Audit report

Organisation - Cyber Resilience Act (EU) 2024/2847

Organisation	**Example Machine Works B.V.**
Generated	2026-09-16
Subject	the organisation
Legal basis	Cyber Resilience Act (EU) 2024/2847
Assessed against	IEC 62443-4-1, IEC 62443-2-3, ISO/IEC 29147, ISO/IEC 30111 (clause references; official standard texts not included)
Source snapshot	be4aea5f · 2026-09-16 21:03

Contents

Scope and context

This document records the compliance position of the organisation for Cyber Resilience Act (EU) 2024/2847: the assessed control sets, the recorded implementation and evidence, the open gaps and the recommended actions. It is generated from the live assessment data and is intended for the QMS or the compliance archive.

Compliance status

Secure development lifecycle (IEC 62443-4-1)

Status	Count
In place	46
In place, evidence missing	0
Partially implemented	0
Planned	1
Not in place	0
Not yet assessed	0
Not applicable	0
Applicable total	47

Control	Requirement	Status	Evidence recorded
SM-1	Development process	In place	yes
SM-2	Identification of responsibilities	In place	yes
SM-3	Identification of applicability	In place	yes
SM-4	Security expertise	In place	yes
SM-5	Process scoping	In place	yes
SM-6	File integrity	In place	yes
SM-7	Development environment security	In place	yes
SM-8	Controls for private keys	In place	yes
SM-9	Security requirements for externally provided components	In place	yes
SM-10	Custom developed components from third-party suppliers	In place	yes
SM-11	Assessing and addressing security-related issues	In place	yes
SM-12	Process verification	In place	yes
SM-13	Continuous improvement	In place	yes
SR-1	Product security context	In place	yes
SR-2	Threat model	In place	yes
SR-3	Product security requirements	In place	yes
SR-4	Product security requirements content	In place	yes
SR-5	Security requirements review	In place	yes
SD-1	Secure design principles	In place	yes
SD-2	Defense in depth design	In place	yes
SD-3	Security design review	In place	yes
SD-4	Secure design best practices	In place	yes
SI-1	Security implementation review	In place	yes

Control	Requirement	Status	Evidence recorded
SI-2	Secure coding standards	In place	yes
SVV-1	Security requirements testing	In place	yes
SVV-2	Threat mitigation testing	In place	yes
SVV-3	Vulnerability testing	In place	yes
SVV-4	Penetration testing	Planned	yes
SVV-5	Independence of testers	In place	yes
DM-1	Receiving notifications of security-related issues	In place	yes
DM-2	Reviewing security-related issues	In place	yes
DM-3	Assessing security-related issues	In place	yes
DM-4	Addressing security-related issues	In place	yes
DM-5	Disclosing security-related issues	In place	yes
DM-6	Periodic review of security defect management practice	In place	yes
SUM-1	Security update qualification	In place	yes
SUM-2	Security update documentation	In place	yes
SUM-3	Dependent component or operating system security update documentation	In place	yes
SUM-4	Security update delivery	In place	yes
SUM-5	Timely delivery of security patches	In place	yes
SG-1	Product defense in depth	In place	yes
SG-2	Defense in depth measures expected in the environment	In place	yes
SG-3	Security hardening guidelines	In place	yes
SG-4	Secure disposal guidelines	In place	yes
SG-5	Secure operation guidelines	In place	yes
SG-6	Account management guidelines	In place	yes
SG-7	Documentation review	In place	yes

Recorded implementation and evidence

SM-1 - Development process — In place

Implementation Implemented in the hardening baseline applied to every shipped controller, with the deviations list kept per customer.

Evidence Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026) - see the Documentation index and the attached excerpt "PSP-01 v2.4 (excerpt).md". Owner: product security officer.

SM-2 - Identification of responsibilities — In place

Implementation Documented in the secure development policy and enforced as a blocking release-gate check; owner: product security officer.

Evidence Release checklist RC-2.1, gate "SM-2" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

SM-3 - Identification of applicability — In place

Implementation Covered by the engineering work instruction and checked at the design review; the reviewer signs the checklist before release.

Evidence Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

SM-4 - Security expertise

In place

Implementation Assigned to the product security officer, executed per release and recorded in the release checklist.

Evidence FAT/SAT acceptance report FAT-2026-11, case "SM-4 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

SM-5 - Process scoping

In place

Implementation Carried by the supplier agreements and verified on intake, with the acceptance record kept per delivery.

Evidence Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

SM-6 - File integrity

In place

Implementation Automated in the CI/CD pipeline (build fails on violation); the manual fallback is described in the operations runbook.

Evidence Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "SM-6" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

SM-7 - Development environment security

In place

Implementation Handled by the toolchain: the setting is fixed in the build configuration and verified by an automated check on every merge.

Evidence Configuration audit pack SCR-SM-7 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-SM-7/, cross-checked against hardening baseline HB-2.

SM-8 - Controls for private keys

In place

Implementation Part of the design rules for the control system; conformance is sampled in the internal audit twice a year.

Evidence Release checklist RC-2.1, gate "SM-8" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

SM-9 - Security requirements for externally provided components

In place

Implementation Implemented in the reference control-system architecture and applied across the MX series; deviations are tracked in the risk register.

Evidence Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

SM-10 - Custom developed components from third-party suppliers

In place

Implementation Built into the product platform, so every variant inherits it; deviations need an approved exception in the risk register.

Evidence FAT/SAT acceptance report FAT-2026-11, case "SM-10 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

SM-11 - Assessing and addressing security-related issues

In place

Implementation Implemented in the hardening baseline applied to every shipped controller, with the deviations list kept per customer.

Evidence Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

SM-12 - Process verification

In place

Implementation Documented in the secure development policy and enforced as a blocking release-gate check; owner: product security officer.

Evidence Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "SM-12" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

SM-13 - Continuous improvement

In place

Implementation	Covered by the engineering work instruction and checked at the design review; the reviewer signs the checklist before release.
Evidence	Configuration audit pack SCR-SM-13 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-SM-13/, cross-checked against hardening baseline HB-2.

SR-1 - Product security context

In place

Implementation	Assigned to the product security officer, executed per release and recorded in the release checklist.
Evidence	Release checklist RC-2.1, gate "SR-1" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

SR-2 - Threat model

In place

Implementation	Carried by the supplier agreements and verified on intake, with the acceptance record kept per delivery.
Evidence	Machine threat model TM-MX540 v2 (19 Jan 2026) - Documentation index, attached excerpt "TM-MX540 v2 (excerpt).md"; review ticket SEC-733 closed.

