CYBERGLASS RAIL CYBERSECURITY PROGRAM · FOUNDATIONS KIT

Start Here: Building Your Rail Cybersecurity Program

A step-by-step guide to using this kit: what each document is for, the order to use them, who to involve, how to adapt them, and the pitfalls to avoid.

Organization	[Company Name]
Document ID	RAIL-00
Document owner	[Name, title]
Approved by	[Name, title]
Version	1.0 [draft / approved]
Effective date	[YYYY-MM-DD]
Next review	[YYYY-MM-DD] (at least every 12 months)
Classification	Internal

PREVIEW

About this template (delete this box before publishing)

This document is a template to help [Company Name] write its own policy. It is a guideline based on common industry practice and publicly available frameworks, not a finished policy, legal advice or a guarantee of compliance. Every organization is different: review each requirement, remove what does not apply, add what is missing, and set values your organization can actually meet. Have the final version reviewed by people who know your systems, obligations and risks.

- Read this guide before opening any other document in the kit.
- Use section 5 to choose your starting point based on your role.
- Keep this guide for reference; it does not need to be published.
- Replace every highlighted **[placeholder]** with your organization's details, then remove the highlighting.
- Grey **Guidance** boxes explain what auditors, insurers and clients look for. Read them, then delete them before publishing.

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

When	What happened	What it means for this document
Oct 2022	Trains across a Scandinavian national operator stopped for several hours on a Saturday morning after criminals attacked a test environment at a subcontractor of the supplier whose platform gives drivers safety-critical operating information on tablets.	A supplier's platform stopped trains. Supplier and subcontractor security is part of the program from day one.
Aug 2023	More than 20 trains in Central Europe were brought to an automatic emergency stop by unauthorized 'radio-stop' tones broadcast on the unencrypted 150 MHz analogue train radio. The tones were publicly documented and the radio equipment was cheap.	Legacy, unauthenticated train radio was enough to stop trains. Legacy systems need a plan, not just an exception.
Mar 2023	The EU cybersecurity agency's study of transport incidents (Jan 2021 to Oct 2022) found ransomware was the most prominent threat (38%), that most attacks hit IT systems but still disrupted operations, and that ransomware groups are likely to target OT.	Ransomware is the main threat to transport, and most attacks begin in IT.

Summarized by CyberGlass from public reporting: The Olive Press and Rus Tourism News, Sep 2026; Ara and AP, May 2025; Security Affairs and Reuters, Nov 2022; International Railway Journal, Aug 2023; ENISA Transport Threat Landscape, Mar 2023. Organizations are described, not named. Figures are as publicly reported at the time.

How this document connects

Document or register	How records and decisions flow
RAIL-07 Context	First document to complete for a project
RAIL-08 Management Plan	Project plan built on the context
RAIL-05 Risk Method	Risk assessment and SL-T
RAIL-04 / RAIL-06	Operator-level policy and standard
Rail Workbook (Risk Register, Essential Functions, Security Conditions Register, Zones & Conduits)	Live records: R-NNN, EF-NN, SC-NNN, zones and SL-T
Hazard log (safety case)	Security events with safety consequences are cross-referenced, not duplicated

Record flow example: Context (RAIL-07) lists 'signalling data link' as an essential function EF-03 → RAIL-05 assessment sets SL-T 3 for the interlocking zone → RAIL-06 requirements apply → evidence in the security assurance report (RAIL-08 11.2).

PREVIEW

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

CYBERGLASS RAIL CYBERSECURITY PROGRAM · FOUNDATIONS KIT

Rail Cybersecurity Program Charter

Establishes the cybersecurity program for [Company Name]'s railway systems, aligned with CLC/TS 50701 (successor: IEC 63452), ISA/IEC 62443 and the EN 50126 lifecycle.

Organization	[Company Name]
Document ID	RAIL-01
Document owner	[Name, title]
Approved by	[Name, title]
Version	1.0 [draft / approved]
Effective date	[YYYY-MM-DD]
Next review	[YYYY-MM-DD] (at least every 12 months)
Classification	Internal

PREVIEW

About this template (delete this box before publishing)

This document is a template to help [Company Name] write its own policy. It is a guideline based on common industry practice and publicly available frameworks, not a finished policy, legal advice or a guarantee of compliance. Every organization is different: review each requirement, remove what does not apply, add what is missing, and set values your organization can actually meet. Have the final version reviewed by people who know your systems, obligations and risks.

