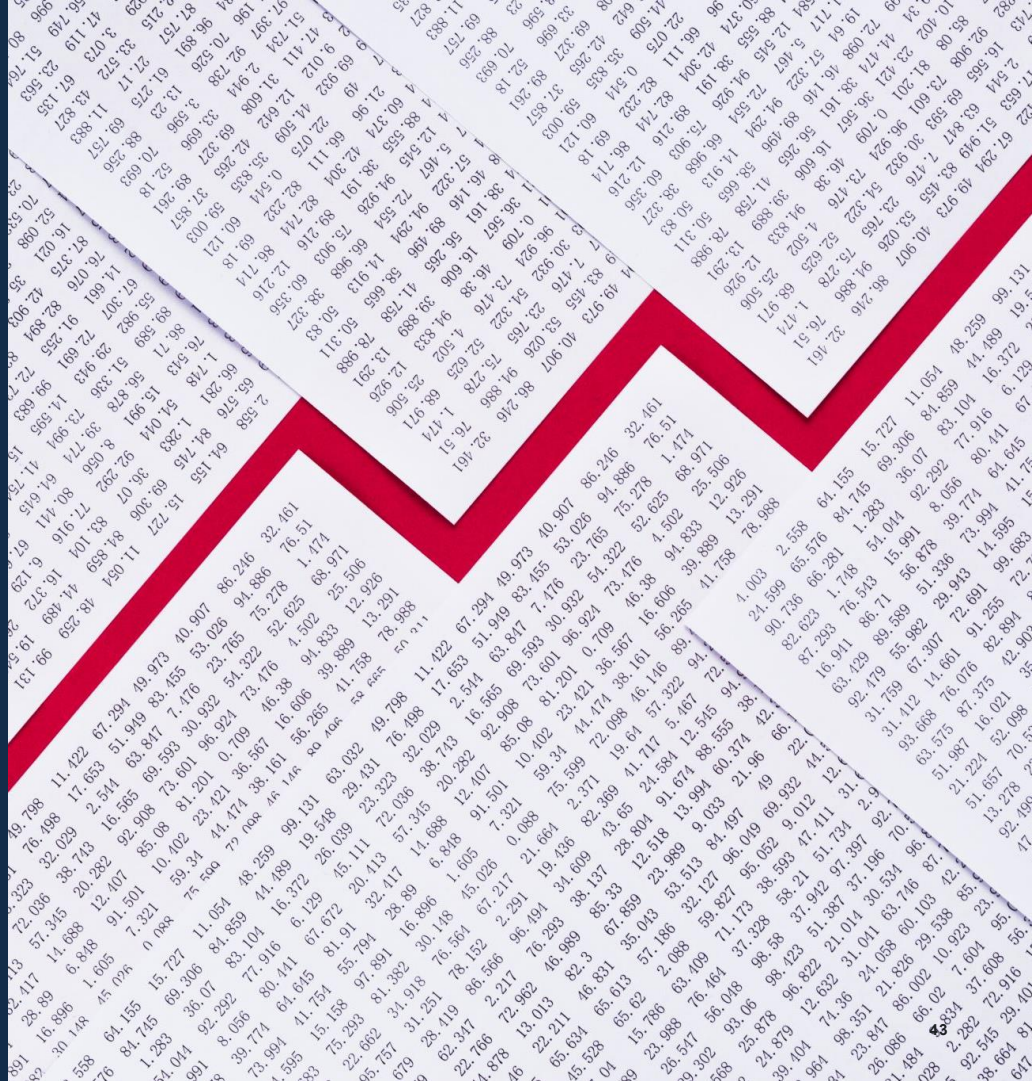
4.03

Average Rating



6.5 (e) -

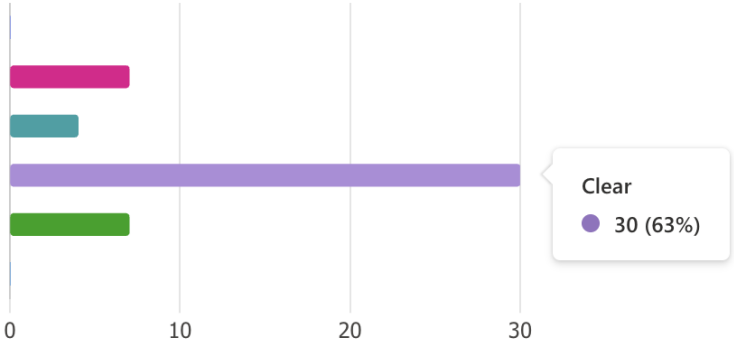
Confidentiality (Disclosure)



2. Clarity and Understandability: How clear and easy to understand is the proposed content for this section?

More details

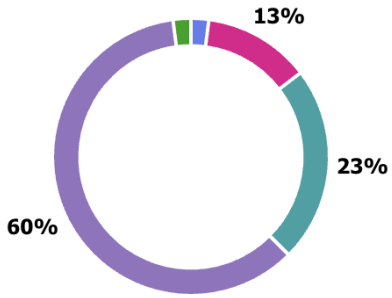
Not Clear	0
Somewhat clear	7
Neutral	4
Clear	30
Very Clear	7
Other	0



3. Practicality and Implementability: How practical and implementable do you find the requirements/guidance in this section for your organization or typical stakeholders?

More details

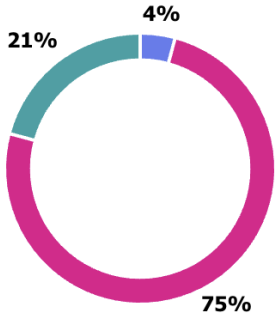
Not Practical	1
Somewhat practical	6
Neutral	11
Practical	29
Very Practical	1



4. Do you feel anything significant is missing from this section?

More details

Yes	2
No	36
Maybe	10



5. If you felt that something significant is missing please specify:

More details

7
Responses

Latest Responses
"Several concept for confidentiality: Personal data / Know how of the compan..."
...

3 respondents (43%) answered data for this question.

5.If you felt that something significant is missing please specify:

1	So do I get it right, that noch every "applicable" requirement will be dropped and replaced by risk assessment? Where do you draw the line?
2	I think this is missing / or too much of what is asked: - there are product types which have only one way to get connected, e.g. sensor / controller combinations. These interfaces are proprietary in digital, mechanical and electrical way. It is not much benefit to encrypt such communication, as, if an attack is successful, it will be on the controller side (as this has e.g. LAN of Wifi). Also note that e.g. Hach products (and for sure many competitor products as well) are >95% installed in OT with non-digital communication (mA output) to SCADA systems. Waste water plants are critical infrastructure and therefore configure their products often very conservatively. So the FAQ needs to show ways out of this. Companies will have to encrypt protocols of many products without much benefit other than being clean for an audit. For security, the win is low to zero. The same topic is for many OT protocols, Modbus RTU, Profibus etc - they are all not encrypted as per their own industry standard.
3	The topic is again huge; in a sense, the CIA triad covers all of the essential cyber security requirements. Of course, it needs to be there, but best (vertical) practices are difficult to derive. The guidance on crypto was good in this regard!
4	Handling the "remote data processing", Most remote data processing is managed following ISO 27001 and this is missing.

5.If you felt that something significant is missing please specify:

5	Difficult to map what encryption algorithm (strength) should be used for what type of data, will depend on the risk assessment, but very subjective.
6	Clear indication if a requirement is valid for Default, Important or Critical.
7	Several concept for confidentiality: Personal data / Know how of the company / risk related to competitors or external intelligence with bad intention...

6. Suggestions for Improvement: What specific changes or additions would you recommend for this section?

More details

2

Responses

Latest Responses

"too close of the regulation maybe"

...

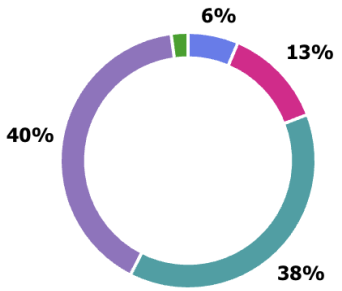
6.Suggestions for Improvement: What specific changes or additions would you recommend for this section?

1	no
2	too close of the regulation maybe

7. In your opinion, is the proposed section proportionate to the cybersecurity risks it aims to address for organizations of all sizes, particularly Small and Medium-sized Enterprises (SMEs)?

More details

Not at all proportionate/Excessive burden	3
Somewhat disproportionate/Significant burden for SMEs	6
Neutral/Unsure	18
Somewhat proportionate/Manageable for most SMEs	19
Very proportionate/Well-adapted for SMEs	1



8. Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

More details

5
Responses

Latest Responses

"Require HW witht crypto accelerators for acceptable performance: not realis... "

...

3 respondents (60%) answered products for this question.

8.Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

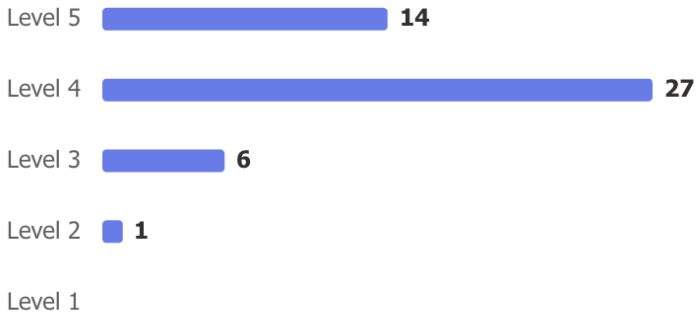
1	ENISA ACM could kill "average" hardware and coders
2	too high impact to products of certain types, see explanation above.
3	While I see that is feasible to protect certain data, it seems very hard to protect all data processed
4	Small companies have no knowledge of the encryption used in the services and servers that they employ for the remote data processing. This is also for software products (apps, and deployed software) where the SME simply follows the best practices as given by the plaform and the IDE.
5	Require HW witht crypto accelerators for acceptable performance: not realistic for small embedded IoT devices. Also not possible for old legacy products (this comment is probably not relevant regarding CRA goals, but note that it has large business impact for some EU companies)