SR-3 - Product security requirements

In place

Implementation	Automated in the CI/CD pipeline (build fails on violation); the manual fallback is described in the operations runbook.
Evidence	FAT/SAT acceptance report FAT-2026-11, case "SR-3 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

SR-4 - Product security requirements content

In place

Implementation	Handled by the toolchain: the setting is fixed in the build configuration and verified by an automated check on every merge.
Evidence	Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

SR-5 - Security requirements review

In place

Implementation	Part of the design rules for the control system; conformance is sampled in the internal audit twice a year.
Evidence	Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "SR-5" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

SD-1 - Secure design principles

In place

Implementation	Part of the design rules for the control system; conformance is sampled in the internal audit twice a year.
Evidence	Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "SD-1" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

SD-2 - Defense in depth design

In place

Implementation	Implemented in the reference control-system architecture and applied across the MX series; deviations are tracked in the risk register.
Evidence	Configuration audit pack SCR-SD-2 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-SD-2/, cross-checked against hardening baseline HB-2.

SD-3 - Security design review

In place

Implementation	Built into the product platform, so every variant inherits it; deviations need an approved exception in the risk register.
Evidence	Release checklist RC-2.1, gate "SD-3" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

SD-4 - Secure design best practices

In place

Implementation Implemented in the hardening baseline applied to every shipped controller, with the deviations list kept per customer.

Evidence Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

SI-1 - Security implementation review

In place

Implementation Implemented in the reference control-system architecture and applied across the MX series; deviations are tracked in the risk register.

Evidence Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

SI-2 - Secure coding standards

In place

Implementation Built into the product platform, so every variant inherits it; deviations need an approved exception in the risk register.

Evidence Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "SI-2" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

SVV-1 - Security requirements testing

In place

Implementation Assigned to the product security officer, executed per release and recorded in the release checklist.

Evidence Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "SVV-1" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

SVV-2 - Threat mitigation testing

In place

Implementation Carried by the supplier agreements and verified on intake, with the acceptance record kept per delivery.

Evidence Configuration audit pack SCR-SVV-2 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-SVV-2/, cross-checked against hardening baseline HB-2.

SVV-3 - Vulnerability testing

In place

Implementation Automated in the CI/CD pipeline (build fails on violation); the manual fallback is described in the operations runbook.

Evidence Release checklist RC-2.1, gate "SVV-3" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

SVV-4 - Penetration testing

Planned

Implementation External penetration test of the MX-540 control system commissioned for Q4 2026 (order PO-2026-118, supplier Secura); internal fuzzing already runs in CI. No penetration-test report exists yet.

Evidence Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

SVV-5 - Independence of testers

In place

Implementation Part of the design rules for the control system; conformance is sampled in the internal audit twice a year.

Evidence FAT/SAT acceptance report FAT-2026-11, case "SVV-5 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

DM-1 - Receiving notifications of security-related issues

In place

Implementation Documented in the secure development policy and enforced as a blocking release-gate check; owner: product security officer.

Evidence Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "DM-1" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

DM-2 - Reviewing security-related issues — In place

Implementation	Covered by the engineering work instruction and checked at the design review; the reviewer signs the checklist before release.
Evidence	Configuration audit pack SCR-DM-2 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-DM-2/, cross-checked against hardening baseline HB-2.

DM-3 - Assessing security-related issues — In place

Implementation	Assigned to the product security officer, executed per release and recorded in the release checklist.
Evidence	Release checklist RC-2.1, gate "DM-3" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

DM-4 - Addressing security-related issues — In place

Implementation	Carried by the supplier agreements and verified on intake, with the acceptance record kept per delivery.
Evidence	Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

DM-5 - Disclosing security-related issues — In place

Implementation	Automated in the CI/CD pipeline (build fails on violation); the manual fallback is described in the operations runbook.
Evidence	FAT/SAT acceptance report FAT-2026-11, case "DM-5 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

DM-6 - Periodic review of security defect management practice — In place

Implementation	Handled by the toolchain: the setting is fixed in the build configuration and verified by an automated check on every merge.
Evidence	Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

SUM-1 - Security update qualification — In place

Implementation	Implemented in the reference control-system architecture and applied across the MX series; deviations are tracked in the risk register.
Evidence	Configuration audit pack SCR-SUM-1 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-SUM-1/, cross-checked against hardening baseline HB-2.

SUM-2 - Security update documentation — In place

Implementation	Built into the product platform, so every variant inherits it; deviations need an approved exception in the risk register.
Evidence	Release checklist RC-2.1, gate "SUM-2" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

SUM-3 - Dependent component or operating system security update documentation — In place

Implementation	Implemented in the hardening baseline applied to every shipped controller, with the deviations list kept per customer.
Evidence	Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

SUM-4 - Security update delivery — In place

Implementation	Documented in the secure development policy and enforced as a blocking release-gate check; owner: product security officer.
Evidence	FAT/SAT acceptance report FAT-2026-11, case "SUM-4 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

SUM-5 - Timely delivery of security patches — In place

Implementation Covered by the engineering work instruction and checked at the design review; the reviewer signs the checklist before release.

Evidence Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

SG-1 - Product defense in depth — In place

Implementation Documented in the secure development policy and enforced as a blocking release-gate check; owner: product security officer.

Evidence FAT/SAT acceptance report FAT-2026-11, case "SG-1 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

SG-2 - Defense in depth measures expected in the environment — In place

Implementation Covered by the engineering work instruction and checked at the design review; the reviewer signs the checklist before release.

Evidence Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

SG-3 - Security hardening guidelines — In place

Implementation Assigned to the product security officer, executed per release and recorded in the release checklist.

Evidence Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "SG-3" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

SG-4 - Secure disposal guidelines — In place

Implementation Carried by the supplier agreements and verified on intake, with the acceptance record kept per delivery.

Evidence Configuration audit pack SCR-SG-4 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-SG-4/, cross-checked against hardening baseline HB-2.

SG-5 - Secure operation guidelines — In place

Implementation Automated in the CI/CD pipeline (build fails on violation); the manual fallback is described in the operations runbook.

Evidence Release checklist RC-2.1, gate "SG-5" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

SG-6 - Account management guidelines — In place

Implementation Handled by the toolchain: the setting is fixed in the build configuration and verified by an automated check on every merge.

Evidence Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

SG-7 - Documentation review — In place

Implementation Part of the design rules for the control system; conformance is sampled in the internal audit twice a year.

Evidence FAT/SAT acceptance report FAT-2026-11, case "SG-7 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

Secure code review checklist (CRA Annex I Part I / SI)

Status	Count
In place	11
In place, evidence missing	0
Partially implemented	0
Planned	0
Not in place	0

Status	Count
Not yet assessed	0
Not applicable	0
Applicable total	11

Control	Requirement	Status	Evidence recorded
RV-1	Input validation	**In place**	yes
RV-2	Injection prevention	**In place**	yes
RV-3	Output encoding (XSS)	**In place**	yes
RV-4	Path traversal prevention	**In place**	yes
RV-5	No hardcoded credentials	**In place**	yes
RV-6	Authentication & session management	**In place**	yes
RV-7	Authorisation / access control	**In place**	yes
RV-8	Strong cryptography	**In place**	yes
RV-9	Secrets & key management	**In place**	yes
RV-10	Safe error handling	**In place**	yes
RV-11	Security logging	**In place**	yes

Recorded implementation and evidence

RV-1 - Input validation — In place

Implementation Automated in the CI/CD pipeline (build fails on violation); the manual fallback is described in the operations runbook.