- First decide which role(s) [Company Name] plays: asset owner/operator, infrastructure manager, system integrator, product supplier or maintainer. The rest of the kit adapts to that.
- Write it with the heads of engineering, safety assurance and operations. Rail cybersecurity can't be separated from safety.
- Check which standard edition your contracts reference (CLC/TS 50701:2021, :2023 or IEC 63452) and record it in section 3.
- Replace every highlighted **[placeholder]** with your organization's details, then remove the highlighting.
- Grey **Guidance** boxes explain what auditors, insurers and clients look for. Read them, then delete them before publishing.

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

How this document connects

Document or register	How records and decisions flow
RAIL-03 Governance	Committee, safety-security interface, lifecycle
RAIL-04 Policy	Approved under this charter
Rail Workbook (Risk Register, Essential Functions, Security Conditions Register, Zones & Conduits)	Live records: R-NNN, EF-NN, SC-NNN, zones and SL-T
Hazard log (safety case)	Security events with safety consequences are cross-referenced, not duplicated

Record flow example: Charter objective 'all supplier remote access via approved gateway' → Remote Access sheet → R-005 closed when last vendor VPN removed.

PREVIEW

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

CYBERGLASS RAIL CYBERSECURITY PROGRAM · FOUNDATIONS KIT

Rail First 90 Days Plan

A practical 30-60-90 day plan for a new rail cybersecurity lead at [Company Name], following the CLC/TS 50701 approach.

Organization	[Company Name]
Document ID	RAIL-02
Document owner	[Name, title]
Approved by	[Name, title]
Version	1.0 [draft / approved]
Effective date	[YYYY-MM-DD]
Next review	[YYYY-MM-DD] (at least every 12 months)
Classification	Internal

PREVIEW

About this template (delete this box before publishing)

This document is a template to help [Company Name] write its own policy. It is a guideline based on common industry practice and publicly available frameworks, not a finished policy, legal advice or a guarantee of compliance. Every organization is different: review each requirement, remove what does not apply, add what is missing, and set values your organization can actually meet. Have the final version reviewed by people who know your systems, obligations and risks.

- Rail access is controlled for safety. Arrange track safety training and escorts before site visits.
- Never connect tools or run scans on signalling, onboard or SCADA networks without engineering and safety approval, and only in an approved possession or test window.
- Align changes with engineering change processes and possessions.
- Replace every highlighted **[placeholder]** with your organization's details, then remove the highlighting.
- Grey **Guidance** boxes explain what auditors, insurers and clients look for. Read them, then delete them before publishing.

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

Document or register	How records and decisions flow
RAIL-05 Risk Method	Initial risk assessment by day 90
Rail Workbook (Risk Register, Essential Functions, Security Conditions Register, Zones & Conduits)	Live records: R-NNN, EF-NN, SC-NNN, zones and SL-T
Hazard log (safety case)	Security events with safety consequences are cross-referenced, not duplicated

Record flow example: Day 14 interview: maintainers use personal laptops on signalling equipment → R-008 → controlled maintenance laptops issued by day 60 → RAIL-06 3.9 applies.

PREVIEW

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

CYBERGLASS RAIL CYBERSECURITY PROGRAM · FOUNDATIONS KIT

Rail Cybersecurity Governance Framework

How cybersecurity is managed across the railway lifecycle at [Company Name]: management plan, safety-security interface, security conditions of use, security assurance report, deliverables and supplier requirements.

Organization	[Company Name]
Document ID	RAIL-03
Document owner	[Name, title]
Approved by	[Name, title]
Version	1.0 [draft / approved]
Effective date	[YYYY-MM-DD]
Next review	[YYYY-MM-DD] (at least every 12 months)
Classification	Internal

PREVIEW

About this template (delete this box before publishing)

This document is a template to help [Company Name] write its own policy. It is a guideline based on common industry practice and publicly available frameworks, not a finished policy, legal advice or a guarantee of compliance. Every organization is different: review each requirement, remove what does not apply, add what is missing, and set values your organization can actually meet. Have the final version reviewed by people who know your systems, obligations and risks.