9. Overall, how satisfied are you with this section?

More details

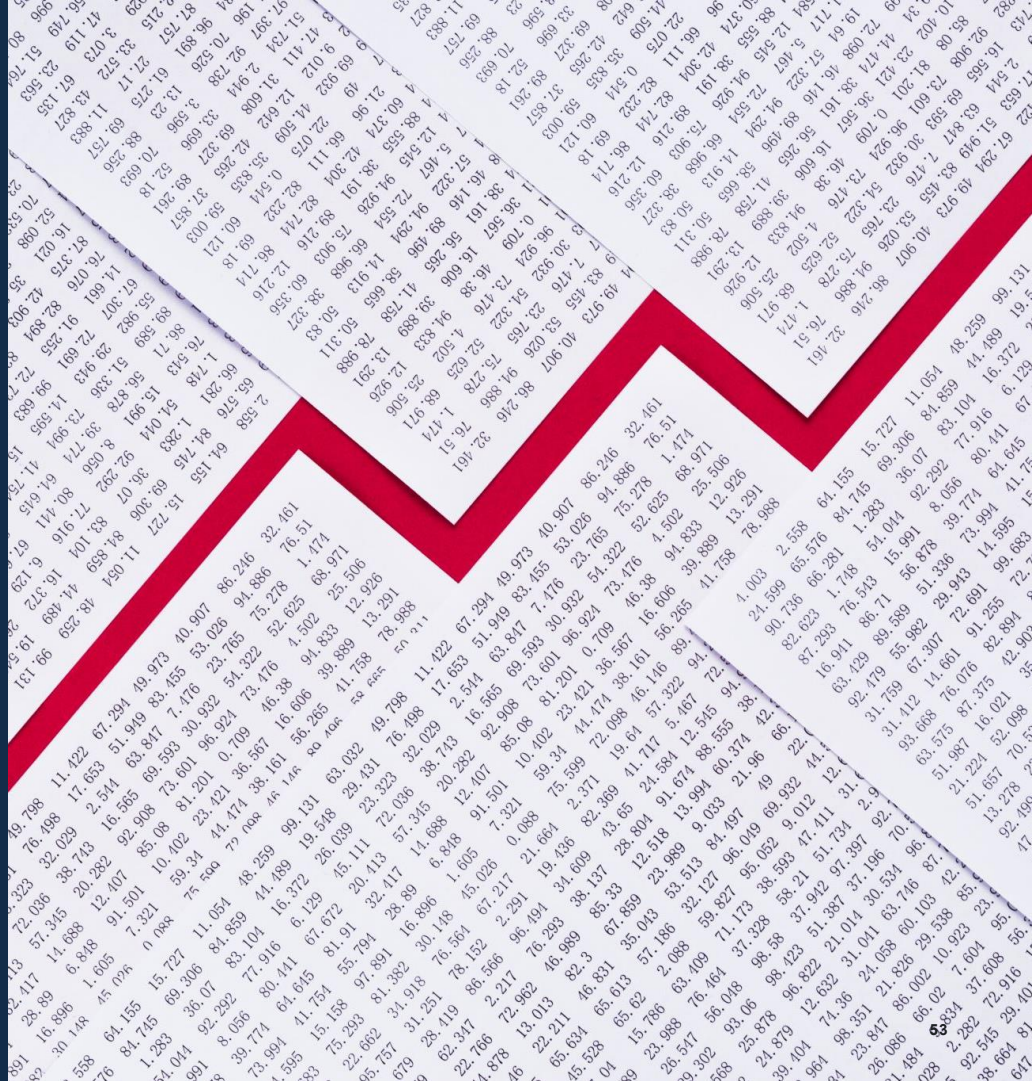
4.13

Average Rating



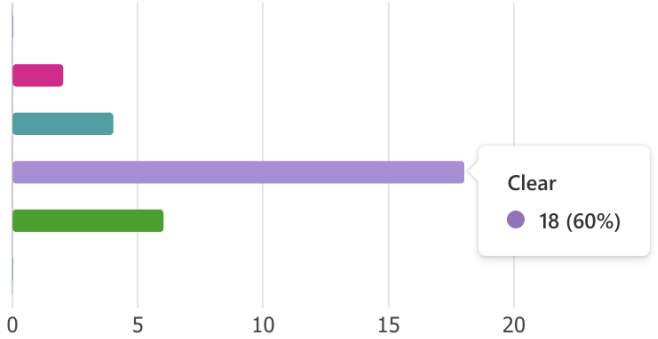
6.6 (f) -

Integrity (Tampering)



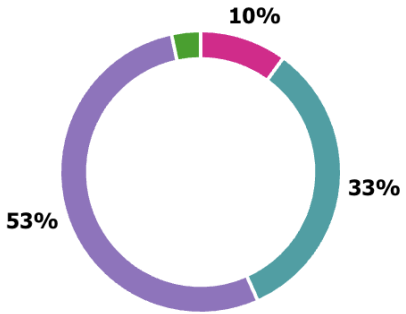
2. Clarity and Understandability: How clear and easy to understand is the proposed content for this section? More details

Not Clear	0
Somewhat clear	2
Neutral	4
Clear	18
Very Clear	6
Other	0



3. Practicality and Implementability: How practical and implementable do you find the requirements/guidance in this section for your organization or typical stakeholders? More details

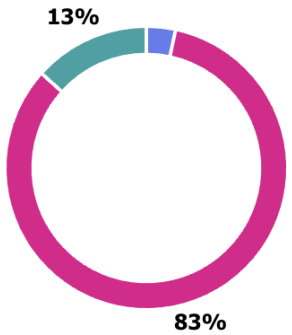
Not Practical	0
Somewhat practical	3
Neutral	10
Practical	16
Very Practical	1



4. Do you feel anything significant is missing from this section?

More details

Yes	1
No	25
Maybe	4



5. If you felt that something significant is missing please specify:

More details

2

Responses

Latest Responses

...

5.If you felt that something significant is missing please specify:

1	more clarity / specifics

6. Suggestions for Improvement: What specific changes or additions would you recommend for this section?

More details

2

Responses

Latest Responses

""

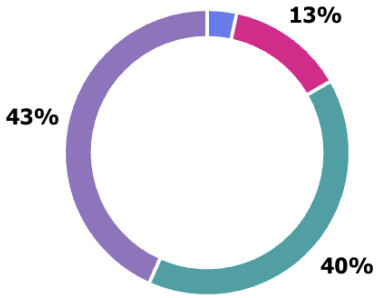
...

6.Suggestions for Improvement: What specific changes or additions would you recommend for this section?

1	more clarity / specifics

7. In your opinion, is the proposed section proportionate to the cybersecurity risks it aims to address for organizations of all sizes, particularly Small and Medium-sized Enterprises (SMEs)? More details

Not at all proportionate/Excessive burden	1
Somewhat disproportionate/Significant burden for SMEs	4
Neutral/Unsure	12
Somewhat proportionate/Manageable for most SMEs	13
Very proportionate/Well-adapted for SMEs	0



8. Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME: More details

1
Responses

Latest Responses

"I understand logfiles are also data at rest, and they are as a file exported e.g.... "

8.Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

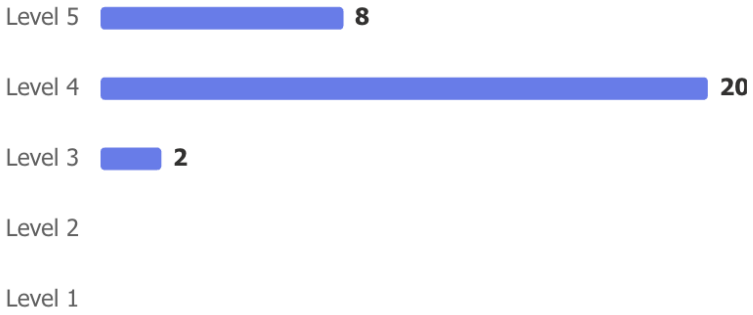
1	I understand logfiles are also data at rest, and they are as a file exported e.g. through USB and the user processes this on e.g. PC. In our products, we would have to add integrity checks in a tool chain and add properties to support these checks. The source of those files though is unlikely to be the source of an attack.

9. Overall, how satisfied are you with this section?

More details

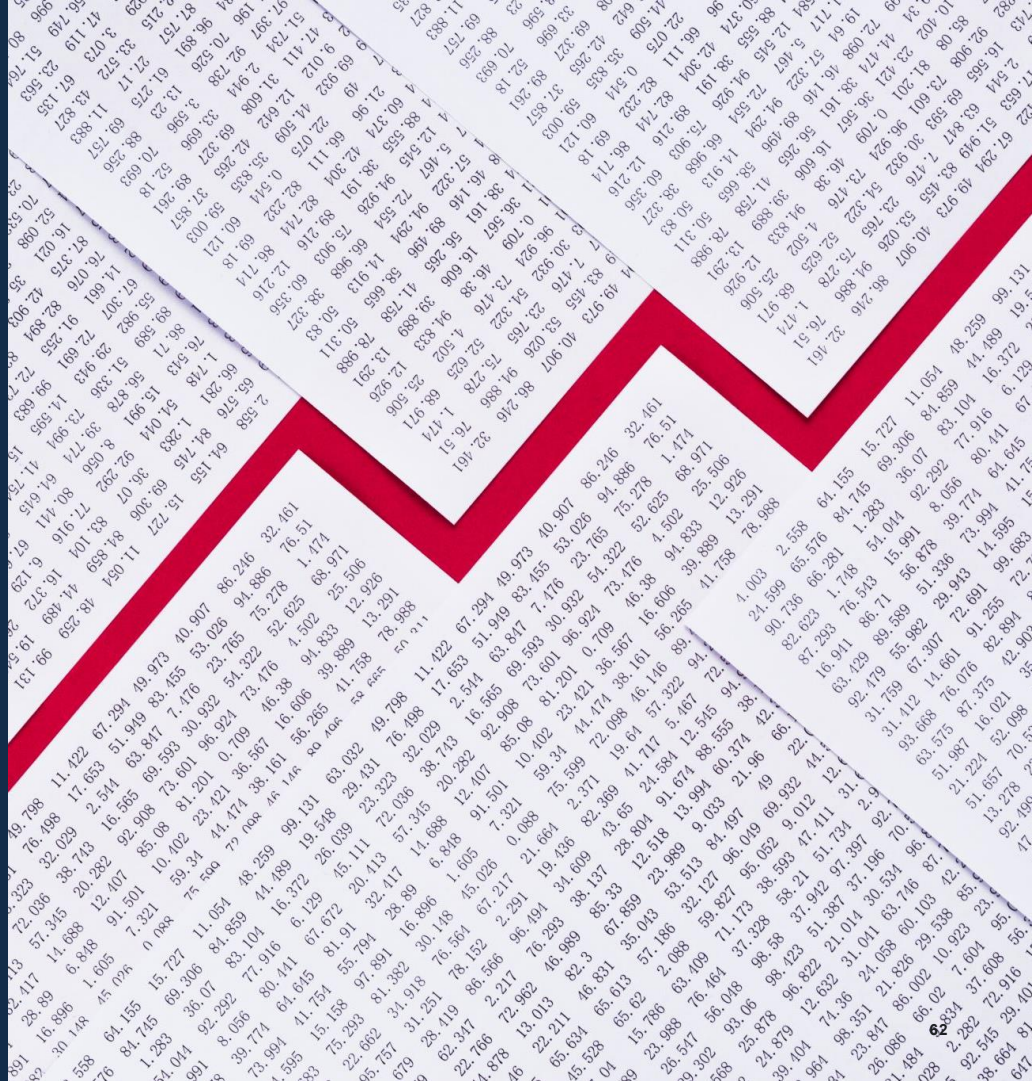
4.20

Average Rating



6.7 (g) -

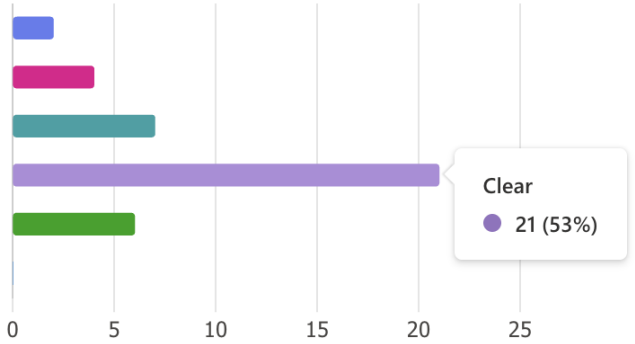
Data minimization



Vulnir

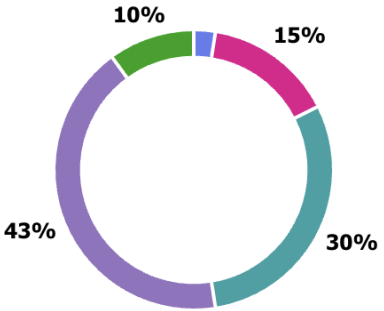
2. Clarity and Understandability: How clear and easy to understand is the proposed content for this section? More detai

Not Clear	2
Somewhat clear	4
Neutral	7
Clear	21
Very Clear	6
Other	0



3. Practicality and Implementability: How practical and implementable do you find the requirements/guidance in this section for your organization or typical stakeholders? More details

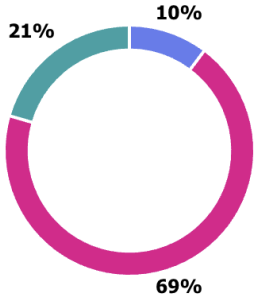
Not Practical	1
Somewhat practical	6
Neutral	12
Practical	17
Very Practical	4



4. Do you feel anything significant is missing from this section?

More details

Yes	4
No	27
Maybe	8



5. If you felt that something significant is missing please specify:

More details

8
Responses

Latest Responses

"The talk was good; it is indeed a new requirement in the security realm, alth... "

"In fact, this a "merge" between GDPR and Data Act. These regulations impos... "

...

5 respondents (63%) answered data for this question.

5.If you felt that something significant is missing please specify:

1	What about data which is not directly used for intended purpose of the product but e.g. for service or data for product/ use case optimization?
2	more clarity on what information is necessary - currently very vague
3	Link with Data Act (obligation to share data with users and recipients except for some good reasons such as security).
4	Does not seem to apply to IIOT device
5	The secure development lifecycle process is somehow touching the topic (not specific but with secure by design, threat model and minimization of unneeded communication paths)
6	how to make the effort for this appropriate to the risk and not do ways to much effort, for people not familiar with what data protection intends
7	In fact, this a "merge" between GDPR and Data Act. These regulations impose already, data classification, lifecycle and user request and user consent... Normally, already covered
8	The talk was good; it is indeed a new requirement in the security realm, although from the GDPR enforcement perspective we know that it is continuously violated with respect to personal data. Therefore, some practical guidance would be beneficial.

