

# E DIN EN 40000-1-2:2025-11 (E)

Erscheinungsdatum: 2025-10-24

## Cybersecurity requirements for products with digital elements - Part 1-2: Principles for cyber resilience; English version prEN 40000-1-2:2025

---

### Contents

	Page
European foreword .....	6
<b>1</b> Scope.....	<b>7</b>
<b>2</b> Normative references .....	<b>7</b>
<b>3</b> Terms and definitions.....	<b>7</b>
<b>4</b> Introduction .....	<b>7</b>
<b>5</b> Cybersecurity Principles.....	<b>8</b>
5.1 General.....	8
5.2 Risk-based approach to cybersecurity .....	8
5.2.1 Principle .....	8
5.2.2 Guidance.....	9
5.3 Security by Design .....	9
5.3.1 Principle .....	9
5.3.2 Guidance.....	9
5.4 Secure by Default.....	10
5.4.1 Principle .....	10
5.4.2 Guidance.....	10
5.5 Transparency.....	11
5.5.1 Principle .....	11
5.5.2 Guidance.....	11
<b>6</b> Risk management elements.....	<b>11</b>
6.1 General.....	11
6.2 Product context.....	13
6.2.1 General.....	13
6.2.1.1 Context purpose .....	13
6.2.1.2 Product intended purpose and reasonable foreseeable use .....	13
6.2.1.3 Product functions.....	13
6.2.1.4 Product operational environment .....	14
6.2.1.5 Product architecture overview .....	14
6.2.1.6 Product user description.....	14
6.2.2 Input .....	15
6.2.3 Requirement .....	15
6.2.4 Output .....	15
6.2.5 Assessment criteria .....	15
6.3 Risk acceptance criteria and risk management methodology.....	16
6.3.1 General.....	16
6.3.2 Input .....	17
6.3.3 Requirement .....	17
6.3.4 Output .....	18
6.3.5 Assessment criteria .....	18
6.4 Risk assessment.....	18
6.4.1 General.....	18
6.4.2 Asset and cybersecurity objective identification.....	19
6.4.2.1 General.....	19
6.4.2.2 Input.....	19
6.4.2.3 Requirement.....	19

6.4.2.4	Output.....	19
6.4.2.5	Assessment criteria.....	19
6.4.3	Threat identification .....	20
6.4.3.1	General.....	20
6.4.3.2	Input.....	20
6.4.3.3	Requirement .....	20
6.4.3.4	Output.....	20
6.4.3.5	Assessment criteria.....	20
6.4.4	Risk estimation .....	21
6.4.4.1	General.....	21
6.4.4.2	Input.....	21
6.4.4.3	Requirement .....	21
6.4.4.4	Output.....	21
6.4.4.5	Assessment criteria.....	22
6.4.5	Risk evaluation .....	22
6.4.5.1	General.....	22
6.4.5.2	Input.....	22
6.4.5.3	Requirement .....	22
6.4.5.4	Output.....	22
6.4.5.5	Assessment criteria.....	22
6.5	Risk Treatment .....	23
6.5.1	General .....	23
6.5.1.1	Aim of risk treatment .....	23
6.5.1.2	Risk avoidance.....	23
6.5.1.3	Risk mitigation .....	23
6.5.1.4	Risk acceptance.....	23
6.5.1.5	Risk transfer.....	23
6.5.1.6	Risk treatment preference .....	23
6.5.2	Input.....	24
6.5.3	Requirement.....	24
6.5.4	Output.....	24
6.5.5	Assessment criteria .....	24
6.6	Risk communication.....	25
6.6.1	General .....	25
6.6.2	Input.....	25
6.6.3	Requirement.....	25
6.6.4	Output.....	26
6.6.5	Assessment criteria .....	26
6.7	Risk monitoring and review .....	26
6.7.1	General .....	26
6.7.2	Input.....	26
6.7.3	Requirement.....	27
6.7.4	Output.....	27
6.7.5	Assessment criteria .....	27
7	Cybersecurity activities.....	28
7.1	General .....	28
7.2	Product cybersecurity planning.....	28
7.2.1	General .....	28
7.2.2	Input.....	28
7.2.3	Requirement.....	28
7.2.4	Output.....	28
7.2.5	Assessment criteria .....	28
7.3	Product cybersecurity requirements .....	29
7.3.1	General .....	29
7.3.2	Input.....	29
7.3.3	Requirement.....	30
7.3.4	Output.....	30