Evidence FAT/SAT acceptance report FAT-2026-11, case "RV-1 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

RV-2 - Injection prevention — In place

Implementation Handled by the toolchain: the setting is fixed in the build configuration and verified by an automated check on every merge.

Evidence Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

RV-3 - Output encoding (XSS) — In place

Implementation Part of the design rules for the control system; conformance is sampled in the internal audit twice a year.

Evidence Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "RV-3" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

RV-4 - Path traversal prevention — In place

Implementation Implemented in the reference control-system architecture and applied across the MX series; deviations are tracked in the risk register.

Evidence Configuration audit pack SCR-RV-4 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-RV-4/, cross-checked against hardening baseline HB-2.

RV-5 - No hardcoded credentials — In place

Implementation Built into the product platform, so every variant inherits it; deviations need an approved exception in the risk register.

Evidence Release checklist RC-2.1, gate "RV-5" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

RV-6 - Authentication & session management — In place

Implementation	Implemented in the hardening baseline applied to every shipped controller, with the deviations list kept per customer.
Evidence	Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

RV-7 - Authorisation / access control — In place

Implementation	Documented in the secure development policy and enforced as a blocking release-gate check; owner: product security officer.
Evidence	FAT/SAT acceptance report FAT-2026-11, case "RV-7 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

RV-8 - Strong cryptography — In place

Implementation	Covered by the engineering work instruction and checked at the design review; the reviewer signs the checklist before release.
Evidence	Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

RV-9 - Secrets & key management — In place

Implementation	Assigned to the product security officer, executed per release and recorded in the release checklist.
Evidence	Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "RV-9" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

RV-10 - Safe error handling — In place

Implementation	Carried by the supplier agreements and verified on intake, with the acceptance record kept per delivery.
Evidence	Configuration audit pack SCR-RV-10 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-RV-10/, cross-checked against hardening baseline HB-2.

RV-11 - Security logging — In place

Implementation	Automated in the CI/CD pipeline (build fails on violation); the manual fallback is described in the operations runbook.
Evidence	Release checklist RC-2.1, gate "RV-11" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

Security testing checklist (CRA Annex I Part II(3) / SVV)

Status	Count
In place	12
In place, evidence missing	0
Partially implemented	0
Planned	0
Not in place	0
Not yet assessed	0
Not applicable	0
Applicable total	12

Control	Requirement	Status	Evidence recorded
ST-1	Static application security testing (SAST)	In place	yes
ST-2	Software composition analysis (SCA)	In place	yes
ST-3	SBOM generation	In place	yes
ST-4	Automated security gates	In place	yes
ST-5	Dynamic application security testing (DAST)	In place	yes

Control	Requirement	Status	Evidence recorded
ST-6	Fuzz testing	**In place**	yes
ST-7	Security-functionality verification	**In place**	yes
ST-8	Penetration testing	**In place**	yes
ST-9	Offline / acceptance testing (OT)	**In place**	yes
ST-10	CRA traceability matrix	**In place**	yes
ST-11	Test strategy documented	**In place**	yes
ST-12	10-year retention of test evidence	**In place**	yes

Recorded implementation and evidence

ST-1 - Static application security testing (SAST) — In place

Implementation Built into the product platform, so every variant inherits it; deviations need an approved exception in the risk register.

Evidence Release checklist RC-2.1, gate "ST-1" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

ST-2 - Software composition analysis (SCA) — In place

Implementation Implemented in the hardening baseline applied to every shipped controller, with the deviations list kept per customer.

Evidence Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

ST-3 - SBOM generation — In place

Implementation Documented in the secure development policy and enforced as a blocking release-gate check; owner: product security officer.

Evidence FAT/SAT acceptance report FAT-2026-11, case "ST-3 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

ST-4 - Automated security gates — In place

Implementation Covered by the engineering work instruction and checked at the design review; the reviewer signs the checklist before release.

Evidence Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

ST-5 - Dynamic application security testing (DAST) — In place

Implementation Assigned to the product security officer, executed per release and recorded in the release checklist.

Evidence Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "ST-5" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

ST-6 - Fuzz testing — In place

Implementation Carried by the supplier agreements and verified on intake, with the acceptance record kept per delivery.

Evidence Configuration audit pack SCR-ST-6 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-ST-6/, cross-checked against hardening baseline HB-2.

ST-7 - Security-functionality verification — In place

Implementation Automated in the CI/CD pipeline (build fails on violation); the manual fallback is described in the operations runbook.

Evidence Release checklist RC-2.1, gate "ST-7" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

ST-8 - Penetration testing — In place

Implementation Handled by the toolchain: the setting is fixed in the build configuration and verified by an automated check on every merge.

Evidence Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

ST-9 - Offline / acceptance testing (OT) — In place

Implementation Part of the design rules for the control system; conformance is sampled in the internal audit twice a year.

Evidence FAT/SAT acceptance report FAT-2026-11, case "ST-9 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

ST-10 - CRA traceability matrix — In place

Implementation Implemented in the reference control-system architecture and applied across the MX series; deviations are tracked in the risk register.

Evidence Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

ST-11 - Test strategy documented — In place

Implementation Built into the product platform, so every variant inherits it; deviations need an approved exception in the risk register.

Evidence Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "ST-11" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

ST-12 - 10-year retention of test evidence — In place

Implementation Implemented in the hardening baseline applied to every shipped controller, with the deviations list kept per customer.

Evidence Configuration audit pack SCR-ST-12 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-ST-12/, cross-checked against hardening baseline HB-2.

Vulnerability handling & disclosure (CVD) (CRA Annex I Part II)

Status	Count
In place	12
In place, evidence missing	0
Partially implemented	1
Planned	0
Not in place	0
Not yet assessed	0
Not applicable	0
Applicable total	13

Control	Requirement	Status	Evidence recorded
VH-1	Identify & document vulnerabilities and components (SBOM)	In place	yes
VH-3	Apply effective and regular security tests and reviews	In place	yes
VH-9	Systematically document cybersecurity aspects (Art. 13(7))	In place	yes
VH-11	Exercise due diligence over integrated third-party & open-source components (Art. 13(5))	In place	yes
VH-2	Remediate vulnerabilities without delay	In place	yes
VH-7	Securely distribute updates	In place	yes

Control	Requirement	Status	Evidence recorded
VH-8	Disseminate updates without delay, free of charge, with advisories	In place	yes
VH-10	Keep issued security updates available >=10 years (Art. 13(9))	In place	yes
VH-12	Subsequent software versions: keep prior users on the maintained version (Art. 13(10))	In place	yes
VH-13	Keep a record of issued security updates (Art. 13(9) / Annex I Part II(8))	In place	yes
VH-4	Publicly disclose information about fixed vulnerabilities	Partially implemented	yes
VH-5	Coordinated vulnerability disclosure (CVD) policy	In place	yes
VH-6	Facilitate information sharing & provide a reporting contact	In place	yes

Recorded implementation and evidence

VH-1 - Identify & document vulnerabilities and components (SBOM)

In place

Implementation Implemented in the reference control-system architecture and applied across the MX series; deviations are tracked in the risk register.