6. Suggestions for Improvement: What specific changes or additions would you recommend for this section?

More details

6

Responses

Latest Responses

"I think clarifying (a) opt-in versus opt-out (by default) would be a good thing..."

"Make a deeper link to GDPR and Data Act"

...

2 respondents (33%) answered Data for this question.

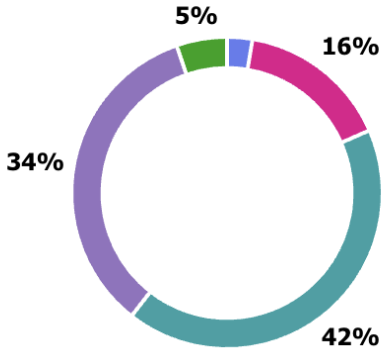
6.Suggestions for Improvement: What specific changes or additions would you recommend for this section?

1	more clarity on what information is necessary - currently very vague
2	Data act link
3	Perhaps relate to ISO 27001
4	practical help for keeping the efforts within bounds
5	Make a deeper link to GDPR and Data Act
6	I think clarifying (a) opt-in versus opt-out (by default) would be a good thing. In addition, (b) some practical examples would be beneficial regarding potential conflicts with the other essential requirements. For instance, if a vendor says that they do zero trust, they could collect basically everything on that basis, regardless whether it would violate the data minimization requirement. It would be good to know whether (c) transparency, traceability, and documentation is required for users too.

7. In your opinion, is the proposed section proportionate to the cybersecurity risks it aims to address for organizations of all sizes, particularly Small and Medium-sized Enterprises (SMEs)?

More details

Not at all proportionate/Excessive burden	1
Somewhat disproportionate/Significant burden for SMEs	6
Neutral/Unsure	16
Somewhat proportionate/Manageable for most SMEs	13
Very proportionate/Well-adapted for SMEs	2



8. Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

More details

3

Responses

Latest Responses

"We consider the telemetry data non-personal (it's from the equipment of th... "

. . .

8.Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

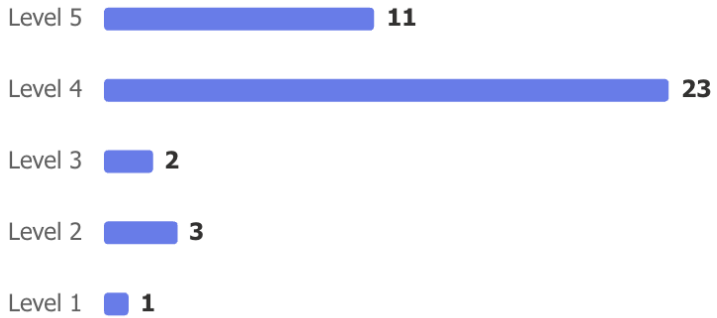
1	IIOT does not seem to apply
2	inexperience with GDPR for non-PII, and how to keep this within appropriate efforts
3	We consider the telemetry data non-personal (it's from the equipment of the customer though) and we keep it forever for machine maintenance. There is no clear statement that justifies that this is legitimate way to deal with this data.

9. Overall, how satisfied are you with this section?

More details

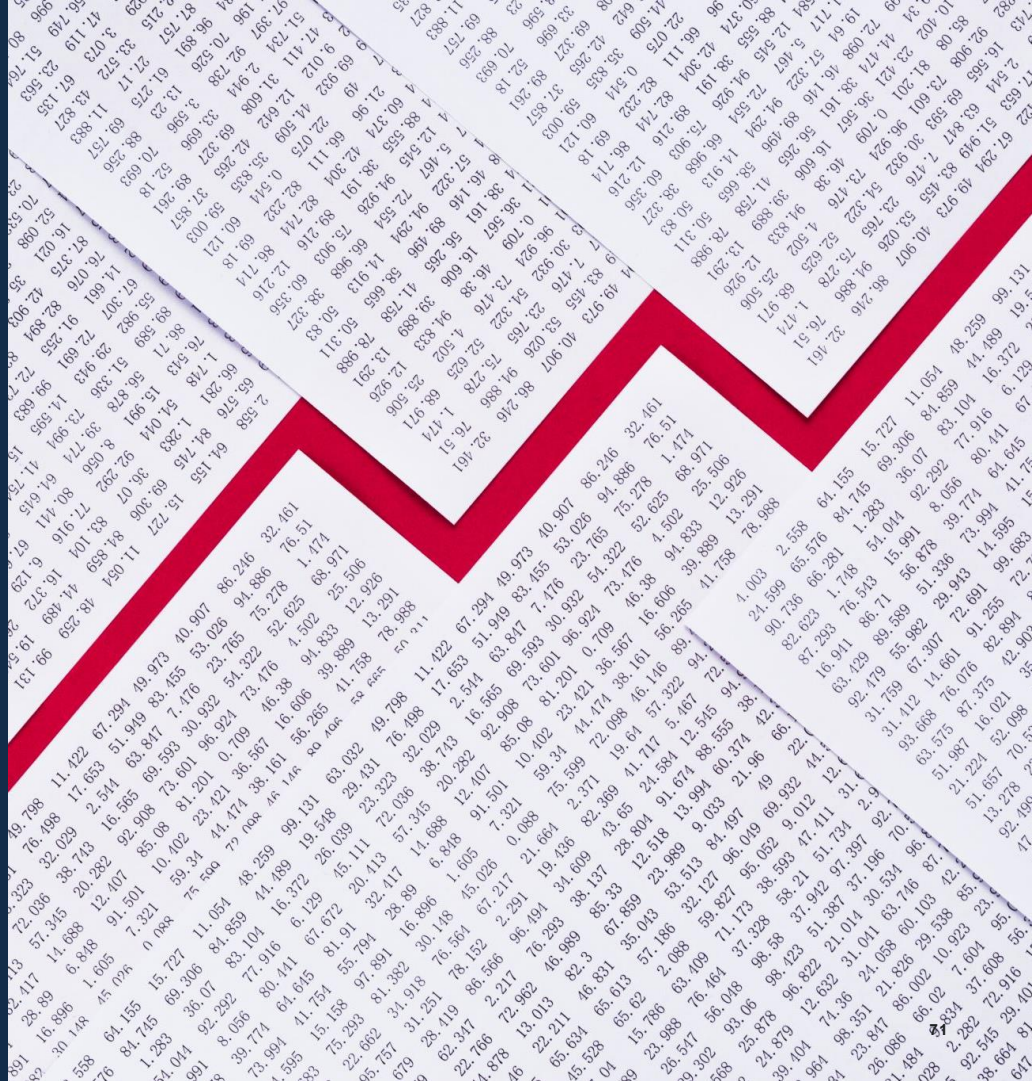
4.00

Average Rating



6.8 (h) -

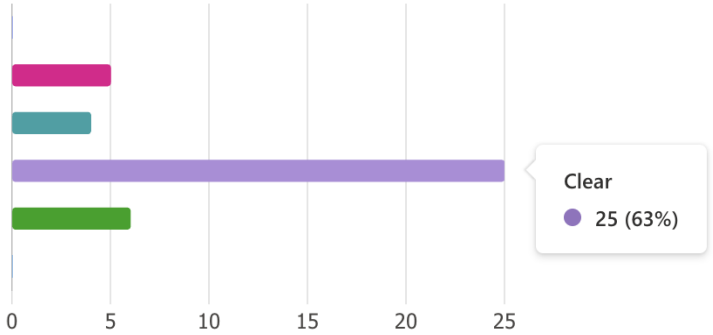
Availability



2. Clarity and Understandability: How clear and easy to understand is the proposed content for this section?

More details

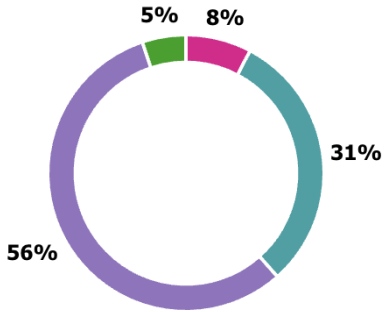
Not Clear	0
Somewhat clear	5
Neutral	4
Clear	25
Very Clear	6
Other	0



3. Practicality and Implementability: How practical and implementable do you find the requirements/guidance in this section for your organization or typical stakeholders?

More details

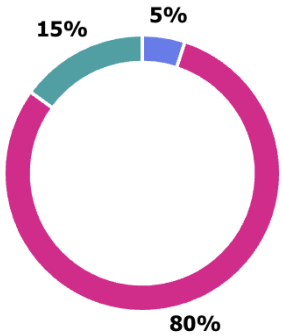
Not Practical	0
Somewhat practical	3
Neutral	12
Practical	22
Very Practical	2



4. Do you feel anything significant is missing from this section?

More details

Yes	2
No	32
Maybe	6



5. If you felt that something significant is missing please specify:

More details

2

Responses

Latest Responses

...

5.If you felt that something significant is missing please specify:

1	Need more clarity on resilience standard
2	Backup and Restore, geo-locations for backup

6. Suggestions for Improvement: What specific changes or additions would you recommend for this section?

More details

1

Responses

Latest Responses

...

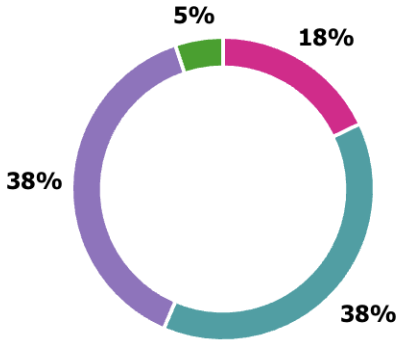
6.Suggestions for Improvement: What specific changes or additions would you recommend for this section?

1	Need more clarity on resilience standard

7. In your opinion, is the proposed section proportionate to the cybersecurity risks it aims to address for organizations of all sizes, particularly Small and Medium-sized Enterprises (SMEs)?

More details

Not at all proportionate/Excessive burden	0
Somewhat disproportionate/Significant burden for SMEs	7
Neutral/Unsure	15
Somewhat proportionate/Manageable for most SMEs	15
Very proportionate/Well-adapted for SMEs	2



8. Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

More details

1

Responses

Latest Responses

...

8.Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

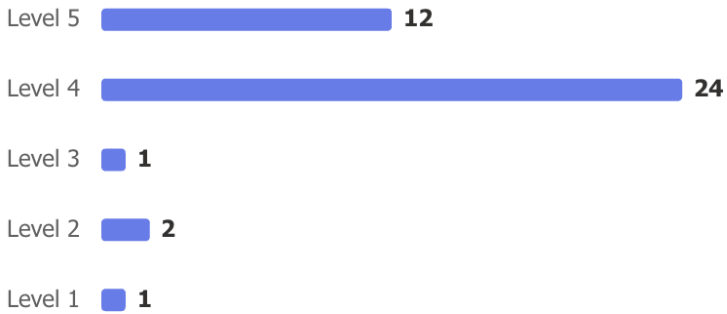
1	Great clarification!