7.3.5	Assessment criteria .....	30
7.4	Cybersecurity architecture and design .....	30
7.4.1	General.....	30
7.4.2	Input .....	31
7.4.3	Requirement .....	31
7.4.4	Output .....	31
7.4.5	Assessment criteria .....	31
7.5	Secure implementation .....	32
7.5.1	General.....	32
7.5.2	Input .....	32
7.5.3	Requirement .....	33
7.5.4	Output .....	33
7.5.5	Assessment criteria .....	33
7.6	Cybersecurity verification and validation.....	33
7.6.1	General.....	33
7.6.2	Input .....	35
7.6.3	Requirement .....	35
7.6.4	Output .....	35
7.6.5	Assessment criteria .....	36
7.7	Secure Production and Distribution .....	36
7.7.1	General.....	36
7.7.2	Digital Production.....	36
7.7.2.1	7.7.2.1General .....	36
7.7.2.2	7.7.2.2Input.....	37
7.7.2.3	Requirement.....	37
7.7.2.4	Output.....	37
7.7.2.5	Assessment criteria.....	38
7.7.3	Manufacturing .....	38
7.7.3.1	General .....	38
7.7.3.2	Input.....	38
7.7.3.3	Requirement.....	38
7.7.3.4	Output.....	39
7.7.3.5	Assessment criteria.....	39
7.8	Cybersecurity issue management.....	39
7.8.1	General.....	39
7.8.2	Input .....	39
7.8.3	Requirement .....	39
7.8.4	Output .....	39
7.8.5	Assessment criteria .....	40
7.9	Product monitoring .....	40
7.9.1	General.....	40
7.9.2	Input .....	40
7.9.3	Requirement .....	41
7.9.4	Output .....	41
7.9.5	Assessment criteria .....	41
7.10	Planning for secure decommissioning .....	41
7.10.1	General.....	41
7.10.2	Input .....	41
7.10.3	Requirement .....	41
7.10.4	Output .....	42
7.10.5	Assessment criteria .....	42
7.11	Third-Party Component Cybersecurity Management.....	42
7.11.1	General.....	42
7.11.2	Input .....	44
7.11.3	Requirement .....	44
7.11.4	Output .....	44
7.11.5	Assessment criteria .....	44

<b>Annex A (informative) Coherence with vertical standards</b> .....	<b>45</b>
<b>A.1 Coherence elements</b> .....	<b>45</b>
<b>Annex B (informative) Cybersecurity Supplier Agreements Example</b> .....	<b>46</b>
<b>B.1 General</b> .....	<b>46</b>
<b>B.2 CSSA Example</b> .....	<b>48</b>
<b>Annex C (informative) Relationship between this European Standard and the essential cybersecurity requirements of REGULATION (EU) 2024/2847</b> .....	<b>54</b>
<b>C.1 General</b> .....	<b>54</b>
<b>C.2 Reference to Essential Requirements</b> .....	<b>54</b>
<b>C.3 Mapping to essential requirements</b> .....	<b>54</b>
<b>C.4 Normative or Informative</b> .....	<b>60</b>
<b>C.5 Assessment criteria</b> .....	<b>60</b>
<b>Annex D (informative) Accessible and Inclusive Cybersecurity</b> .....	<b>61</b>
<b>D.1 Scope</b> .....	<b>61</b>
<b>D.2 Legal reasoning</b> .....	<b>61</b>
<b>D.3 The user</b> .....	<b>61</b>
<b>D.4 Nature of the required interaction</b> .....	<b>62</b>
<b>D.5 Consequences of the interaction method on the user’s cybersecurity</b> .....	<b>62</b>
<b>D.6 Recommended solution to ensure maximum cybersecurity to the potential users</b> .....	<b>62</b>
<b>D.7 Communication with the user</b> .....	<b>63</b>
<b>Bibliography</b> .....	<b>64</b>

## Figures

<b>Figure 1 — Risk management elements overview</b> .....	<b>12</b>
<b>Figure B.1 — Example of CSSAs in the supply chain</b> .....	<b>46</b>

## Tables

<b>Table B.1 — Example of a CSSA</b> .....	<b>48</b>
<b>Table C.1 — Relationship between this European Standard and Annex I of Regulation 2024/2847 [OJEU L 60]</b> .....	<b>55</b>
<b>Table C.2 — Normative status of the structure of each clause</b> .....	<b>60</b>