Evidence Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

VH-3 - Apply effective and regular security tests and reviews

In place

Implementation Built into the product platform, so every variant inherits it; deviations need an approved exception in the risk register.

Evidence Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "VH-3" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

VH-9 - Systematically document cybersecurity aspects (Art. 13(7))

In place

Implementation Implemented in the hardening baseline applied to every shipped controller, with the deviations list kept per customer.

Evidence Configuration audit pack SCR-VH-9 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-VH-9/, cross-checked against hardening baseline HB-2.

VH-11 - Exercise due diligence over integrated third-party & open-source components (Art. 13(5))

In place

Implementation Documented in the secure development policy and enforced as a blocking release-gate check; owner: product security officer.

Evidence Release checklist RC-2.1, gate "VH-11" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

VH-2 - Remediate vulnerabilities without delay

In place

Implementation Covered by the engineering work instruction and checked at the design review; the reviewer signs the checklist before release.

Evidence Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

VH-7 - Securely distribute updates

In place

Implementation Assigned to the product security officer, executed per release and recorded in the release checklist.

Evidence FAT/SAT acceptance report FAT-2026-11, case "VH-7 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

VH-8 - Disseminate updates without delay, free of charge, with advisories — In place

Implementation Carried by the supplier agreements and verified on intake, with the acceptance record kept per delivery.

Evidence Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

VH-10 - Keep issued security updates available >=10 years (Art. 13(9)) — In place

Implementation Automated in the CI/CD pipeline (build fails on violation); the manual fallback is described in the operations runbook.

Evidence Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "VH-10" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

VH-12 - Subsequent software versions: keep prior users on the maintained version (Art. 13(10)) — In place

Implementation Handled by the toolchain: the setting is fixed in the build configuration and verified by an automated check on every merge.

Evidence Configuration audit pack SCR-VH-12 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-VH-12/, cross-checked against hardening baseline HB-2.

VH-13 - Keep a record of issued security updates (Art. 13(9) / Annex I Part II(8)) — In place

Implementation Part of the design rules for the control system; conformance is sampled in the internal audit twice a year.

Evidence Release checklist RC-2.1, gate "VH-13" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

VH-4 - Publicly disclose information about fixed vulnerabilities — Partially implemented

Implementation Fixed vulnerabilities are disclosed to registered machine owners via the customer portal; the PUBLIC advisory page is still in build (epic SEC-540, target Sep 2026).

Evidence Interim: portal advisory archive (customer-portal/advisories) + epic SEC-540. The public page and its process note complete this item.

VH-5 - Coordinated vulnerability disclosure (CVD) policy — In place

Implementation Built into the product platform, so every variant inherits it; deviations need an approved exception in the risk register.

Evidence FAT/SAT acceptance report FAT-2026-11, case "VH-5 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

VH-6 - Facilitate information sharing & provide a reporting contact — In place

Implementation Implemented in the hardening baseline applied to every shipped controller, with the deviations list kept per customer.

Evidence Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

Incident & vulnerability reporting (CRA Art. 14)

Status	Count
In place	7
In place, evidence missing	0
Partially implemented	0
Planned	0
Not in place	0
Not yet assessed	0
Not applicable	0
Applicable total	7

Control	Requirement	Status	Evidence recorded

Control	Requirement	Status	Evidence recorded
IR-1	Awareness of the reporting duty and deadlines	**In place**	yes
IR-2	Documented incident-response process & ownership	**In place**	yes
IR-3	Single reporting platform (Art. 16) set-up	**In place**	yes
IR-4	Actively-exploited-vulnerability notification (24h / 72h / 14-day)	**In place**	yes
IR-5	Severe-incident notification (24h / 72h / 1-month) & severity criteria	**In place**	yes
IR-7	Intermediate report on CSIRT request (Art. 14(6))	**In place**	yes
IR-6	Inform impacted users	**In place**	yes

Recorded implementation and evidence

IR-1 - Awareness of the reporting duty and deadlines — In place

Implementation Covered by the engineering work instruction and checked at the design review; the reviewer signs the checklist before release.

Evidence Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

IR-2 - Documented incident-response process & ownership — In place

Implementation Assigned to the product security officer, executed per release and recorded in the release checklist.

Evidence FAT/SAT acceptance report FAT-2026-11, case "IR-2 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

IR-3 - Single reporting platform (Art. 16) set-up — In place

Implementation Carried by the supplier agreements and verified on intake, with the acceptance record kept per delivery.

Evidence Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

IR-4 - Actively-exploited-vulnerability notification (24h / 72h / 14-day) — In place

Implementation Automated in the CI/CD pipeline (build fails on violation); the manual fallback is described in the operations runbook.

Evidence Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "IR-4" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

IR-5 - Severe-incident notification (24h / 72h / 1-month) & severity criteria — In place

Implementation Handled by the toolchain: the setting is fixed in the build configuration and verified by an automated check on every merge.

Evidence Configuration audit pack SCR-IR-5 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-IR-5/, cross-checked against hardening baseline HB-2.

IR-7 - Intermediate report on CSIRT request (Art. 14(6)) — In place

Implementation Part of the design rules for the control system; conformance is sampled in the internal audit twice a year.

Evidence Release checklist RC-2.1, gate "IR-7" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

IR-6 - Inform impacted users — In place

Implementation Implemented in the reference control-system architecture and applied across the MX series; deviations are tracked in the risk register.

Evidence Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

Placing on market & post-market (CRA Art. 13(14)–(23) / Art. 23)

Status	Count
In place	10
In place, evidence missing	0
Partially implemented	0
Planned	0
Not in place	0
Not yet assessed	0
Not applicable	0
Applicable total	10

Control	Requirement	Status	Evidence recorded
PM-1	Product identification (type / batch / serial) (Art. 13(15))	In place	yes
PM-2	Manufacturer name & contact on the product (Art. 13(16))	In place	yes
PM-3	Single point of contact for users (Art. 13(17))	In place	yes
PM-9	Support-period end date at the point of purchase (Art. 13(19))	In place	yes
PM-4	Series production stays in conformity (Art. 13(14))	In place	yes
PM-5	Corrective measures, withdrawal or recall (Art. 13(21))	In place	yes
PM-6	Information & cooperation on reasoned request (Art. 13(22))	In place	yes
PM-7	Traceability: who supplied / whom supplied (Art. 23)	In place	yes
PM-8	Cessation of operations (Art. 13(23))	In place	yes
PM-10	Public software archives: warn about unsupported software (Art. 13(11))	In place	yes

Recorded implementation and evidence

PM-1 - Product identification (type / batch / serial) (Art. 13(15)) — In place

Implementation Handled by the toolchain: the setting is fixed in the build configuration and verified by an automated check on every merge.

Evidence Configuration audit pack SCR-PM-1 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-PM-1/, cross-checked against hardening baseline HB-2.