9. Overall, how satisfied are you with this section?

More details

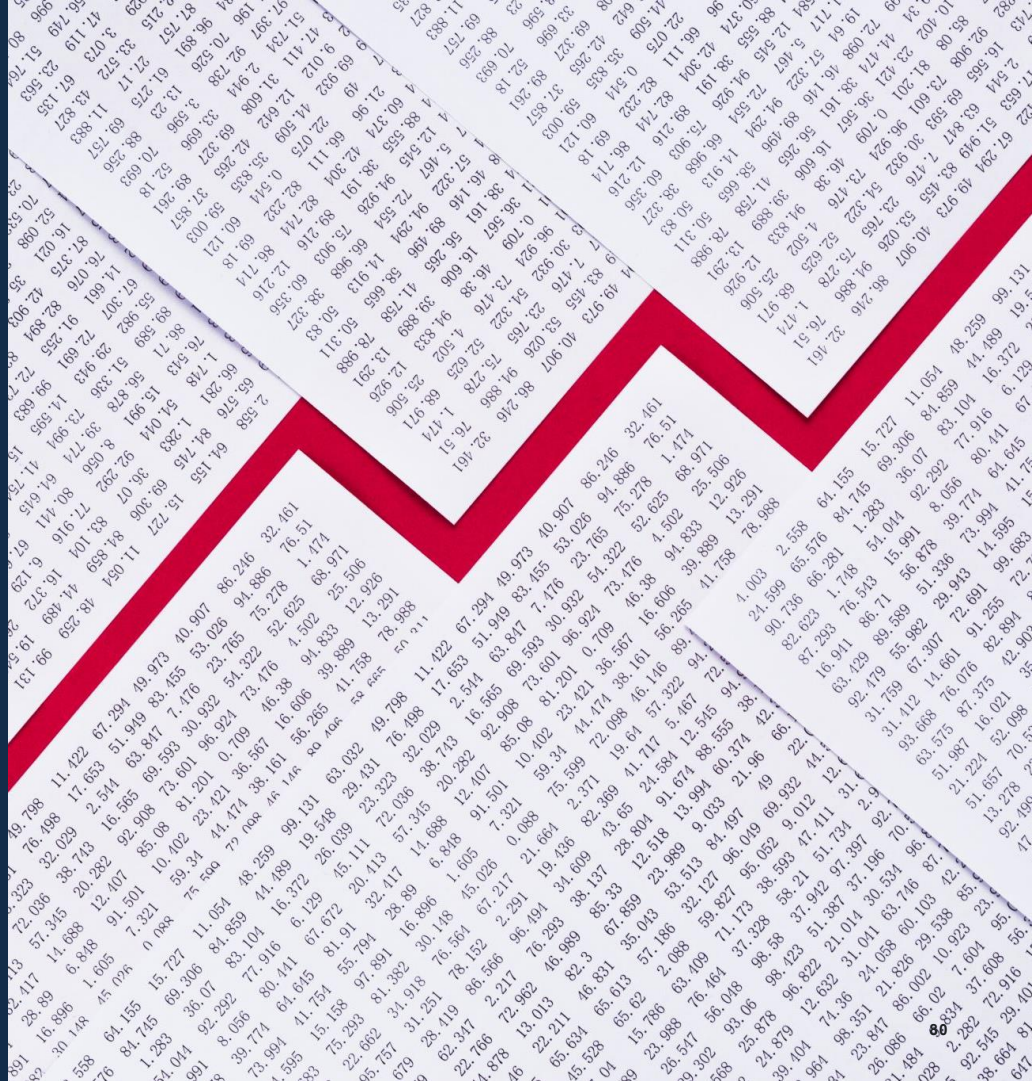
4.10

Average Rating



6.9 (i) -

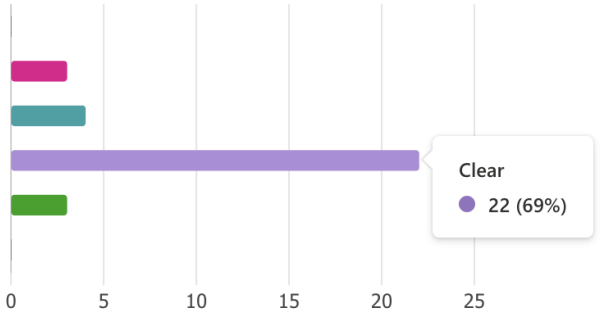
Minimize negative impact (External impact)



2. Clarity and Understandability: How clear and easy to understand is the proposed content for this section?

More details

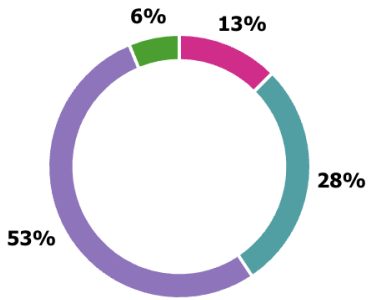
Not Clear	0
Somewhat clear	3
Neutral	4
Clear	22
Very Clear	3
Other	0



3. Practicality and Implementability: How practical and implementable do you find the requirements/guidance in this section for your organization or typical stakeholders?

More details

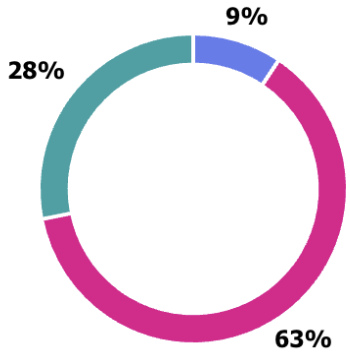
Not Practical	0
Somewhat practical	4
Neutral	9
Practical	17
Very Practical	2



4. Do you feel anything significant is missing from this section?

More details

Yes	3
No	20
Maybe	9



5. If you felt that something significant is missing please specify:

More details

4

Responses

Latest Responses

"I feel there is still some clarification to be provided on limitations of manufac..."

"This is very challenging requirement since it cannot be transparent what is ef..."

...

5.If you felt that something significant is missing please specify:

1	How to evaluate negative impact - what standard is applied - too vague.
2	independence from qty classification at CRA core text
3	This is very challenging requirement since it cannot be transparent what is effective
4	I feel there is still some clarification to be provided on limitations of manufacturer responsibility for adjacent systems.

6. Suggestions for Improvement: What specific changes or additions would you recommend for this section? More details

4
Responses

Latest Responses

"The talk was good; similar examples would be good for the standard too. As... "

...

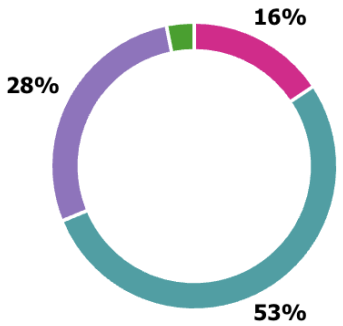
6.Suggestions for Improvement: What specific changes or additions would you recommend for this section?

1	no
2	How to evaluate negative impact - what standard is applied - too vague.
3	further specify API security control (SBOM to include API directory?)
4	The talk was good; similar examples would be good for the standard too. As a legal requirement, attack propagation minimization is quite new too (but very much needed!). It is also a relevant research topic, which further underlines the newness of the topic (incl. w.r.t. best practices).

7. In your opinion, is the proposed section proportionate to the cybersecurity risks it aims to address for organizations of all sizes, particularly Small and Medium-sized Enterprises (SMEs)?

More details

Not at all proportionate/Excessive burden	0
Somewhat disproportionate/Significant burden for SMEs	5
Neutral/Unsure	17
Somewhat proportionate/Manageable for most SMEs	9
Very proportionate/Well-adapted for SMEs	1



8. Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

0 responses submitted

0

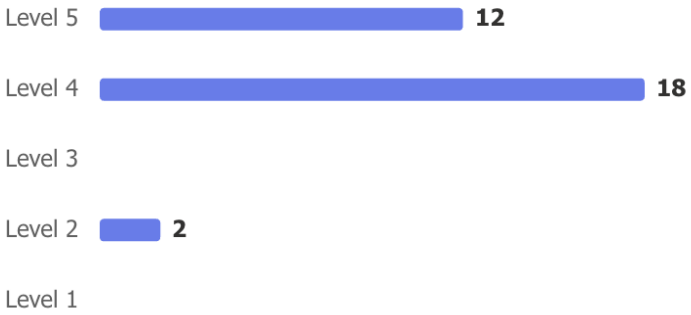
Responses

9. Overall, how satisfied are you with this section?

More details

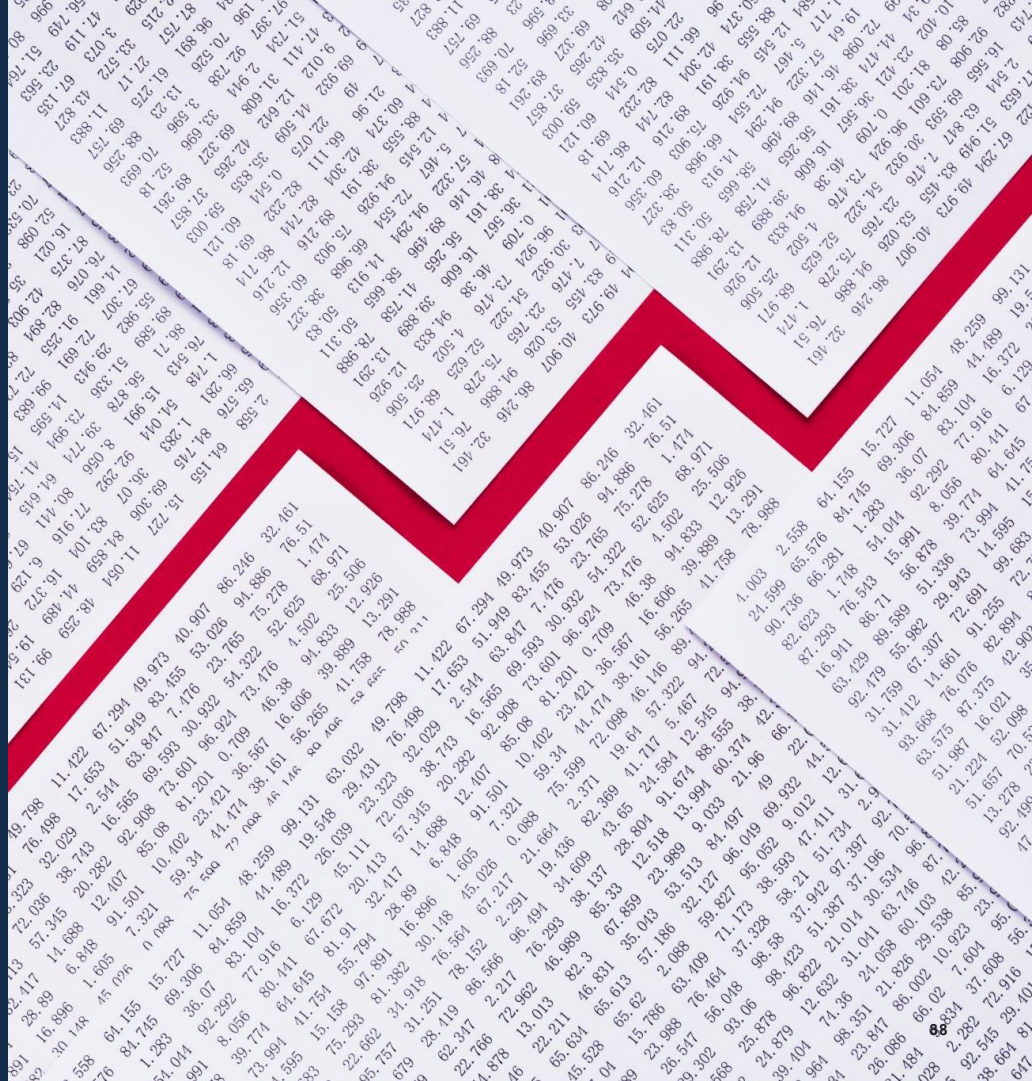
4.25

Average Rating



6.10 (j) -

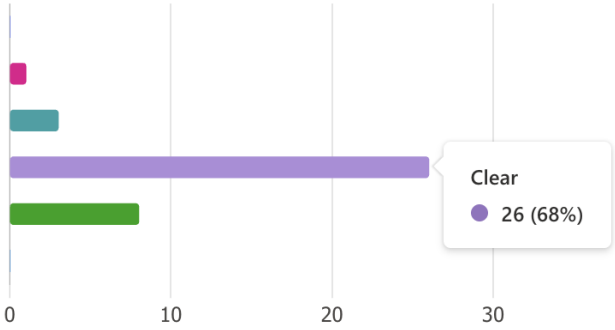
Attack Surface Minimization



2. Clarity and Understandability: How clear and easy to understand is the proposed content for this section?

More details

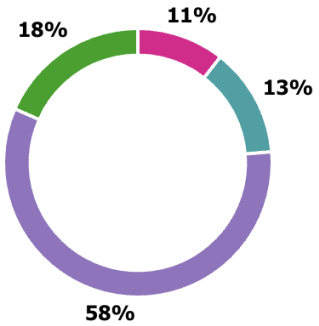
Not Clear	0
Somewhat clear	1
Neutral	3
Clear	26
Very Clear	8
Other	0



3. Practicality and Implementability: How practical and implementable do you find the requirements/guidance in this section for your organization or typical stakeholders?

More details

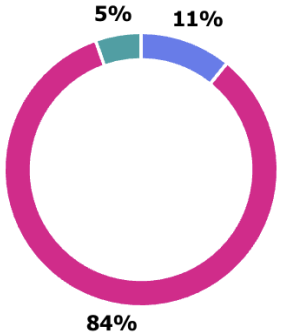
Not Practical	0
Somewhat practical	4
Neutral	5
Practical	22
Very Practical	7



4. Do you feel anything significant is missing from this section?

More details

Yes	4
No	31
Maybe	2



5. If you felt that something significant is missing please specify:

More details

6
Responses

Latest Responses

"A few further examples might clarify things a little more; now the focus was l..."

