



with carriers, ports, airports and border agencies, which places the security of the supply chain at the centre of the organisation's responsibilities.

The key processes of the SMS are the receipt, storage, handling, consolidation and dispatch of cargo; the control of access to sites, cargo and conveyances; the vetting of people, carriers and suppliers; the sealing and inspection of loads; and the detection of, and response to, security threats and violations. The high-level structure places top management at the apex, a Security Officer as the system owner, site and functional managers as process owners, and all workers as participants. Relevant licences and registrations, for example the customs warehouse authorisation and any supply-chain security programme membership, are recorded as [registration number].

Security is central to the organisation's value proposition because its customers entrust it with goods that are attractive to theft, sensitive to tampering and, in the case of bonded stock, subject to strict customs control. A single successful cargo theft can cost a customer a full container of high-value goods, expose the organisation to contractual penalties and insurance consequences, and damage the relationships on which the business depends. The organisation therefore treats the protection of cargo, conveyances, facilities and information as a core operational discipline, exercised at every handover in the flow of goods and reinforced by the culture, competence and vigilance of its people. The security management system described in this manual is the framework through which that discipline is organised, resourced, measured and improved, and through which the organisation demonstrates to its customers, its insurers, the authorities and the certification body that the security of the supply chain in its care is managed to a recognised international standard.

2.3 Using and maintaining this manual

The Security Officer maintains this manual. It is reviewed at least every three years and whenever a significant change to the organisation, its context or the standard occurs. Changes are made under the control of documented information procedure (QP-09): revisions are identified in the revision history, approved before issue, and distributed to controlled-copy holders, and superseded versions are withdrawn. The current version is the one held in the SMS document library; users confirm they are working from the current revision before relying on the manual.

2.4 Sites and the secure flow of goods

The security management system is best understood by following a consignment through the organisation. Goods arrive at a distribution centre by road, where the vehicle and driver are checked at the gatehouse against a pre-advised booking before entry is granted. At the inbound dock the load is



External issues determined for the example organisation include the threat environment for organised cargo theft, hijacking and pilferage on the road corridors and at the ports it uses; customs, transport-security and trade-compliance obligations in the countries of operation; the security expectations of customers, particularly those shipping high-value or controlled goods; the security posture of carriers, ports, airports and border agencies on which the organisation depends; insurer conditions; and technological developments such as telematics, electronic seals and access-control systems. Internal issues include the layout and perimeter of each site, the concentration of high-value and duty-suspended cargo at DC-1, workforce turnover and the resulting training load, the maturity of the security culture, the condition and coverage of security equipment, and the reliability of the information systems that hold consignment and access data.

The output of the review, the analysed and prioritised list of issues, is an input to the determination of interested-party requirements (4.2), to risk and opportunity planning (6.1) and to the setting of objectives (6.2), closing the loop between context and action.

In practice the context review is run as a facilitated workshop that the Security Officer prepares from the previous year's incident and audit data and holds with the site managers and the compliance lead. Each proposed issue is challenged for evidence and for its bearing on the intended results of the SMS, and only issues with a demonstrable effect are carried into the register. Where an issue is judged material, for example a rise in curtain-slashing theft on a particular corridor, it is linked directly to a risk in the register and, if needed, to an objective, so that the understanding of context visibly changes what the organisation does rather than remaining a background note.

Conformity with this clause is demonstrated to an auditor by the current Context and Issues Register, by the dated minutes of the review that produced it, and by the traceable links from material issues to entries in the risk register and, where relevant, to security objectives. The organisation can therefore show not only that it has considered its context but that the consideration changed the system, which is the test the standard sets.

A concrete illustration is the organisation's treatment of a seasonal surge: when peak-season volumes bring agency labour and overflow storage, the context review recognises the higher turnover and the temporary loss of segregation at DC-2 as internal issues, and the increased road movements at night as an external exposure. These issues are logged and drive temporary controls, additional vetting of agency staff and enhanced yard patrols, so that a predictable change in context is met with a planned change in control rather than a reactive one.