PM-2 - Manufacturer name & contact on the product (Art. 13(16)) — In place

Implementation Part of the design rules for the control system; conformance is sampled in the internal audit twice a year.

Evidence Release checklist RC-2.1, gate "PM-2" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

PM-3 - Single point of contact for users (Art. 13(17)) — In place

Implementation Implemented in the reference control-system architecture and applied across the MX series; deviations are tracked in the risk register.

Evidence Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

PM-9 - Support-period end date at the point of purchase (Art. 13(19)) — In place

Implementation	Built into the product platform, so every variant inherits it; deviations need an approved exception in the risk register.
Evidence	FAT/SAT acceptance report FAT-2026-11, case "PM-9 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

PM-4 - Series production stays in conformity (Art. 13(14)) — In place

Implementation	Implemented in the hardening baseline applied to every shipped controller, with the deviations list kept per customer.
Evidence	Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

PM-5 - Corrective measures, withdrawal or recall (Art. 13(21)) — In place

Implementation	Documented in the secure development policy and enforced as a blocking release-gate check; owner: product security officer.
Evidence	Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "PM-5" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

PM-6 - Information & cooperation on reasoned request (Art. 13(22)) — In place

Implementation	Covered by the engineering work instruction and checked at the design review; the reviewer signs the checklist before release.
Evidence	Configuration audit pack SCR-PM-6 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-PM-6/, cross-checked against hardening baseline HB-2.

PM-7 - Traceability: who supplied / whom supplied (Art. 23) — In place

Implementation	Assigned to the product security officer, executed per release and recorded in the release checklist.
Evidence	Release checklist RC-2.1, gate "PM-7" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

PM-8 - Cessation of operations (Art. 13(23)) — In place

Implementation	Carried by the supplier agreements and verified on intake, with the acceptance record kept per delivery.
Evidence	Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

PM-10 - Public software archives: warn about unsupported software (Art. 13(11)) — In place

Implementation	Automated in the CI/CD pipeline (build fails on violation); the manual fallback is described in the operations runbook.
Evidence	FAT/SAT acceptance report FAT-2026-11, case "PM-10 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

Patch management (IEC 62443-2-3, optional) (IEC 62443-2-3)

Status	Count
In place	14
In place, evidence missing	0
Partially implemented	1
Planned	0
Not in place	0
Not yet assessed	0
Not applicable	0
Applicable total	15

Control	Requirement	Status	Evidence recorded

Control	Requirement	Status	Evidence recorded
SP-5-a	establish and maintain an inventory of all electronic	In place	yes
SP-5-b	establish and maintain an accurate record of the	In place	yes
SP-5-c	determine on a regular schedule what upgrades and	Partially implemented	yes
SP-5-d	determine on a regular schedule the `released versions'	In place	yes
SP-5-e	test the installation of IACS patches in a	In place	yes
SP-5-f	schedule authorized, effective patches for installation at the	In place	yes
SP-5-g	update records at a planned interval, at least	In place	yes
SP-5-h	identify a planned interval for installation of patches	In place	yes
SP-5-i	install patches and/or implement compensating countermeasures to mitigate	In place	yes
SP-6-a	provide documentation describing the software patching policy for	In place	yes
SP-6-b	qualify in terms of applicability and compatibility, all	In place	yes
SP-6-c	provide a list of all patches and their	In place	yes
SP-6-d	inform the asset owners, and update the list	In place	yes
SP-6-e	provide adequate warning (at least two years in	In place	yes
SP-6-f	provide information to IACS users regarding the policy	In place	yes

Recorded implementation and evidence

SP-5-a - establish and maintain an inventory of all electronic — In place

Implementation Implemented as a standing process across engineering and service, with the records kept per machine and per site.

Evidence Work instruction WI-SEC-SP-5-a with signed records from the last two maintenance cycles - service portal, 2026.

SP-5-b - establish and maintain an accurate record of the — In place

Implementation Implemented as a standing process across engineering and service, with the records kept per machine and per site.

Evidence IACS security programme handbook SP-01 v1.3, section SP-5-b (approved 3 Mar 2026); quarterly security board minutes Q1/Q2 2026.

SP-5-c - determine on a regular schedule what upgrades and — Partially implemented

Implementation Upgrades and patches for the supported control software are determined per release; the fixed quarterly review that IEC 62443-2-3 expects for the whole installed base starts in Q4 2026 (owner @mark).

Evidence Interim: release notes 3.1.x/3.2.0 with the component upgrade list; SBOM watch runs continuously.

SP-5-d - determine on a regular schedule the `released versions' — In place

Implementation Implemented as a standing process across engineering and service, with the records kept per machine and per site.

Evidence Work instruction WI-SEC-SP-5-d with signed records from the last two maintenance cycles - service portal, 2026.

SP-5-e - test the installation of IACS patches in a — In place

Implementation	Implemented as a standing process across engineering and service, with the records kept per machine and per site.
Evidence	IACS security programme handbook SP-01 v1.3, section SP-5-e (approved 3 Mar 2026); quarterly security board minutes Q1/Q2 2026.

SP-5-f - schedule authorized, effective patches for installation at the — In place

Implementation	Implemented as a standing process across engineering and service, with the records kept per machine and per site.
Evidence	Programme review R-2026-06 (12 Jun 2026): SP-5-f assessed effective; findings and actions in the programme action list.

SP-5-g - update records at a planned interval, at least — In place

Implementation	Implemented as a standing process across engineering and service, with the records kept per machine and per site.
Evidence	Work instruction WI-SEC-SP-5-g with signed records from the last two maintenance cycles - service portal, 2026.

SP-5-h - identify a planned interval for installation of patches — In place

Implementation	Implemented as a standing process across engineering and service, with the records kept per machine and per site.
Evidence	IACS security programme handbook SP-01 v1.3, section SP-5-h (approved 3 Mar 2026); quarterly security board minutes Q1/Q2 2026.

SP-5-i - install patches and/or implement compensating countermeasures to mitigate — In place

Implementation	Implemented as a standing process across engineering and service, with the records kept per machine and per site.
Evidence	Programme review R-2026-06 (12 Jun 2026): SP-5-i assessed effective; findings and actions in the programme action list.

SP-6-a - provide documentation describing the software patching policy for — In place

Implementation	Implemented as a standing process across engineering and service, with the records kept per machine and per site.
Evidence	Work instruction WI-SEC-SP-6-a with signed records from the last two maintenance cycles - service portal, 2026.

SP-6-b - qualify in terms of applicability and compatibility, all — In place

Implementation	Implemented as a standing process across engineering and service, with the records kept per machine and per site.
Evidence	IACS security programme handbook SP-01 v1.3, section SP-6-b (approved 3 Mar 2026); quarterly security board minutes Q1/Q2 2026.

SP-6-c - provide a list of all patches and their — In place

Implementation	Implemented as a standing process across engineering and service, with the records kept per machine and per site.
Evidence	Programme review R-2026-06 (12 Jun 2026): SP-6-c assessed effective; findings and actions in the programme action list.