"For mobile code such as plugins: need also to consider integrity digest and/... "

5.If you felt that something significant is missing please specify:

1	Missing ref to CIS
2	More clarity on expectations / standard
3	Definition of "external/exposed interface". In industrial control systems there are lot of interfaces. Some of those are in "isolated network" and some interfaces are exposed to 3rd party products. Clarify those.
4	Guidance how to handle secure and unsecure protocol versions, which are not state of the art, dependent on the risk in operational environment. CIP Security / Profinet Class 3.
5	For mobile code such as plugins: need also to consider integrity digest and/or signature.
6	A few further examples might clarify things a little more; now the focus was largely on external interfaces, including network interfaces in particular.

6. Suggestions for Improvement: What specific changes or additions would you recommend for this section?

More details

2

Responses

Latest Responses

...

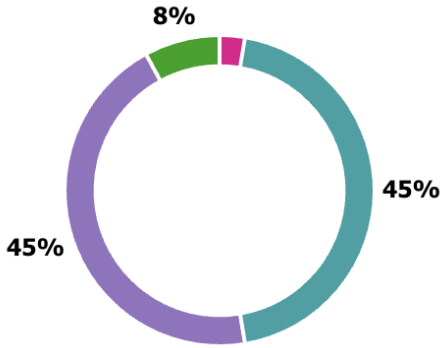
6.Suggestions for Improvement: What specific changes or additions would you recommend for this section?

1	no
2	More clarity on expectations / standard

7. In your opinion, is the proposed section proportionate to the cybersecurity risks it aims to address for organizations of all sizes, particularly Small and Medium-sized Enterprises (SMEs)?

More details

Not at all proportionate/Excessive burden	0
Somewhat disproportionate/Significant burden for SMEs	1
Neutral/Unsure	17
Somewhat proportionate/Manageable for most SMEs	17
Very proportionate/Well-adapted for SMEs	3



8. Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

More details

2

Responses

Latest Responses

"Has already been a part of good practices for the past 20-30 years."

"Technical controls / requirements are not clear here: this section is too broad..."

8.Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

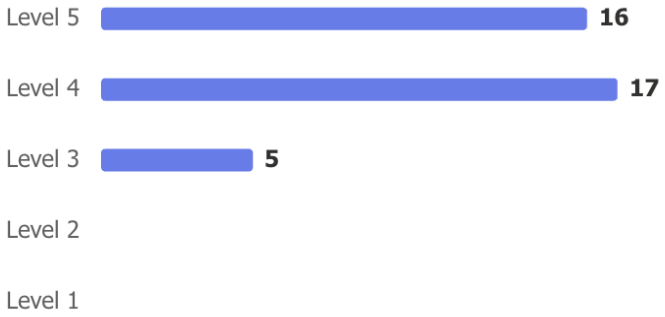
1	Technical controls / requirements are not clear here: this section is too broad and impact many aspects of product design
2	Has already been a part of good practices for the past 20-30 years.

9. Overall, how satisfied are you with this section?

More details

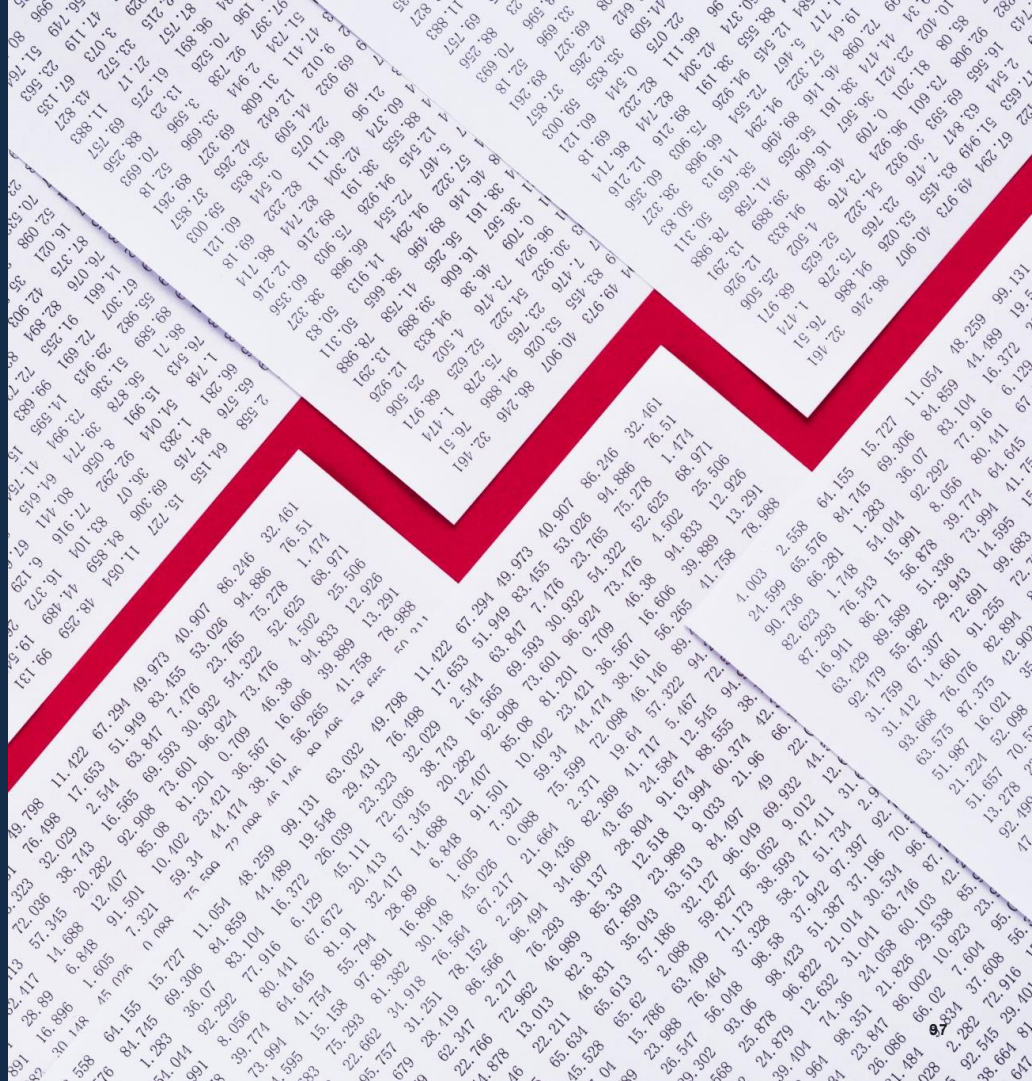
4.29

Average Rating



6.11 (k) -

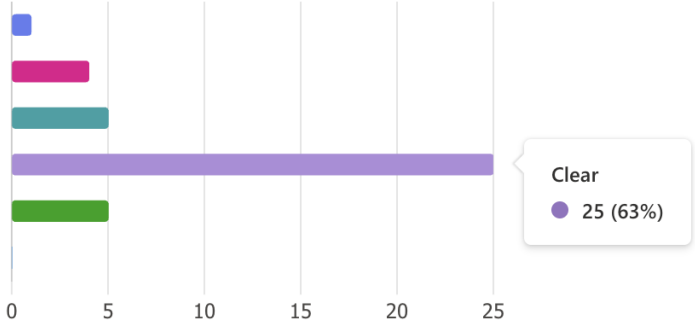
Incident impact reduction (Impact of incident)



2. Clarity and Understandability: How clear and easy to understand is the proposed content for this section?

More details

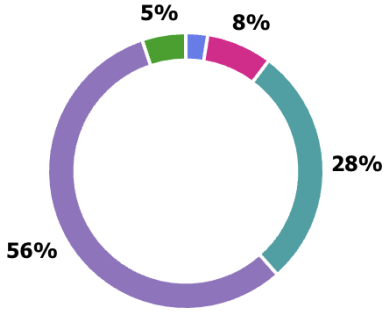
Not Clear	1
Somewhat clear	4
Neutral	5
Clear	25
Very Clear	5
Other	0



3. Practicality and Implementability: How practical and implementable do you find the requirements/guidance in this section for your organization or typical stakeholders?

More details

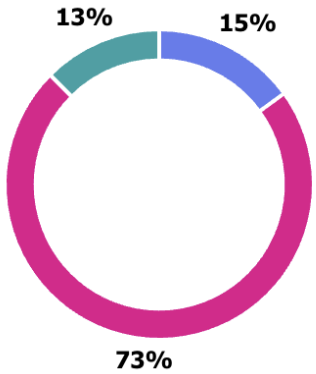
Not Practical	1
Somewhat practical	3
Neutral	11
Practical	22
Very Practical	2



4. Do you feel anything significant is missing from this section?

More details

Yes	6
No	29
Maybe	5



5. If you felt that something significant is missing please specify:

More details

5

Responses

Latest Responses

"The CRA is MUCH wider than just IOT devices and the scope of 62443 indust..."

"IPS, firewall data rate limitation, firewall IP "not allowed" lists and other IT te... "

...

5.If you felt that something significant is missing please specify:

1	This seems like quite an ill-defined requirement - it will be a challenge for anyone to assess a product and reach a pass/fail decision (based solely on what has been presented today, anyway).
2	Mechanisms to reassess hardening measures are still in place
3	It is difficult to know what is enough for compliance with this requirement.
4	IPS, firewall data rate limitation, firewall IP "not allowed" lists and other IT techniques for network attacks mitigation
5	The CRA is MUCH wider than just IOT devices and the scope of 62443 industrial control devices. The discussing is far too focused on these devices. Migitations such as ASLR are NOT relevant for software products that run on commercial operating systems and not relevant for real-time operating systems. Recommend to take this up.

6. Suggestions for Improvement: What specific changes or additions would you recommend for this section?

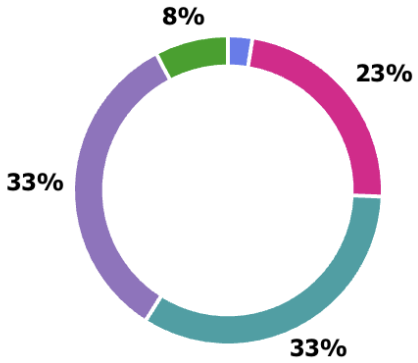
0
Responses

0 responses submitted

7. In your opinion, is the proposed section proportionate to the cybersecurity risks it aims to address for organizations of all sizes, particularly Small and Medium-sized Enterprises (SMEs)?

More details

Not at all proportionate/Excessive burden	1
Somewhat disproportionate/Significant burden for SMEs	9
Neutral/Unsure	13
Somewhat proportionate/Manageable for most SMEs	13
Very proportionate/Well-adapted for SMEs	3



8. Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

More details

1

Responses

Latest Responses

"Lots of confusion as to how to implement. Worried that it will take years to f... "

8.Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

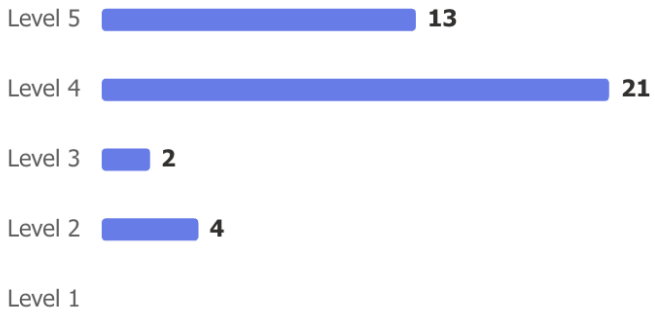
1	Lots of confusion as to how to implement. Worried that it will take years to fully understand.