- Section 4 (safety-security interface) is the most important part. Agree it with your safety assurance team and independent safety assessor.
- Use section 5 to place cybersecurity activities and deliverables into every project's lifecycle plan.
- Attach sections 6 and 7 to supplier and integrator contracts.
- Replace every highlighted **[placeholder]** with your organization's details, then remove the highlighting.
- Grey **Guidance** boxes explain what auditors, insurers and clients look for. Read them, then delete them before publishing.

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

When	What happened	What it means for this document
Aug 2023	More than 20 trains in Central Europe were brought to an automatic emergency stop by unauthorized 'radio-stop' tones broadcast on the unencrypted 150 MHz analogue train radio. The tones were publicly documented and the radio equipment was cheap.	Legacy systems (section 3) need compensating countermeasures and a migration date.

Summarized by CyberGlass from public reporting: The Olive Press and Rus Tourism News, Sep 2026; Security Affairs and Reuters, Nov 2022; International Railway Journal, Aug 2023. Organizations are described, not named. Figures are as publicly reported at the time.

How this document connects

Document or register	How records and decisions flow
RAIL-08 Management Plan	Applies this framework to a project
RAIL-06 Standard	Technical requirements
Rail Workbook (Risk Register, Essential Functions, Security Conditions Register, Zones & Conduits)	Live records: R-NNN, EF-NN, SC-NNN, zones and SL-T
Hazard log (safety case)	Security events with safety consequences are cross-referenced, not duplicated

Record flow example: Legacy interlocking cannot support authentication → exception with compensating countermeasures (section 3) → SecRAC SC-004 'physical access to equipment room controlled' exported to operator → referenced in safety case.

PREVIEW

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

CYBERGLASS RAIL CYBERSECURITY PROGRAM · FOUNDATIONS KIT

Rail Cybersecurity Policy

[Company Name]'s commitment, objectives, values, risk appetite and accountabilities for the cybersecurity of its railway systems.

Organization	[Company Name]
Document ID	RAIL-04
Document owner	[Name, title]
Approved by	[Name, title]
Version	1.0 [draft / approved]
Effective date	[YYYY-MM-DD]
Next review	[YYYY-MM-DD] (at least every 12 months)
Classification	Internal

PREVIEW

About this template (delete this box before publishing)

This document is a template to help [Company Name] write its own policy. It is a guideline based on common industry practice and publicly available frameworks, not a finished policy, legal advice or a guarantee of compliance. Every organization is different: review each requirement, remove what does not apply, add what is missing, and set values your organization can actually meet. Have the final version reviewed by people who know your systems, obligations and risks.

- This is the Tier 1 policy. Keep it short and strategic; technical requirements belong in the Rail Cybersecurity Standard (RAIL-06) and system-specific risks in the rail risk register (RAIL-05).
- Have your Board or Executive set the risk appetite in section 5.1 before publishing.
- Agree sections 2.2, 4 and 9 with engineering and safety assurance. Rail cybersecurity cannot be separated from safety.
- Replace every highlighted **[placeholder]** with your organization's details, then remove the highlighting.
- Grey **Guidance** boxes explain what auditors, insurers and clients look for. Read them, then delete them before publishing.

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

When	What happened	What it means for this document
Mar 2023	The EU cybersecurity agency's study of transport incidents (Jan 2021 to Oct 2022) found ransomware was the most prominent threat (38%), that most attacks hit IT systems but still disrupted operations, and that ransomware groups are likely to target OT.	Appetite (5.1) should reflect ransomware as the leading threat.

Summarized by CyberGlass from public reporting: Ara and AP, May 2025; Security Affairs and Reuters, Nov 2022; ENISA Transport Threat Landscape, Mar 2023. Organizations are described, not named. Figures are as publicly reported at the time.

How this document connects

Document or register	How records and decisions flow
RAIL-06 Standard	Technical requirements
RAIL-05 Risk Method	Applies the appetite
RAIL-03 Governance	Exceptions and reporting
Rail Workbook (Risk Register, Essential Functions, Security Conditions Register, Zones & Conduits)	Live records: R-NNN, EF-NN, SC-NNN, zones and SL-T
Hazard log (safety case)	Security events with safety consequences are cross-referenced, not duplicated

Record flow example: Policy rule 'no unauthenticated remote commands to safety-related equipment' → RAIL-06 3.4/3.8 → legacy radio exception with migration plan → risk R-011.