[Company Name]
Security Management System

POL-01
Rev [Revision]

Document Control

Document number	POL-01
Title	Security Management System Policy
Revision	[Revision]
Date of issue	[Date]
Standard / clauses	ISO 28000:2022 5.2.1, 5.2.2
Prepared by	ISO Consultant Panel
Reviewed by	[Name]
Approved by	[Name], [Designation Here]
Next review date	[Date]
Status	Controlled document

Revision History

Version	Date	Description of change	Author	Approval
1	[Date]	First issue of the controlled document.	ISO Consultant Panel	[Name]

Contents

1 Purpose and context	3
2 Scope	3
3 Policy statement and commitments	3
4 Framework for security objectives	4
5 Accountabilities and responsibilities	4



- ISO 28000:2022, clauses 8.3, 8.5.1, 8.5.2, 8.5.3
- ISO 31000 (risk management, referenced by 8.3)
- QP-04 Actions to Address Risks and Opportunities
- QP-10 Operational Planning and Control
- QP-11 Security Plans and Response Structure
- T-01 Security Risk Assessment and Treatment Register
- WI-05-01 Threat and Vulnerability Assessment
- WI-05-02 Security Risk Scoring and Risk Matrix

4 Responsibilities

The roles below carry the responsibilities and authorities stated. Where a role is consolidated in a smaller organisation, the segregation and impartiality note in the appendix applies.

Role	Responsibility and authority in this process
Security Officer	Owns the process; runs assessments; maintains the register and treatment plans.
Process / site owners	Provide operational detail; implement and maintain assigned treatments.
Top management	Approves treatment of significant risks, resource requirements and residual-risk acceptance.
[Designation Here]	Approves residual-risk acceptance above the routine threshold.

5 Definitions, scales and criteria

A security-related risk is the effect of uncertainty from a deliberate act (theft, tamper, diversion, intrusion, contraband, sabotage) on the organisation or the supply chain. A threat is a potential cause of a security incident; a vulnerability is a weakness a threat can exploit; a consequence is the outcome if the threat is realised. A security treatment is a measure that reduces the likelihood or the consequence of a risk, and a security strategy is a combination of procedures, processes and treatments selected to address a risk.

Likelihood and consequence are each rated one to five; the risk score is their product on a one-to-twenty-five scale. Risk bands are Low (1 to 6), Medium (8 to 12) and High (15 to 25). Treatment is mandatory when a score is twelve or higher, or when a legal, regulatory or customer security requirement applies, regardless of score. Residual risk of six or below is accepted; eight to twelve is



The process runs on change, after incidents and for each high-value consignment, producing the risk records, strategy selection and treatment plans.

Step 6.1 Establish the assessment scope

Who	Security Officer
Trigger and timing	On change, after an incident, or per high-value consignment
Location	Relevant site
Method	Define what is being assessed, a site, a recurring process or a specific consignment, and its boundaries and assets.
Acceptance criteria / decision rule	The scope, assets and boundaries of the assessment are defined before analysis begins.
Record	Security Risk Assessment and Treatment Record (QF-05-02)

Step 6.2 Analyse threats and vulnerabilities

Who	Security Officer with process owner
Trigger and timing	At assessment
Location	Relevant site
Method	Using WI-05-01, identify the credible threats and the vulnerabilities they could exploit, drawing on incident history, intelligence and site knowledge.
Acceptance criteria / decision rule	Credible threats and the vulnerabilities they exploit are identified and recorded.
Record	Threat and Vulnerability Assessment Worksheet (QF-05-01)

Step 6.3 Identify and analyse risks

Who	Security Officer
Trigger and timing	At assessment



- QP-08 Communication
- WI-11-01 Security Incident Response Activation
- QP-15 Nonconformity, Corrective Action and Continual Improvement

4 Responsibilities

The roles below carry the responsibilities and authorities stated. Where a role is consolidated in a smaller organisation, the segregation and impartiality note in the appendix applies.

Role	Responsibility and authority in this process
Top management	Provides authority and resources; takes part in decisions during significant events.
Security Officer	Owns the plans and the response structure; maintains rosters and thresholds.
Duty manager	Reachable at all hours; assesses threats against thresholds; activates the response.
Response team	Executes the plans; manages the event to priorities with life safety first.
Control room	Detects, alerts and logs; supports communication.