9. Overall, how satisfied are you with this section?

More details

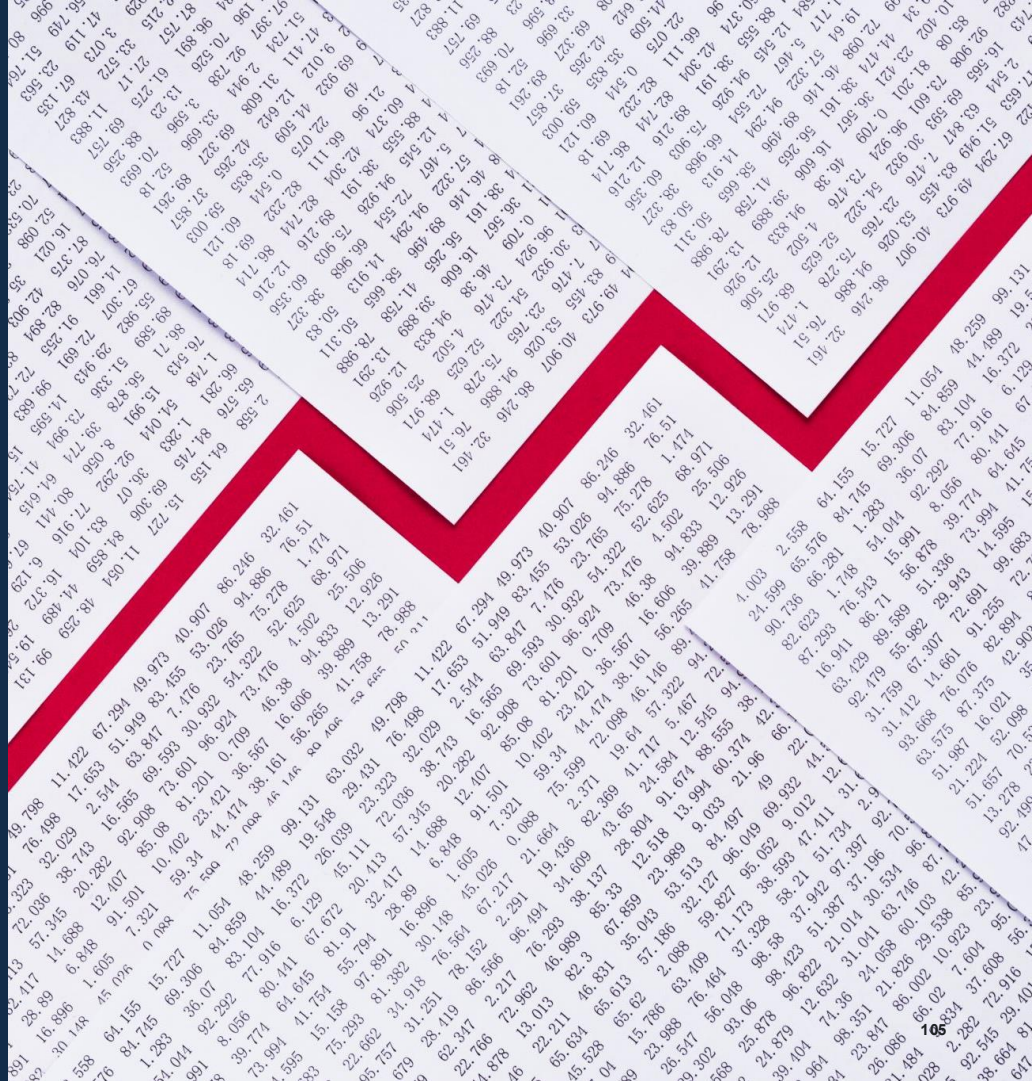
4.08

Average Rating



6.12 (I) -

Monitoring and Logging

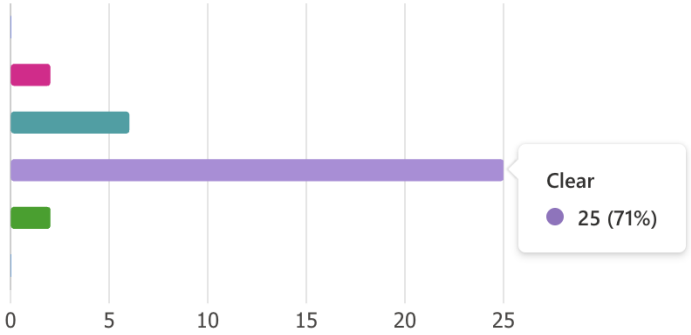


Vulnir

2. Clarity and Understandability: How clear and easy to understand is the proposed content for this section?

More details

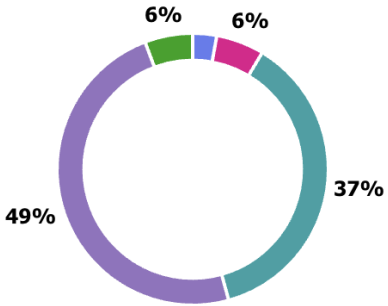
Not Clear	0
Somewhat clear	2
Neutral	6
Clear	25
Very Clear	2
Other	0



3. Practicality and Implementability: How practical and implementable do you find the requirements/guidance in this section for your organization or typical stakeholders?

More details

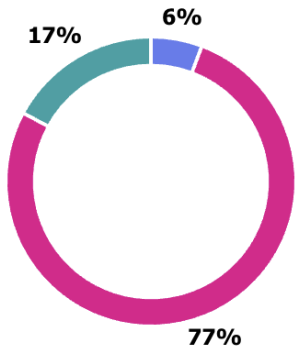
Not Practical	1
Somewhat practical	2
Neutral	13
Practical	17
Very Practical	2



4. Do you feel anything significant is missing from this section?

More details

Yes	2
No	27
Maybe	6



5. If you felt that something significant is missing please specify:

More details

1

Responses

Latest Responses

...

5.If you felt that something significant is missing please specify:

1	Requirement for appropriate log retention

6. Suggestions for Improvement: What specific changes or additions would you recommend for this section? More details

2
Responses

Latest Responses

"Need to widen the view to all of the possible products, the Default Class pro... "

"Tools without battery are not capable for logging the absolute time. More pr..."

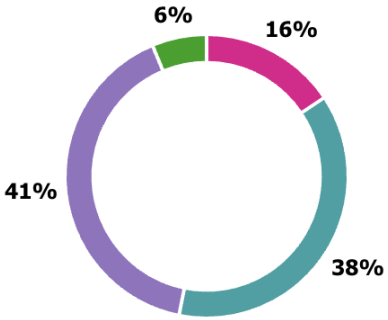
6.Suggestions for Improvement: What specific changes or additions would you recommend for this section?

1	Tools without battery are not capable for logging the absolute time. More precise definition of timestamp.
2	Need to widen the view to all of the possible products, the Default Class products will be the largest and there is a distinct need for these manufacturers to understand.

7. In your opinion, is the proposed section proportionate to the cybersecurity risks it aims to address for organizations of all sizes, particularly Small and Medium-sized Enterprises (SMEs)?

More details

Not at all proportionate/Excessive burden	0
Somewhat disproportionate/Significant burden for SMEs	5
Neutral/Unsure	12
Somewhat proportionate/Manageable for most SMEs	13
Very proportionate/Well-adapted for SMEs	2



8. Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

More details

1

Responses

Latest Responses

"Too much interpretation needed."

8.Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

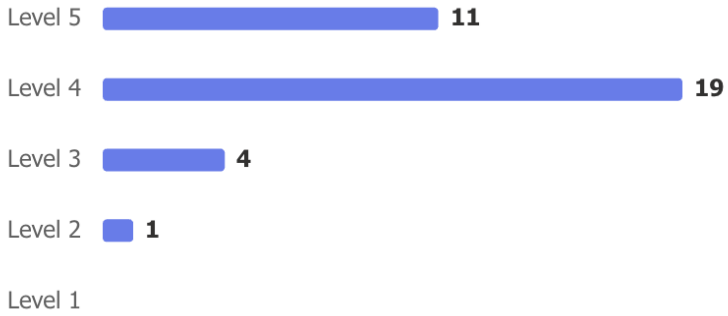
1	Too much interpretation needed.

9. Overall, how satisfied are you with this section?

More details

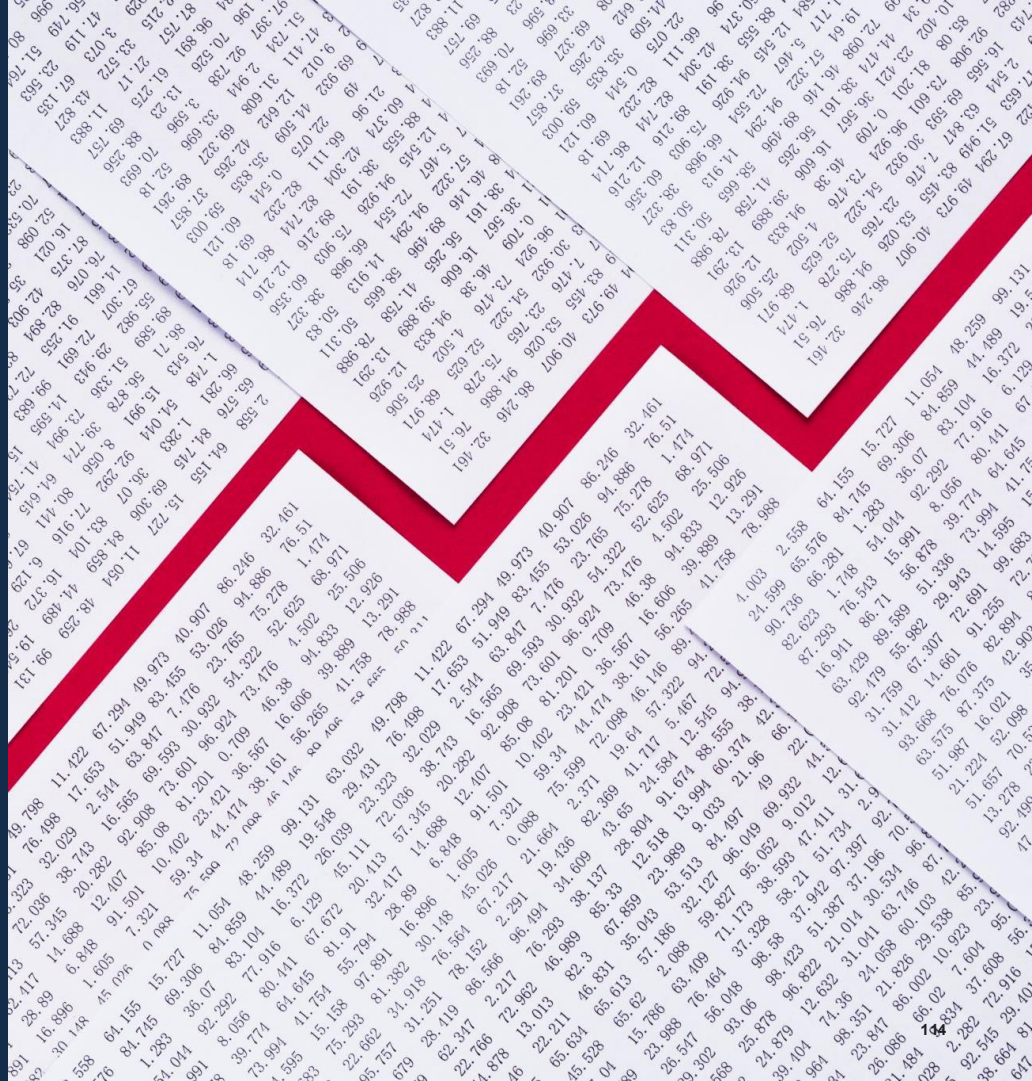
4.14

Average Rating



6.13 (m) -

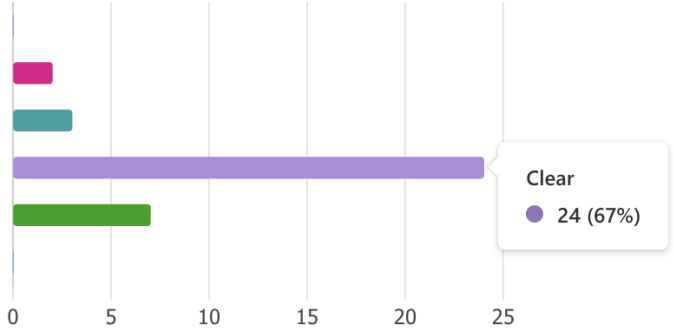
Secure Deletion



2. Clarity and Understandability: How clear and easy to understand is the proposed content for this section?

More details

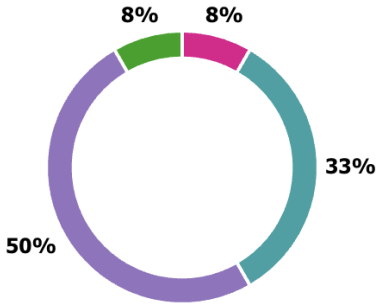
Not Clear	0
Somewhat clear	2
Neutral	3
Clear	24
Very Clear	7
Other	0



3. Practicality and Implementability: How practical and implementable do you find the requirements/guidance in this section for your organization or typical stakeholders?