SP-6-d - inform the asset owners, and update the list — In place

Implementation	Implemented as a standing process across engineering and service, with the records kept per machine and per site.
Evidence	Work instruction WI-SEC-SP-6-d with signed records from the last two maintenance cycles - service portal, 2026.

SP-6-e - provide adequate warning (at least two years in — In place

Implementation Implemented as a standing process across engineering and service, with the records kept per machine and per site.

Evidence IACS security programme handbook SP-01 v1.3, section SP-6-e (approved 3 Mar 2026); quarterly security board minutes Q1/Q2 2026.

SP-6-f - provide information to IACS users regarding the policy — In place

Implementation Implemented as a standing process across engineering and service, with the records kept per machine and per site.

Evidence Programme review R-2026-06 (12 Jun 2026): SP-6-f assessed effective; findings and actions in the programme action list.

Vulnerability disclosure (ISO/IEC 29147) (ISO/IEC 29147:2020)

Status	Count
In place	20
In place, evidence missing	0
Partially implemented	1
Planned	0
Not in place	0
Not yet assessed	0
Not applicable	0
Applicable total	21

Control	Requirement	Status	Evidence recorded
CVD-6.1	General	In place	yes
CVD-6.2	Vulnerability reports	In place	yes
CVD-6.3	Initial assessment	In place	yes
CVD-6.4	Further investigation	In place	yes
CVD-6.5	On-going communication	In place	yes
CVD-6.6	Coordinator involvement	In place	yes
CVD-6.7	Operational security	In place	yes
CVD-7.1	General	In place	yes
CVD-7.2	Advisory	In place	yes
CVD-7.3	Advisory publication timing	Partially implemented	yes
CVD-7.4	Advisory elements	In place	yes
CVD-7.5	Advisory communication	In place	yes
CVD-7.6	Advisory format	In place	yes
CVD-7.7	Advisory authenticity	In place	yes
CVD-7.8	Remediations	In place	yes
CVD-8.1	General	In place	yes
CVD-8.2	Vendors playing multiple roles	In place	yes
CVD-9.1	General	In place	yes
CVD-9.2	Required policy elements	In place	yes
CVD-9.3	Recommended policy elements	In place	yes
CVD-9.4	Optional policy elements	In place	yes

Recorded implementation and evidence

CVD-6.1 - General

In place

Implementation Operated through the security contact and the case register: every report is recorded, acknowledged and tracked to closure.

Evidence Case register entries CASE-1 (reported under CRA Art. 14) and CASE-2 (handled, not reportable), both covering CVD-6.1.

CVD-6.2 - Vulnerability reports

In place

Implementation Operated through the security contact and the case register: every report is recorded, acknowledged and tracked to closure.

Evidence Procedure POP-07 v1.5 (Jan 2026), step CVD-6.2 - QMS 04-Procedures; worked through end to end in cases CASE-1 and CASE-2.

CVD-6.3 - Initial assessment

In place

Implementation Operated through the security contact and the case register: every report is recorded, acknowledged and tracked to closure.

Evidence Advisory SA-2026-001 and SA-2026-002 as the published artefacts of CVD-6.3; disclosure policy in the product manuals.

CVD-6.4 - Further investigation

In place

Implementation Operated through the security contact and the case register: every report is recorded, acknowledged and tracked to closure.

Evidence Case register entries CASE-1 (reported under CRA Art. 14) and CASE-2 (handled, not reportable), both covering CVD-6.4.

CVD-6.5 - On-going communication

In place

Implementation Operated through the security contact and the case register: every report is recorded, acknowledged and tracked to closure.

Evidence Procedure POP-07 v1.5 (Jan 2026), step CVD-6.5 - QMS 04-Procedures; worked through end to end in cases CASE-1 and CASE-2.

CVD-6.6 - Coordinator involvement

In place

Implementation Operated through the security contact and the case register: every report is recorded, acknowledged and tracked to closure.

Evidence Advisory SA-2026-001 and SA-2026-002 as the published artefacts of CVD-6.6; disclosure policy in the product manuals.

CVD-6.7 - Operational security

In place

Implementation Operated through the security contact and the case register: every report is recorded, acknowledged and tracked to closure.

Evidence Case register entries CASE-1 (reported under CRA Art. 14) and CASE-2 (handled, not reportable), both covering CVD-6.7.

CVD-7.1 - General

In place

Implementation Operated through the security contact and the case register: every report is recorded, acknowledged and tracked to closure.

Evidence Procedure POP-07 v1.5 (Jan 2026), step CVD-7.1 - QMS 04-Procedures; worked through end to end in cases CASE-1 and CASE-2.

CVD-7.2 - Advisory

In place

Implementation Operated through the security contact and the case register: every report is recorded, acknowledged and tracked to closure.

Evidence Advisory SA-2026-001 and SA-2026-002 as the published artefacts of CVD-7.2; disclosure policy in the product manuals.

CVD-7.3 - Advisory publication timing

Partially implemented

Implementation	Advisories are published to registered machine owners within 5 working days of a fix; the publicly reachable advisory page that ISO/IEC 29147 clause 7.3 assumes is in build (epic SEC-540, target Sep 2026).
Evidence	Interim: portal advisory archive (customer-portal/advisories), SA-2026-001 published 21 May 2026. Epic SEC-540 carries the public page.

CVD-7.4 - Advisory elements

In place

Implementation	Operated through the security contact and the case register: every report is recorded, acknowledged and tracked to closure.
Evidence	Procedure POP-07 v1.5 (Jan 2026), step CVD-7.4 - QMS 04-Procedures; worked through end to end in cases CASE-1 and CASE-2.

CVD-7.5 - Advisory communication

In place

Implementation	Operated through the security contact and the case register: every report is recorded, acknowledged and tracked to closure.
Evidence	Advisory SA-2026-001 and SA-2026-002 as the published artefacts of CVD-7.5; disclosure policy in the product manuals.

CVD-7.6 - Advisory format

In place

Implementation	Operated through the security contact and the case register: every report is recorded, acknowledged and tracked to closure.
Evidence	Case register entries CASE-1 (reported under CRA Art. 14) and CASE-2 (handled, not reportable), both covering CVD-7.6.

CVD-7.7 - Advisory authenticity

In place

Implementation	Operated through the security contact and the case register: every report is recorded, acknowledged and tracked to closure.
Evidence	Procedure POP-07 v1.5 (Jan 2026), step CVD-7.7 - QMS 04-Procedures; worked through end to end in cases CASE-1 and CASE-2.

CVD-7.8 - Remediations

In place

Implementation	Operated through the security contact and the case register: every report is recorded, acknowledged and tracked to closure.
Evidence	Advisory SA-2026-001 and SA-2026-002 as the published artefacts of CVD-7.8; disclosure policy in the product manuals.