PREVIEW

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

CYBERGLASS RAIL CYBERSECURITY PROGRAM · FOUNDATIONS KIT

Rail Cyber Risk Assessment Methodology

How [Company Name] defines systems under consideration, assesses cyber risk, partitions zones and conduits, derives target security levels and writes cybersecurity requirements, following CLC/TS 50701 clauses 6 and 7.

Organization	[Company Name]
Document ID	RAIL-05
Document owner	[Name, title]
Approved by	[Name, title]
Version	1.0 [draft / approved]
Effective date	[YYYY-MM-DD]
Next review	[YYYY-MM-DD] (at least every 12 months)
Classification	Internal

PREVIEW

About this template (delete this box before publishing)

This document is a template to help [Company Name] write its own policy. It is a guideline based on common industry practice and publicly available frameworks, not a finished policy, legal advice or a guarantee of compliance. Every organization is different: review each requirement, remove what does not apply, add what is missing, and set values your organization can actually meet. Have the final version reviewed by people who know your systems, obligations and risks.

- Run assessments with engineering, operations and safety assurance together.
- Adjust the service disruption and financial thresholds to your network before first use.
- Record results in the Rail-Workbook: Essential Functions, Risk Register, Zones & Conduits and Security Conditions Register sheets.
- Replace every highlighted **[placeholder]** with your organization's details, then remove the highlighting.
- Grey **Guidance** boxes explain what auditors, insurers and clients look for. Read them, then delete them before publishing.

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

When	What happened	What it means for this document
Aug 2023	More than 20 trains in Central Europe were brought to an automatic emergency stop by unauthorized 'radio-stop' tones broadcast on the unencrypted 150 MHz analogue train radio. The tones were publicly documented and the radio equipment was cheap.	A scenario to test your impact scale: low-cost attacker, legacy radio, many trains stopped.
Jan 2008	A teenager used a modified TV remote control to switch tram points in a Central European city, derailing four trams and injuring about a dozen people. The signalling interface accepted commands with no authentication.	Unauthenticated field commands can cause derailment; safety consequence reaches the top band.
Oct 2022	Trains across a Scandinavian national operator stopped for several hours on a Saturday morning after criminals attacked a test environment at a subcontractor of the supplier whose platform gives drivers safety-critical operating information on tablets.	Supplier-hosted tools can stop service without touching signalling.

Summarized by CyberGlass from public reporting: The Olive Press and Rus Tourism News, Sep 2026; Ara and AP, May 2025; International Railway Journal, Aug 2023; European press reporting, 2008; Security Affairs and Reuters, Nov 2022. Organizations are described, not named. Figures are as publicly reported at the time.

How this document connects

Document or register	How records and decisions flow
RAIL-07 Context	System under consideration and essential functions
RAIL-06 Standard	Countermeasures by FR
RAIL-08 Management Plan 5	Applies this method on a project
Rail Workbook (Risk Register, Essential Functions, Security Conditions Register, Zones & Conduits)	Live records: R-NNN, EF-NN, SC-NNN, zones and SL-T
Hazard log (safety case)	Security events with safety consequences are cross-referenced, not duplicated

Record flow example: Threat scenario 'maintenance laptop infects interlocking engineering workstation' → R-014 (L3 × I5) → SL-T 3 for engineering zone → countermeasures in RAIL-06 3.6/3.9 → residual risk Medium → SecRAC SC-007 'laptops controlled by operator' exported.

PREVIEW

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

CYBERGLASS RAIL CYBERSECURITY PROGRAM · FOUNDATIONS KIT

Rail Cybersecurity Standard

Mandatory technical cybersecurity requirements for [Company Name]'s railway systems, organized by the ISA/IEC 62443 foundational requirements and the CLC/TS 50701 lifecycle (successor IEC 63452).

Organization	[Company Name]
Document ID	RAIL-06
Document owner	[Name, title]
Approved by	[Name, title]
Version	1.0 [draft / approved]
Effective date	[YYYY-MM-DD]
Next review	[YYYY-MM-DD] (at least every 12 months)
Classification	Internal

PREVIEW

About this template (delete this box before publishing)

This document is a template to help [Company Name] write its own policy. It is a guideline based on common industry practice and publicly available frameworks, not a finished policy, legal advice or a guarantee of compliance. Every organization is different: review each requirement, remove what does not apply, add what is missing, and set values your organization can actually meet. Have the final version reviewed by people who know your systems, obligations and risks.