More details

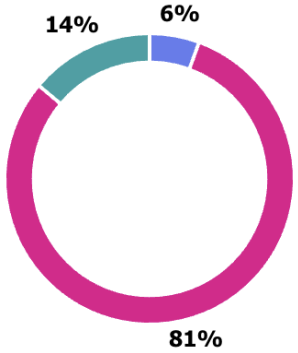
Not Practical	0
Somewhat practical	3
Neutral	12
Practical	18
Very Practical	3



4. Do you feel anything significant is missing from this section?

More details

Yes	2
No	29
Maybe	5



5. If you felt that something significant is missing please specify:

0

Responses

0 responses submitted

6. Suggestions for Improvement: What specific changes or additions would you recommend for this section?

More details

4

Responses

Latest Responses

...

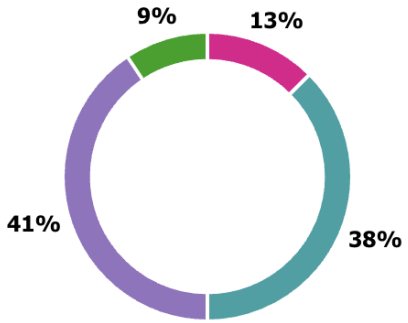
6.Suggestions for Improvement: What specific changes or additions would you recommend for this section?

1	DLM-4 is not required in my view as this is a subset of SCM.
2	no
3	Maybe you want to add this to scope: device wiping for international travel to countries where customs authorities may compromise device integrity
4	Define scope more precise. E.g. an app used optionally with a product, but is not needed for the product's basic functionality (e.g. a battery pack with bluetooth connection for connection to an app, can supply a product standalone). Deletion concerns data on the product as well as data on the backend, which might only be possible to be deleted by the app and not the product. What about data on backup servers?

7. In your opinion, is the proposed section proportionate to the cybersecurity risks it aims to address for organizations of all sizes, particularly Small and Medium-sized Enterprises (SMEs)?

More details

Not at all proportionate/Excessive burden	0
Somewhat disproportionate/Significant burden for SMEs	4
Neutral/Unsure	12
Somewhat proportionate/Manageable for most SMEs	13
Very proportionate/Well-adapted for SMEs	3



8. Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

More details

1

Responses

Latest Responses

"Methods of secure deletion vary hugely between different software products..."

8.Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

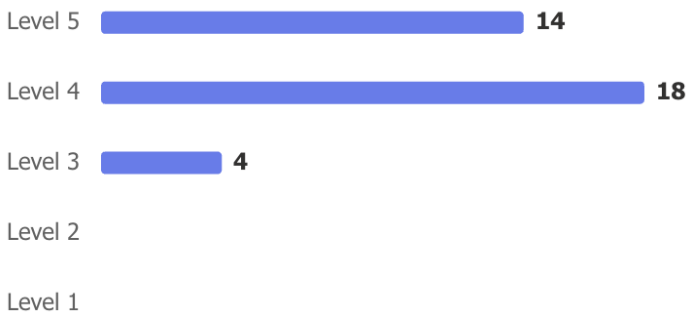
1	Methods of secure deletion vary hugely between different software products and devices.

9. Overall, how satisfied are you with this section?

More details

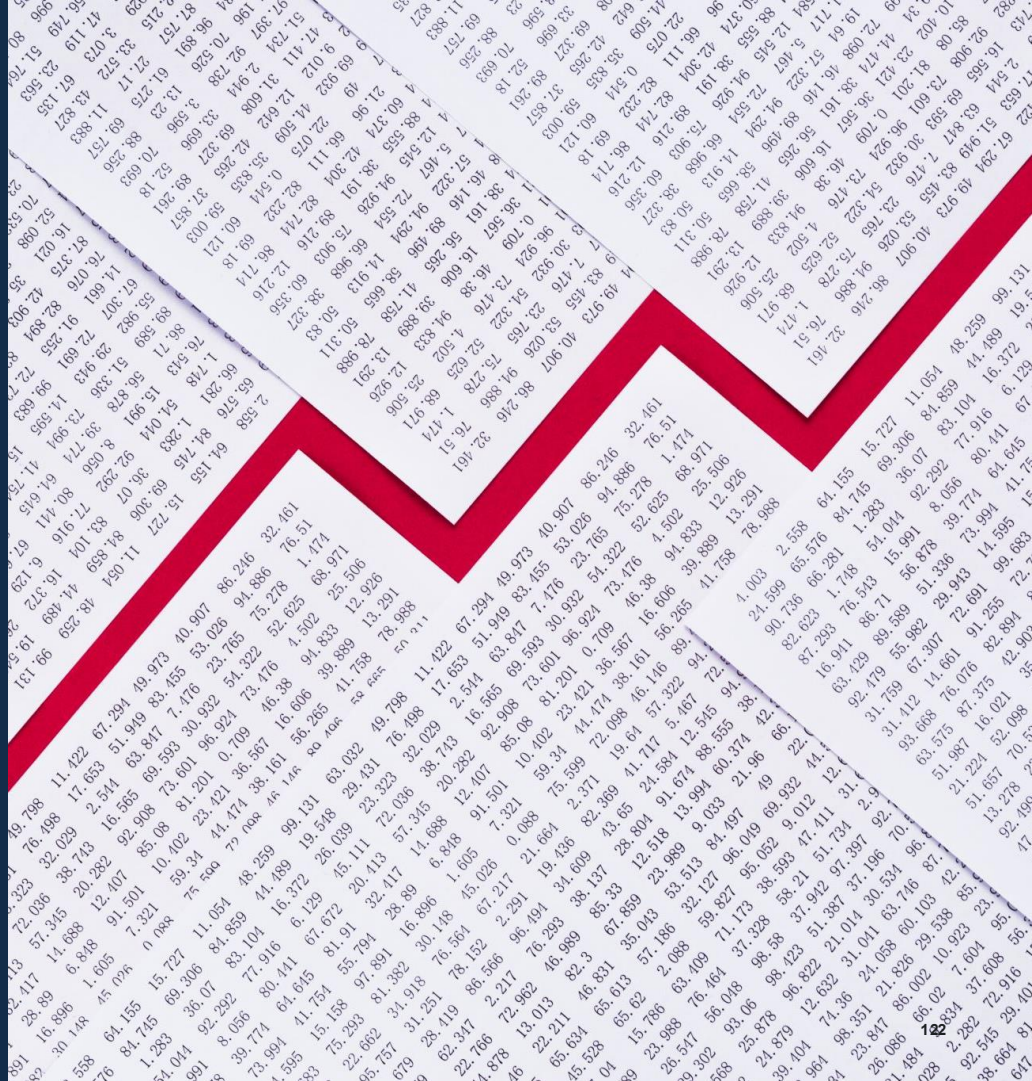
4.28

Average Rating



Conclusion

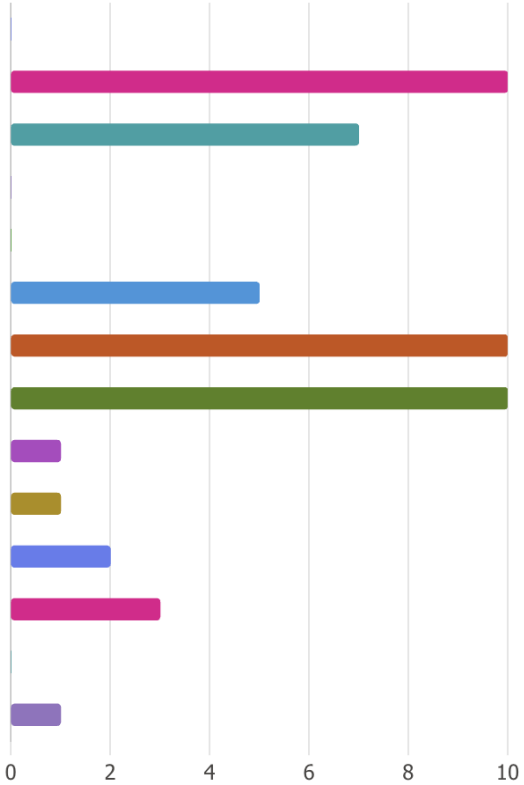
Post-Workshop Survey: Deep Dive Session Security Controls



2. Which of the following best describes your primary affiliation? (Select all that apply)

More details

Open-source community member	0
Small and Medium-sized Enterprise (SME)	10
Large enterprise	7
Academic/Research institution	0
Government/Regulatory body	0
Cybersecurity consultant	5
Software developer/vendor	10
Hardware manufacturer	10
Legal professional	1
Importer	1
Distributor	2
Testing Laboratory	3
None of the above	0
Other	1



3. What is your primary role or area of expertise related to cybersecurity or product development?

More details

22
Responses

Latest Responses

"GRC"

"I come from an SME producing software products and I am in a small team r... "

"Software Manager"

...

6 respondents (27%) answered Cybersecurity for this question.

3.What is your primary role or area of expertise related to cybersecurity or product development?

1	Firmware Engineer
2	Industrial Security
3	Inspector in NoBo, researching NoBo accreditation expansion
4	Product Compliance Officer
5	CISO
6	CISO
7	OT cybersec
8	Cybersecurity test engineer

3.What is your primary role or area of expertise related to cybersecurity or product development?

9	Cybersecurity Govnernance
10	R&D product development
11	My role is to define and deploy and the Cybersecurity processes in a transversal way. These processes and associated requirements muts be aligned with CRA, RED, Data Act,...
12	I am a cybersecurity engineer and I provide support on cybersecurity issues for the industrial products we manufacture.
13	Notified Body Responsible, Cyber Security under RED Directive
14	Product security regulation and compliance
15	Cra, standards related to our business

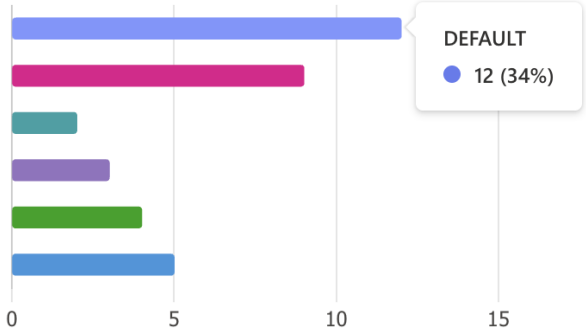
3.What is your primary role or area of expertise related to cybersecurity or product development?

16	FW developer - cybersecurity features
17	Compliance officer
18	Cybersecurity Governance, Risk, and Compliance Engineering Manager
19	Helping our customers assess their products and meet the regulatory requirements
20	Software Manager
21	I come from an SME producing software products and I am in a small team responsible for general security compliance as well as software certifications (currently eldas).
22	GRC

4. Does you organization manufacture product belonging to the following categories?

More details

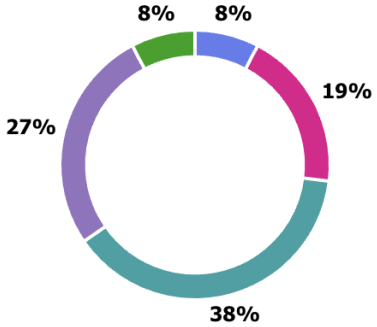
DEFAULT	12
CLASS I	9
CLASS II	2
CRITICAL	3
I DO NOT KNOW	4
NOT APPLICABLE	5



5. Prior to this workshop, how familiar were you with the Cyber Resilience Act (CRA) General Security Requirements?

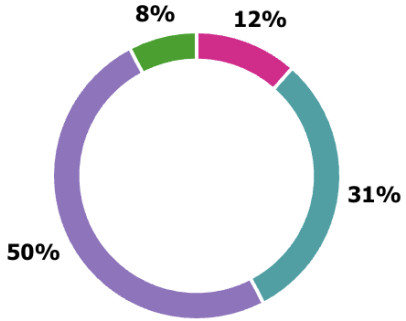
More details

Not at all familiar	2
Slightly familiar	5
Moderately familiar	10
Very familiar	7
Expert	2



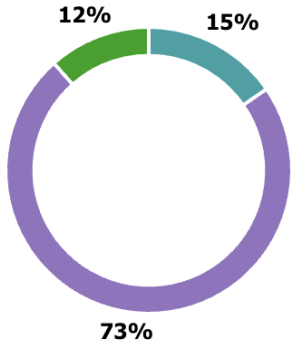
6. How familiar are you with the CRA Product Security Requirements after the workshop? More details

Not at all familiar	0
Slightly familiar	3
Moderately familiar	8
Very familiar	13
Expert	2



7. Do you believe the current draft adequately addresses the key challenges and needs related to digital product security, specifically for product security requirement? More details

Strongly Disagree	0
Disagree	0
Neutral	4
Agree	19
Strongly Agree	3



8. Please elaborate on the previous answer (if you wish to highlight any point on the level of adequacy of PT2 draft stand ard - Future EN 40000-1-4)

More details

12
Responses

Latest Responses

"The upcoming EN 40000-1-4 does not reinvent the wheel but comes rather l..."