CVD-8.1 - General

In place

Implementation	Operated through the security contact and the case register: every report is recorded, acknowledged and tracked to closure.
Evidence	Case register entries CASE-1 (reported under CRA Art. 14) and CASE-2 (handled, not reportable), both covering CVD-8.1.

CVD-8.2 - Vendors playing multiple roles

In place

Implementation	Operated through the security contact and the case register: every report is recorded, acknowledged and tracked to closure.
Evidence	Procedure POP-07 v1.5 (Jan 2026), step CVD-8.2 - QMS 04-Procedures; worked through end to end in cases CASE-1 and CASE-2.

CVD-9.1 - General

In place

Implementation	Operated through the security contact and the case register: every report is recorded, acknowledged and tracked to closure.
Evidence	Advisory SA-2026-001 and SA-2026-002 as the published artefacts of CVD-9.1; disclosure policy in the product manuals.

CVD-9.2 - Required policy elements

In place

Implementation	Operated through the security contact and the case register: every report is recorded, acknowledged and tracked to closure.
Evidence	Case register entries CASE-1 (reported under CRA Art. 14) and CASE-2 (handled, not reportable), both covering CVD-9.2.

CVD-9.3 - Recommended policy elements

In place

Implementation	Operated through the security contact and the case register: every report is recorded, acknowledged and tracked to closure.
Evidence	Procedure POP-07 v1.5 (Jan 2026), step CVD-9.3 - QMS 04-Procedures; worked through end to end in cases CASE-1 and CASE-2.

CVD-9.4 - Optional policy elements

In place

Implementation	Operated through the security contact and the case register: every report is recorded, acknowledged and tracked to closure.
Evidence	Advisory SA-2026-001 and SA-2026-002 as the published artefacts of CVD-9.4; disclosure policy in the product manuals.

Vulnerability handling process (ISO/IEC 30111) (ISO/IEC 30111:2020)

Status	Count
In place	17
In place, evidence missing	0
Partially implemented	0
Planned	0
Not in place	0
Not yet assessed	0
Not applicable	0
Applicable total	17

Control	Requirement	Status	Evidence recorded
VHP-6.1	General	In place	yes
VHP-6.2	Leadership	In place	yes
VHP-6.3	Vulnerability handling policy development	In place	yes
VHP-6.4	Organizational framework development	In place	yes
VHP-6.5	Vendor CSIRT or PSIRT	In place	yes
VHP-6.6	Responsibilities of the product business division	In place	yes
VHP-6.7	Responsibilities of customer support and public relations	In place	yes
VHP-6.8	Legal consultation	In place	yes
VHP-7.1-post-release	Vulnerability handling phases - Post-release	In place	yes
VHP-7.1-preparation	Vulnerability handling phases - Preparation	In place	yes
VHP-7.1-receipt	Vulnerability handling phases - Receipt	In place	yes
VHP-7.1-release	Vulnerability handling phases - Release	In place	yes
VHP-7.1-remediation	Vulnerability handling phases - Remediation development	In place	yes
VHP-7.1-verification	Vulnerability handling phases - Verification	In place	yes
VHP-7.2	Process monitoring	In place	yes
VHP-7.3	Confidentiality of vulnerability information	In place	yes
VHP-8	Supply chain considerations	In place	yes

Recorded implementation and evidence

VHP-6.1 - General

In place

Implementation Implemented in the vulnerability handling procedure POP-07: intake, triage, remediation and disclosure, with named owners and target times per severity.

Evidence Procedure POP-07 v1.5 (Jan 2026), step VHP-6.1 - QMS 04-Procedures; worked through end to end in cases CASE-1 and CASE-2.

VHP-6.2 - Leadership

In place

Implementation Implemented in the vulnerability handling procedure POP-07: intake, triage, remediation and disclosure, with named owners and target times per severity.

Evidence Advisory SA-2026-001 and SA-2026-002 as the published artefacts of VHP-6.2; disclosure policy in the product manuals.

VHP-6.3 - Vulnerability handling policy development

In place

Implementation Implemented in the vulnerability handling procedure POP-07: intake, triage, remediation and disclosure, with named owners and target times per severity.

Evidence Case register entries CASE-1 (reported under CRA Art. 14) and CASE-2 (handled, not reportable), both covering VHP-6.3.

VHP-6.4 - Organizational framework development

In place

Implementation Implemented in the vulnerability handling procedure POP-07: intake, triage, remediation and disclosure, with named owners and target times per severity.

Evidence Procedure POP-07 v1.5 (Jan 2026), step VHP-6.4 - QMS 04-Procedures; worked through end to end in cases CASE-1 and CASE-2.

VHP-6.5 - Vendor CSIRT or PSIRT

In place

Implementation Implemented in the vulnerability handling procedure POP-07: intake, triage, remediation and disclosure, with named owners and target times per severity.

Evidence Advisory SA-2026-001 and SA-2026-002 as the published artefacts of VHP-6.5; disclosure policy in the product manuals.

VHP-6.6 - Responsibilities of the product business division

In place

Implementation Implemented in the vulnerability handling procedure POP-07: intake, triage, remediation and disclosure, with named owners and target times per severity.

Evidence Case register entries CASE-1 (reported under CRA Art. 14) and CASE-2 (handled, not reportable), both covering VHP-6.6.

VHP-6.7 - Responsibilities of customer support and public relations

In place

Implementation Implemented in the vulnerability handling procedure POP-07: intake, triage, remediation and disclosure, with named owners and target times per severity.

Evidence Procedure POP-07 v1.5 (Jan 2026), step VHP-6.7 - QMS 04-Procedures; worked through end to end in cases CASE-1 and CASE-2.

VHP-6.8 - Legal consultation

In place

Implementation Implemented in the vulnerability handling procedure POP-07: intake, triage, remediation and disclosure, with named owners and target times per severity.

Evidence Advisory SA-2026-001 and SA-2026-002 as the published artefacts of VHP-6.8; disclosure policy in the product manuals.

VHP-7.1-post-release - Vulnerability handling phases - Post-release

In place

Implementation Implemented in the vulnerability handling procedure POP-07: intake, triage, remediation and disclosure, with named owners and target times per severity.

Evidence Case register entries CASE-1 (reported under CRA Art. 14) and CASE-2 (handled, not reportable), both covering VHP-7.1-post-release.

VHP-7.1-preparation - Vulnerability handling phases - Preparation — In place

Implementation Implemented in the vulnerability handling procedure POP-07: intake, triage, remediation and disclosure, with named owners and target times per severity.

Evidence Procedure POP-07 v1.5 (Jan 2026), step VHP-7.1-preparation - QMS 04-Procedures; worked through end to end in cases CASE-1 and CASE-2.

VHP-7.1-receipt - Vulnerability handling phases - Receipt — In place

Implementation Implemented in the vulnerability handling procedure POP-07: intake, triage, remediation and disclosure, with named owners and target times per severity.

Evidence Advisory SA-2026-001 and SA-2026-002 as the published artefacts of VHP-7.1-receipt; disclosure policy in the product manuals.