5 Definitions, scales and criteria

A security plan is a documented arrangement for responding to an imminent security threat or an ongoing violation. The response structure is the designated person (the duty manager) and the team or teams responsible for responding. An activation threshold is the predefined condition that justifies initiating a formal response. Recovery is the restoration of normal operations after an event.

Life safety is the first priority in every plan and decision, above the protection of assets, cargo and information. Any confirmed loss of custody of a tracked high-value load, any intrusion at a site, any credible threat to a person, and any tampered seal on receipt are activation thresholds that trigger a formal response. Security plans are exercised at least once per calendar year.

SECTION 6

The security plans and response process



6 Steps	4
7 Records	5
Annex A Clause coverage	5

WORK INSTRUCTION

Cargo Seal Integrity and 7-Point Conveyance Inspection

The exact steps for sealing a load and inspecting a conveyance so that tamper and concealment are detected before dispatch or on receipt.

1 Purpose

This work instruction ensures that seals are applied and verified correctly and that conveyances are inspected consistently, so that tampering, concealment and unauthorised access are detected. It supports procedure QP-10.

2 Scope

It applies to loaders, dispatchers and receiving staff handling full loads at [Company Name] distribution centres and the cross-dock hub.

3 Safety and environmental considerations

Wear the required PPE (high-visibility clothing, safety footwear, gloves). Follow yard traffic rules and do not enter a trailer that is not chocked and secured. Report any suspicious item without disturbing it.

4 Tools, equipment and materials

Item	Specification	Quantity
ISO 17712 high-security bolt seals	Compliant, uniquely numbered	Per load
Seal cutter	Rated for bolt seals	1 per dock



6 Steps	4
7 Records	5
Annex A Clause coverage	5

WORK INSTRUCTION

Security Incident Response Activation

The exact escalation path from a detected threat to an activated response, with life safety first.

1 Purpose

This work instruction ensures that a detected security threat or violation is assessed against the activation thresholds, escalated on the defined ladder, and the appropriate response activated without delay, with life safety as the first priority. It supports procedure QP-11.

2 Scope

It applies to control-room operators, gatehouse staff and the duty manager at any site of [Company Name] and to in-transit events affecting the organisation's loads.

3 Safety and environmental considerations

Life safety is the first priority. Do not confront an intruder or hijacker. Follow the safe-response rules; keep a safe distance; do not disturb evidence unless life safety requires it.

4 Tools, equipment and materials

Item	Specification	Quantity
Response Team Roster and Contacts (QF-11-02)	Current	1
Contact trees and message templates	Current	1
Incident and Event Log (QF-11-04)	Current controlled form	1
Security Incident Report (QF-11-03)	Current controlled form	1



FORM

Threat and Vulnerability Assessment Worksheet

Associated procedure: QP-05 / WI-05-01 Organisation: [Company Name]

QF-05-01

Rev [Revision]

Issue [Date]

Record the credible threats to the assets in scope, the vulnerabilities they exploit, the existing controls and the potential consequence. Feeds the risk scoring (QF-05-02).

1 ASSESSMENT

ASSESSMENT REF

SCOPE

ANALYST

2 THREATS AND VULNERABILITIES

Threat	Vulnerability exploited	Existing controls	Potential consequence

This documentation toolkit was developed by the consultant panel of isofolder.



FORM

Conveyance 7-Point Inspection and Seal Log

Associated procedure: QP-10 / WI-10-01 Organisation: [Company Name]

QF-10-03

Rev [Revision]

Issue [Date]

Record the seven-point conveyance inspection and the seal number at dispatch and receipt.

1 MOVEMENT

CONSIGNMENT

VEHICLE / TRAILER

DATE

2 7-POINT INSPECTION (EMPTY CONVEYANCE)

POINTS INSPECTED AND SOUND ☐ Front wall ☐ Left side ☐ Right side ☐ Floor ☐ Ceiling
☐ Doors ☐ Outside/undercarriage

3 SEAL

SEAL TYPE

SEAL NO. AT DISPATCH

MANIFEST SEAL NO.

4 RECEIPT VERIFICATION

SEAL INTACT ON RECEIPT

SEAL NO. ON RECEIPT

MATCH?

NOTE

A broken, missing or mismatched seal is a security event: do not open further; escalate to the duty manager (QP-11).