- This is the Tier 3 standard. It implements the Rail Cybersecurity Policy (RAIL-04); objectives, risk appetite and approval authorities are in the Policy.
- Replace every [bracketed] value with what your organization can actually achieve.
- "Shall" means mandatory, "should" means expected unless a documented reason exists, and "may" means optional.
- Agree sections 3.6, 3.12 and 6 with your safety assurance team and independent safety assessor before publishing.
- Replace every highlighted **[placeholder]** with your organization's details, then remove the highlighting.
- Grey **Guidance** boxes explain what auditors, insurers and clients look for. Read them, then delete them before publishing.

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

When	What happened	What it means for this document
Sep 2026	Attackers compromised servers at Spain's national rail infrastructure manager, then moved through connections into the national passenger operator's systems after weeks of attempts. Customer names and email addresses were stolen; trains ran normally. The incident was reported to Spain's National Cryptologic Centre.	Section 3.8 restricted data flow applies to links with partner rail organizations too.
Aug 2023	More than 20 trains in Central Europe were brought to an automatic emergency stop by unauthorized 'radio-stop' tones broadcast on the unencrypted 150 MHz analogue train radio. The tones were publicly documented and the radio equipment was cheap.	Section 3.8 and 3.4: commands to safety-related equipment must be authenticated or the channel isolated.
Sep 2024	Public Wi-Fi landing pages at 19 major UK railway stations were defaced with a hateful message through the Wi-Fi service provider's administration system. Station Wi-Fi was suspended while police investigated; a man was later arrested.	Section 3.9 and 3.14: provider admin access to passenger systems must be controlled and monitored.

Summarized by CyberGlass from public reporting: Ara and AP, May 2025; The Olive Press and Rus Tourism News, Sep 2026; International Railway Journal, Aug 2023; UK news reporting, Sep 2024. Organizations are described, not named. Figures are as publicly reported at the time.

How this document connects

Document or register	How records and decisions flow
RAIL-04 Policy	Policy basis
RAIL-05 Risk Method	SL-T per zone decides which requirements apply
RAIL-08 Management Plan	Verification and assurance evidence
Rail Workbook (Risk Register, Essential Functions, Security Conditions Register, Zones & Conduits)	Live records: R-NNN, EF-NN, SC-NNN, zones and SL-T
Hazard log (safety case)	Security events with safety consequences are cross-referenced, not duplicated

Record flow example: Vulnerability advisory for a station network switch (CVSS 8.1) → compensating control in 30 days → patch in next possession → Vulnerabilities sheet closed.

PREVIEW

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

CYBERGLASS RAIL CYBERSECURITY PROGRAM · FOUNDATIONS KIT

Rail Cybersecurity Context

The starting point for every rail cybersecurity project: stakeholders, system and environment, essential functions, obligations, threat landscape, risk acceptance principles, objectives and assumptions.

Organization	[Company Name]
Document ID	RAIL-07
Document owner	[Name, title]
Approved by	[Name, title]
Version	1.0 [draft / approved]
Effective date	[YYYY-MM-DD]
Next review	[YYYY-MM-DD] (at least every 12 months)
Classification	Internal

PREVIEW

About this template (delete this box before publishing)

This document is a template to help [Company Name] write its own policy. It is a guideline based on common industry practice and publicly available frameworks, not a finished policy, legal advice or a guarantee of compliance. Every organization is different: review each requirement, remove what does not apply, add what is missing, and set values your organization can actually meet. Have the final version reviewed by people who know your systems, obligations and risks.

- Complete this document first, at the concept phase, and keep it current until decommissioning.
- Work through it with the operator, safety assurance and key suppliers. Most later disputes come from assumptions nobody wrote down.
- Every assumption that must stay true in operation should become a security condition of use in the security conditions register.
- Replace every highlighted **[placeholder]** with your organization's details, then remove the highlighting.
- Grey **Guidance** boxes explain what auditors, insurers and clients look for. Read them, then delete them before publishing.