"The CRA Product Security Requirements are very clear from the presentation..."

"For default products for the company I am working for, in combination with ..."

...

5 respondents (42%) answered standards for this question.

8. Please elaborate on the previous answer (if you wish to highlight any point on the level of adequacy of PT2 draft standard - Future EN 40000-1-4)

1	I do not like the EN18031 approach. I'd better follow 62443...
2	The document is writen in a very technical way, not easy to read for beginners.
3	CRA-NIS2 side is fine, vertical drafts are also fine - after a few years of CC - EUCC experience...
4	More info about link with PT1 and mandatoryness of SDLC etc. as maybe CCSC in 62443-4-2
5	Good to see it try to map standards, regulations and directives as a common CS requirements
6	Good points to have the link with the 18031, used for the RED 3(3). Some requirements were only applicable depending of the product and functionnalities (Toys, router;, personnal data,...) . It is not clear if it will be the case, and/or "transfered" to vertical standards.
7	As CRA often requires external evaluation/certification it woid be a useful part of standard

8. Please elaborate on the previous answer (if you wish to highlight any point on the level of adequacy of PT2 draft standard - Future EN 40000-1-4)

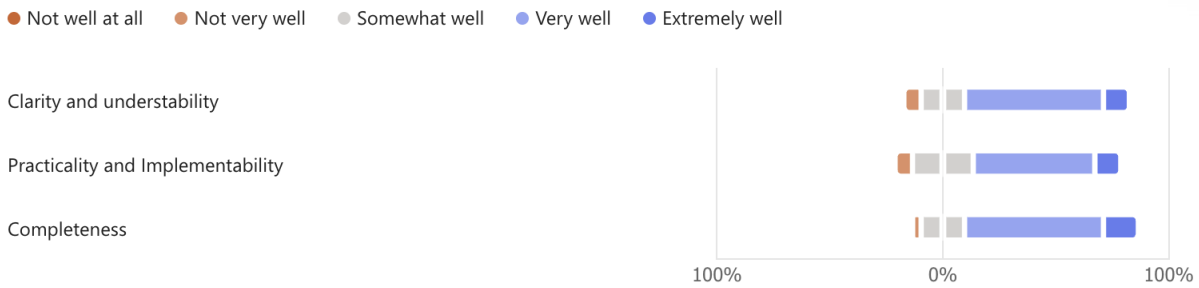
8	As with any cybersecurity regulation that includes OT/ICS it is extremely helpful to have specific guidance/considerations around the specialized technology set in place alongside old inherently insecure protocols necessary for interoperability.
9	I'm really curious to see the first draft. My feeling currently is that CRA gives vendors a lot more freedom with the risk assessment but performing it also requires a lot more effort than just following a standard and checking off a list. I'm a bit worried that this freedom/effort will increase the gap between meaningful security and regulatory compliance and that smaller vendors will really struggle to bring their products to market whereas large enterprises can argue that their objectively insecure products are still compliant based on their extensive risk assessment. I really hope this won't be the case.
10	For default products for the company I am working for, in combination with certain markets, the current draft asks for much more than the products can actually implement. This means the draft is good enough or "too much" already.

8. Please elaborate on the previous answer (if you wish to highlight any point on the level of adequacy of PT2 draft standard - Future EN 40000-1-4)

11	The CRA Product Security Requirements are very clear from the presentation but I have a few concerns. First, all the references to the vast labyrinth of standards that we do not have resources to know. In these meetings standards are "name-dropped" making it harder to follow for people who are not a part of the standardization community. Second, the worry is on the burden on SMEs to have every non-default product certified as well as CC/eldas-certifications and NIS2 activities. It may seem off-topic for this webinar but the references to other standards is some of the problem. The need to argue compliance with all requirements for every product is another.
12	The upcoming EN 40000-1-4 does not reinvent the wheel but comes rather late in the process.

9. How would you rate overall the presented draft standard on the following characteristics?

More details



10. Please explain your reasoning on your rate (at question n 9) if you have additional point to highlight

More details

8
Responses

Latest Responses

"Very good mapping with 18031-X:2014 and IEC 62443-4-2"

"All requirements were thoroughly discussed, however a little less informatio... "

"I understand it is difficult to create a standard that provides practical instruct..."

...

2 respondents (25%) answered OT for this question.

10. Please explain your reasoning on your rate (at question n 9) if you have additional point to highlight

1	QnA scrapped. Might be more often tell the location of 400000-1-4 at the "triangle" and status to verticals.
2	Still a lot of unanswered questions on clarity of CRA controls. That is not the fault of the presentation.
3	Great speaker, but CRA has high complexity
4	Just as I mentioned earlier, it is very helpful to the OT/ICS industry to see some specific considerations made for how different patching looks like when devices are very limited in functionality, what confidentiality looks like with inherently insecure protocols necessary for usage, etc.
5	Really hard to say without seeing a draft
6	I understand it is difficult to create a standard that provides practical instructions on details. But FAQs, even though already quite a few pages long, would need to somehow break down the answers or give insight sorted by product types. The base technology is not so different for embedded systems, and aspects for OT and IT or hybrid OT/IT devices deserve their own chapters in FAQ.

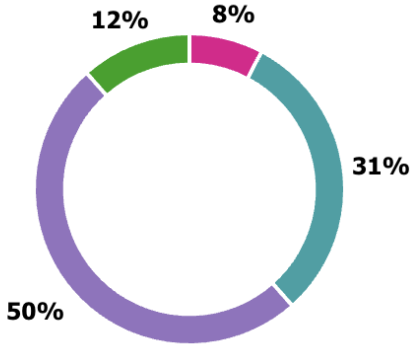
10. Please explain your reasoning on your rate (at question n 9) if you have additional point to highlight

7	All requirements were thoroughly discussed, however a little less information could have made it more clear.
8	Very good mapping with 18031-X:2014 and IEC 62443-4-2

11. How well do you believe the proposed CRA Product Security standard draft integrates with or builds upon existing fr amework?

More details

Poorly Integrated	0
Adequately Integrated	2
Neutral / Unsure	8
Well Integrated	13
Very Well Integrated	3



12. Suggestions for Improvement: What specific changes or additions would you recommend

More details

3

Responses

Latest Responses

"I recommend a relatively small number of new technical controls introduced ..."

"Some overlap with eldas/CC, but for us it will require a different to documen... "

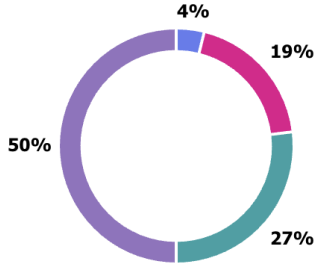
. . .

12. Suggestions for Improvement: What specific changes or additions would you recommend

1	Very good link with RED and 62443
2	Some overlap with eldas/CC, but for us it will require a different to document security although the security is already there. I am unsure how much work that will imply.
3	I recommend a relatively small number of new technical controls introduced compared to EN 18031.

13. In your opinion, is the proposed CRA General security requirement standard draft proportionate to the cybersecurity risks it aims to address for organizations of all sizes, particularly Small and Medium-sized Enterprises (SMEs)? More details

Not at all proportionate/Excessive burden	1
Somewhat disproportionate/Significant burden for SMEs	5
Neutral/Unsure	7
Somewhat proportionate/Manageable for most SMEs	13
Very proportionate/Well-adapted for SMEs	0



14. Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME: More details

6
Responses

Latest Responses

"Significant CRA compliance costs relative to the size of the SME, creating a ri..."
"That depends on how they can be used for companies with multiple importa..."
"it is not so much about the company size, but more about the necessity for ... "
...

3 respondents (50%) answered SME for this question.

CRA SME products

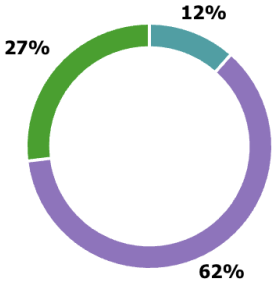
14.Please explain your rating, specifically highlighting any aspects that you perceive as overly burdensome or inadequate for SME:

1	Enterprises have issues on security side - that is new to them to but they have resources and ppl on board. SME won't have 25 ppl to do CRA
2	Fully Redesign of legacy products alreay in the market
3	SMEs cannot be excluded from general cyber and other security requirements as it would weakes their competitiveness. They shoud receive support to fill these requirements and afford certification
4	it is not so much about the company size, but more about the necessity for product types and their interfaces. There are so many digital products which only work on a proprietary ecosystem, for which companies put in effort now. This is not enough considered. To attack anything there, one has to be on site, and if such persons have access, then their primary attack is probably not digital on a single end device, because there are hundreds of them locally and they are all from different vendors. There is much potential to avoid unnecessary efforts if such situations were considered better. Or at least it is not clear that CRA allows for an efficiency.
5	That depends on how they can be used for companies with multiple important products.
6	Significant CRA compliance costs relative to the size of the SME, creating a risk of reallocating funds from R&D to compliance activities. This is contrary to what Mario Draghi recommended in his report.

15. Overall, how valuable was this deep-dive session for you?

More details

Extremely not useful	0
Somewhat not useful	0
Somewhat useful	3
Very useful	16
Extremely useful	7



16. What was the most valuable aspect of this workshop for you?

More details

10
Responses

Latest Responses

"Deep-dive per essential requirement with links to CRA, EN 18031 and IEC 62... "

"The requirement overview mostly - it gave me the essence of what we are ex..."

"To capture more knowledge and bring it into my company."

...

5 respondents (50%) answered CRA for this question.

16. What was the most valuable aspect of this workshop for you?

1	Learning about different aspects of CRA
2	Getting more information about specific CRA requirements.
3	Consolidation of frameworks per CRA control
4	A comprehensive overview of standardization under the CRA
5	Q&A Session
6	link with 18031
7	Seeing the expected difference to 18031
8	To capture more knowledge and bring it into my company.
9	The requirement overview mostly - it gave me the essence of what we are expected to comply with. I know this was a deep dive, but after 3½ hours some of the details escaped me.
10	Deep-dive per essential requirement with links to CRA, EN 18031 and IEC 62443-4-2

17. What was the least valuable aspect, or what could be improved?

More details

6
Responses

Latest Responses

"Detailed 'how-to' guidelines for CRA implementation were missing, yet stron..."

"See above comments."

"The survey for each chapter were a bit too much. I stopped at some point. A..."

...

2 respondents (33%) answered requirements for this question.

17.What was the least valuable aspect, or what could be improved?

1	QnA due the irrelevant questions. Might be hidden to filter to the audience
2	time is very late in Japan
3	more info about new requirements
4	The survey for each chapter were a bit too much. I stopped at some point. Also, the most important field in each survey is at the end and there is not enough time to think about aspects.
5	See above comments.
6	Detailed 'how-to' guidelines for CRA implementation were missing, yet strongly requested — particularly regarding risk assessment, vulnerability management, and the implementation of essential requirements. However, I understand that this was outside the scope of the deep-dive.

18. Any additional comments or feedback you'd like to share regarding the CRA Generic security requirement standard o r the workshop of today?

More details

4

Responses

Latest Responses

"This standard should have been available before the CRA."

"No"

"Keep it up, don't stop doing this."

• • •

18. Any additional comments or feedback you'd like to share regarding the CRA Generic security requirement standard or the workshop of today?

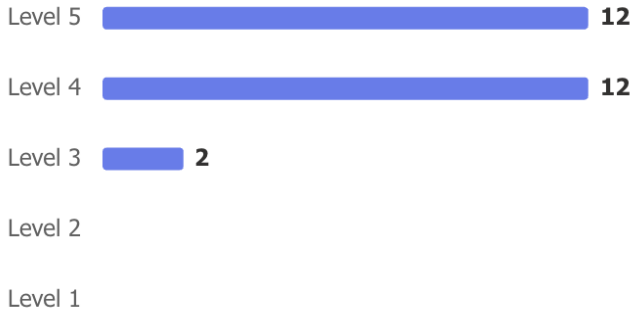
1	Congrats to speaker was a marathon
2	Keep it up, don't stop doing this.
3	No
4	This standard should have been available before the CRA.

19. Overall, how satisfied are you with the PT2 draft presentation as it is today?

More details

4.38

Average Rating



Thank you

VULNIR.com

info@vulnir.com