VHP-7.1-release - Vulnerability handling phases - Release — In place

Implementation Implemented in the vulnerability handling procedure POP-07: intake, triage, remediation and disclosure, with named owners and target times per severity.

Evidence Case register entries CASE-1 (reported under CRA Art. 14) and CASE-2 (handled, not reportable), both covering VHP-7.1-release.

VHP-7.1-remediation - Vulnerability handling phases - Remediation development — In place

Implementation Implemented in the vulnerability handling procedure POP-07: intake, triage, remediation and disclosure, with named owners and target times per severity.

Evidence Procedure POP-07 v1.5 (Jan 2026), step VHP-7.1-remediation - QMS 04-Procedures; worked through end to end in cases CASE-1 and CASE-2.

VHP-7.1-verification - Vulnerability handling phases - Verification — In place

Implementation Implemented in the vulnerability handling procedure POP-07: intake, triage, remediation and disclosure, with named owners and target times per severity.

Evidence Advisory SA-2026-001 and SA-2026-002 as the published artefacts of VHP-7.1-verification; disclosure policy in the product manuals.

VHP-7.2 - Process monitoring — In place

Implementation Implemented in the vulnerability handling procedure POP-07: intake, triage, remediation and disclosure, with named owners and target times per severity.

Evidence Case register entries CASE-1 (reported under CRA Art. 14) and CASE-2 (handled, not reportable), both covering VHP-7.2.

VHP-7.3 - Confidentiality of vulnerability information — In place

Implementation Implemented in the vulnerability handling procedure POP-07: intake, triage, remediation and disclosure, with named owners and target times per severity.

Evidence Procedure POP-07 v1.5 (Jan 2026), step VHP-7.3 - QMS 04-Procedures; worked through end to end in cases CASE-1 and CASE-2.

VHP-8 - Supply chain considerations — In place

Implementation Implemented in the vulnerability handling procedure POP-07: intake, triage, remediation and disclosure, with named owners and target times per severity.

Evidence Advisory SA-2026-001 and SA-2026-002 as the published artefacts of VHP-8; disclosure policy in the product manuals.

Compliance documentation (CRA Art. 28/30/31)

Status	Count
In place	9
In place, evidence missing	0
Partially implemented	0
Planned	0
Not in place	0
Not yet assessed	0

Status	Count
Not applicable	0
Applicable total	9

Control	Requirement	Status	Evidence recorded
CD-1	EU declaration of conformity	**In place**	yes
CD-2	Conformity assessment completed	**In place**	yes
CD-3	CE marking	**In place**	yes
CD-9	Provide the EU DoC (or simplified DoC) with the product (Art. 13(20))	**In place**	yes
CD-4	Technical documentation (Annex VII)	**In place**	yes
CD-5	User information & instructions (Annex II)	**In place**	yes
CD-6	Support-period record	**In place**	yes
CD-7	Software bill of materials	**In place**	yes
CD-8	Authorised representative - written mandate (Art. 18)	**In place**	yes

Recorded implementation and evidence

CD-1 - EU declaration of conformity — In place

Implementation Implemented in the reference control-system architecture and applied across the MX series; deviations are tracked in the risk register.

Evidence Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

CD-2 - Conformity assessment completed — In place

Implementation Built into the product platform, so every variant inherits it; deviations need an approved exception in the risk register.

Evidence Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "CD-2" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

CD-3 - CE marking — In place

Implementation Implemented in the hardening baseline applied to every shipped controller, with the deviations list kept per customer.

Evidence Configuration audit pack SCR-CD-3 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-CD-3/, cross-checked against hardening baseline HB-2.

CD-9 - Provide the EU DoC (or simplified DoC) with the product (Art. 13(20)) — In place

Implementation Documented in the secure development policy and enforced as a blocking release-gate check; owner: product security officer.

Evidence Release checklist RC-2.1, gate "CD-9" signed off for control software v3.2.0 (8 May 2026) - release/3.2.0/checklist.pdf.

CD-4 - Technical documentation (Annex VII) — In place

Implementation Covered by the engineering work instruction and checked at the design review; the reviewer signs the checklist before release.

Evidence Procedure POP-07 v1.5 with signed training records (Jan 2026) - QMS folder 04-Procedures; sample check: 14 of 14 engineers current.

CD-5 - User information & instructions (Annex II) — In place

Implementation Assigned to the product security officer, executed per release and recorded in the release checklist.

Evidence FAT/SAT acceptance report FAT-2026-11, case "CD-5 verification" (11 Mar 2026) - signed by QA in test bay 2; artifacts under qms/fat/2026-11/.

CD-6 - Support-period record — In place

Implementation	Carried by the supplier agreements and verified on intake, with the acceptance record kept per delivery.
Evidence	Machine risk & security assessment RA-MX540 v1.6 (EN ISO 12100 + security annex, 21 Jan 2026) - PLM vault RA-MX540; review ticket SEC-733 closed by the security architect.

CD-7 - Software bill of materials — In place

Implementation	Automated in the CI/CD pipeline (build fails on violation); the manual fallback is described in the operations runbook.
Evidence	Secure Development Policy PSP-01 v2.4 (approved 14 Feb 2026), section "CD-7" - QMS wiki/product-security/psp-01. Owner: product security officer (@daan); management review Feb 2026.

CD-8 - Authorised representative - written mandate (Art. 18) — In place

Implementation	Handled by the toolchain: the setting is fixed in the build configuration and verified by an automated check on every merge.
Evidence	Configuration audit pack SCR-CD-8 + controller audit-log excerpt (5 Jun 2026) - evidence/scr-CD-8/, cross-checked against hardening baseline HB-2.

Gap analysis

4 open item(s) across 4 control set(s).

Secure development lifecycle

- SVV-4 Penetration testing - Planned

Vulnerability handling & disclosure (CVD)

- VH-4 Publicly disclose information about fixed vulnerabilities - Partially implemented

Patch management (IEC 62443-2-3, optional)

- SP-5-c determine on a regular schedule what upgrades and - Partially implemented

Vulnerability disclosure (ISO/IEC 29147)

- CVD-7.3 Advisory publication timing - Partially implemented

Recommendations

Priority: Partially implemented

1. Complete the implementation of VH-4 (Publicly disclose information about fixed vulnerabilities) - Vulnerability handling & disclosure (CVD).

2. Complete the implementation of SP-5-c (determine on a regular schedule what upgrades and) - Patch management (IEC 62443-2-3, optional).

3. Complete the implementation of CVD-7.3 (Advisory publication timing) - Vulnerability disclosure (ISO/IEC 29147).

Priority: Planned

4. Execute the plan for SVV-4 (Penetration testing) - Secure development lifecycle.

Evidence and attachments

162 of 162 requirement(s) carry recorded evidence; it is printed with each requirement under "Recorded implementation and evidence".

File attachments per requirement are kept in the project folder under evidence/ and travel with the audit binder export, in the same control-by-control structure.

Review and sign-off

Role	Name	Date	Signature
Prepared by			
Reviewed by			
Approved by (management)			