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

When	What happened	What it means for this document
Aug 2023	More than 20 trains in Central Europe were brought to an automatic emergency stop by unauthorized 'radio-stop' tones broadcast on the unencrypted 150 MHz analogue train radio. The tones were publicly documented and the radio equipment was cheap.	Section 6.3 should consider low-cost attackers and legacy radio.

Summarized by CyberGlass from public reporting: The Olive Press and Rus Tourism News, Sep 2026; Security Affairs and Reuters, Nov 2022; International Railway Journal, Aug 2023. Organizations are described, not named. Figures are as publicly reported at the time.

How this document connects

Document or register	How records and decisions flow
RAIL-05 Risk Method	Uses this context
RAIL-08 Management Plan	Refers to the context and its assumptions
Rail Workbook (Risk Register, Essential Functions, Security Conditions Register, Zones & Conduits)	Live records: R-NNN, EF-NN, SC-NNN, zones and SL-T
Hazard log (safety case)	Security events with safety consequences are cross-referenced, not duplicated

Record flow example: Assumption 'equipment rooms are physically secured' (section 9) → exported as SecRAC SC-002 → operator confirms ownership at handover.

PREVIEW

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

CYBERGLASS RAIL CYBERSECURITY PROGRAM · FOUNDATIONS KIT

Rail Cybersecurity Management Plan

How cybersecurity will be organized, managed, designed, tested, assured and handed over on a rail project, from roles and risk management to suppliers, deliverables and the security assurance report.

Organization	[Company Name]
Document ID	RAIL-08
Document owner	[Name, title]
Approved by	[Name, title]
Version	1.0 [draft / approved]
Effective date	[YYYY-MM-DD]
Next review	[YYYY-MM-DD] (at least every 12 months)
Classification	Internal

PREVIEW

About this template (delete this box before publishing)

This document is a template to help [Company Name] write its own policy. It is a guideline based on common industry practice and publicly available frameworks, not a finished policy, legal advice or a guarantee of compliance. Every organization is different: review each requirement, remove what does not apply, add what is missing, and set values your organization can actually meet. Have the final version reviewed by people who know your systems, obligations and risks.

- Prepare this plan alongside the project safety plan and agree it with the operator and independent assessor.
- Replace the generic role and document names (section 1.3) with your own, and map Appendix 1 to your project lifecycle.
- Update the plan at every gate; an out-of-date plan is a common assessment finding.
- Replace every highlighted **[placeholder]** with your organization's details, then remove the highlighting.
- Grey **Guidance** boxes explain what auditors, insurers and clients look for. Read them, then delete them before publishing.

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

When	What happened	What it means for this document
Oct 2022	Trains across a Scandinavian national operator stopped for several hours on a Saturday morning after criminals attacked a test environment at a subcontractor of the supplier whose platform gives drivers safety-critical operating information on tablets.	Supply chain (section 9) must cover subcontractors and test environments.
Aug 2023	More than 20 trains in Central Europe were brought to an automatic emergency stop by unauthorized 'radio-stop' tones broadcast on the unencrypted 150 MHz analogue train radio. The tones were publicly documented and the radio equipment was cheap.	Section 2.2 assumptions should state which legacy interfaces remain and how they are protected.
Sep 2025	Ransomware at a third-party supplier of shared check-in and boarding software disrupted Heathrow, Brussels and Berlin airports, forcing manual check-in. The EU cybersecurity agency confirmed a 'third-party ransomware incident'.	Third-party platforms in transport can stop operations; section 9 and 8.3 cover support after handover.

Summarized by CyberGlass from public reporting: The Olive Press and Rus Tourism News, Sep 2026; Security Affairs and Reuters, Nov 2022; International Railway Journal, Aug 2023; ENISA statement reported by TechCrunch, Sep 2025. Organizations are described, not named. Figures are as publicly reported at the time.

How this document connects

Document or register	How records and decisions flow
RAIL-07 Context	D-01 deliverable
RAIL-05 Risk Method	D-04 and D-05
RAIL-06 Standard	Requirements allocated in D-06
Project Deliverables Tracker (workbook)	D-01 to D-12 by EN 50126 phase gate
Rail Workbook (Risk Register, Essential Functions, Security Conditions Register, Zones & Conduits)	Live records: R-NNN, EF-NN, SC-NNN, zones and SL-T
Hazard log (safety case)	Security events with safety consequences are cross-referenced, not duplicated

Record flow example: D-05 detailed risk assessment sets SL-T 3 for interlocking zone → D-06 requirements allocated to supplier → D-09 verification finds default password → issue V-012 closed before Phase 9 gate → D-11 assurance report → SecRACs SC-001 to SC-009 handed over (D-12).

PREVIEW

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

CYBERGLASS RAIL CYBERSECURITY PROGRAM · FOUNDATIONS KIT

Rail Cyber Incident Response Playbooks

Safety-first triage, roles and playbooks that extend the Incident Response Plan (IT-06) to signalling, train control, rolling stock, control centres and stations at [Company Name].

Organization	[Company Name]
Document ID	RAIL-09
Document owner	[Name, title]
Approved by	[Name, title]
Version	1.0 [draft / approved]
Effective date	[YYYY-MM-DD]
Next review	[YYYY-MM-DD] (at least every 12 months)
Classification	Internal

PREVIEW

About this template (delete this box before publishing)

This document is a template to help [Company Name] write its own policy. It is a guideline based on common industry practice and publicly available frameworks, not a finished policy, legal advice or a guarantee of compliance. Every organization is different: review each requirement, remove what does not apply, add what is missing, and set values your organization can actually meet. Have the final version reviewed by people who know your systems, obligations and risks.

- Use this with the Incident Response Plan (IT-06). IT-06 sets the general process; this document covers what is different on a railway.
- Review the triage (section 3) and each playbook with the control centre, Safety Assurance and your main suppliers before approval.
- Exercise at least one playbook a year with the control centre, not only the IT team.
- Replace every highlighted **[placeholder]** with your organization's details, then remove the highlighting.
- Grey **Guidance** boxes explain what auditors, insurers and clients look for. Read them, then delete them before publishing.

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

When	What happened	What it means for this document
Oct 2022	Trains across a Scandinavian national operator stopped for several hours on a Saturday morning after criminals attacked a test environment at a subcontractor of the supplier whose platform gives drivers safety-critical operating information on tablets.	Playbook 6.4: a supplier's platform used by drivers failed; fall-back procedures kept safety intact while service stopped.
May 2025	About 150 m of copper cable feeding signalling and safety systems was cut at five points on Spain's Madrid–Seville high-speed line overnight. Around 30 trains and more than 10,700 passengers were delayed; the transport minister called it deliberate sabotage.	Playbook 6.6: cut signalling cables at several points need police, protection of the line and a check for tampering.
Sep 2026	Attackers compromised servers at Spain's national rail infrastructure manager, then moved through connections into the national passenger operator's systems after weeks of attempts. Customer names and email addresses were stolen; trains ran normally. The incident was reported to Spain's National Cryptologic Centre.	Playbook 6.2 and section 8: an attack moved between connected rail organizations; agree in advance who reports what.

Summarized by CyberGlass from public reporting: International Railway Journal, Aug 2023; Security Affairs and Reuters, Nov 2022; Ara and AP, May 2025; The Olive Press and Rus Tourism News, Sep 2026. Organizations are described, not named. Figures are as publicly reported at the time.

How this document connects

Document or register	How records and decisions flow
IT-06 Incident Response Plan	General process, severity and notification; RAIL-09 severity maps to IT-06 Severity 1–4; same INC-YYYY-NNN log
RAIL-03 section 4 and section 8	Safety-security interface and rail reporting timelines
RAIL-06 sections 3.10, 3.11 and 3.20	Detection, recovery and zone separation used during containment
RAIL-03 Appendix A Supplier Security Schedule	Supplier incident notice (24 h) and support duties
Rail Workbook Risk Register and hazard log	Root causes become risks R-NNN; safety-relevant events cross-referenced in the hazard log

Record flow example: Radio-stop tones stop 12 trains (playbook 6.3) → INC-2026-052, rail severity Critical = IT-06 Severity 1 → control centre applies operating rules → police and telecom regulator informed → risk R-011 'unauthenticated legacy radio' raised to High → migration plan in RAIL-02 roadmap.

PREVIEW

Preview pages · full editable Word/Excel files at cyberglass.ai/shop