

Cyber Security and Data Governance Policy for SteelForm Manufacturing Ltd

Module Name: Networks and Cyber
Security Essentials
Module Code: ACCA4024
Student Name: Hora Big
Student ID: 2509557
Group: 4
Lecturer's Name:

Table of Contents

Table of Contents	1
Abstract	4
1. Introduction	5
2. Threat and Risk Assessment	6
2.1 SFM Threat Environment	6
2.2 External Threats	6
2.3 Internal Threats	7
2.4 CIA Analysis	7
2.5 Risk Assessment: Likelihood and Impact	8
3. Security Policy Framework	11
3.1 NIST CSF 2.0	11
3.2 ISO/IEC 27001	12
3.3 ISA/IEC 62443	13
3.4 UK GDPR and the Data Protection Act 2018	13
3.5 Core Security Policy Suite	13
4. Mitigation Measures and Implementation	14
4.1 Network Segmentation (Priority Control)	14
4.2 Identity, Access, and Detection Controls	14
4.3 Resilience and Data Protection Measures	14
4.4 Phased Implementation Roadmap	16
5. Monitoring and Incident Response	16
5.1 Continuous Monitoring	16
5.2 Incident Response	17
6. Training and Awareness	19
7. Conclusion	21

References	22
Appendix A: Board Presentation	23

Background:

Cybersecurity has become a critical issue for organizations across all sectors, including manufacturing. The rise of Industry 4.0, automation, and the Internet of Things (IoT) has increased the interconnectivity of systems, creating new vulnerabilities. Modern manufacturing environments rely on smart machines, remote monitoring systems, and connected supply chains, all of which expose sensitive operational data to potential cyberattacks. Recent incidents of ransomware targeting industrial control systems and data theft from supply chain partners have shown how cyber threats can disrupt production, cause financial loss, and damage a company's reputation.

Scenario:

You are the IT Security Manager for SteelForm Manufacturing Ltd (SFM), a medium-sized manufacturing company that produces custom-engineered components for the automotive and aerospace industries. SFM has recently adopted smart manufacturing technologies, including IoT-enabled sensors, automated machinery, and a cloud-based production management system. Over the past few months, the company has faced several security incidents, including malware infections, phishing emails targeting procurement staff, and unauthorized access attempts to its production network. The company's board is increasingly concerned about industrial espionage, data breaches, and potential downtime caused by cyberattacks. You have been tasked with developing a comprehensive cybersecurity and data governance policy to strengthen protection against internal and external threats

Abstract

SteelForm Manufacturing Ltd (SFM) has introduced IoT sensors, automated machinery and a cloud-based production management system. At the same time, the company has experienced malware, phishing aimed at procurement staff and attempts to access the production network. This report examines the main internal and external threats created by this environment and considers their effect on confidentiality, integrity and availability. It then recommends a practical security approach using NIST CSF 2.0, ISO/IEC 27001, IEC 62443 and UK data-protection requirements. The main recommendations are IT/OT network segmentation, stronger access controls, monitoring, reliable backups, supplier checks and role-based staff training. The controls are planned in stages so that SFM can improve security without unnecessarily interrupting production. The assessment is based on the scenario provided rather than a technical audit of SFM's live systems.

1. Introduction

Industry 4.0 has made manufacturing more connected. IoT sensors, automated machinery and cloud systems can improve production and make information easier to share, but they also create more points that an attacker could target. The risk becomes more serious when business IT connects to operational technology (OT), because a cyber incident can affect both information and the physical production process.

SFM is a medium sized manufacturer of custom engineered components for the automotive and aerospace sectors. The company has recently introduced connected sensors, automated machinery and a cloud based production management system. It has also experienced malware infections, phishing aimed at procurement staff and unauthorized access attempts against the production network. These incidents suggest that the company is exposed through several areas, including user accounts, email, connected devices, production systems and suppliers.

For SFM, cybersecurity is therefore a business issue, not just an IT issue. Ransomware could stop production, while theft of engineering drawings or customer information could damage the company's commercial position. A compromised supplier or remote connection could also provide an attacker with a route towards production systems. The Board needs controls that reduce these risks but are still realistic for a medium-sized manufacturer.

The report identifies and prioritizes SFM's threats, then considers the security policies, controls, monitoring, incident response and training needed to reduce them. The main recommendation is a layered approach:

MFA can reduce account compromise but does not stop every phishing attack, while backups support recovery but do not prevent data theft. Controls therefore need to work together and be introduced in stages. Where the scenario lacks technical detail, the report identifies the point as an assumption.

2. Threat and Risk Assessment

2.1 SFM Threat Environment

SFM's environment can be considered as five connected areas: corporate IT and email, production OT, IoT devices, the cloud production management system, and supplier or remote-access connections. The scenario does not give the exact network design, so the proposed architecture should be treated as a planning model rather than a description of the live network.

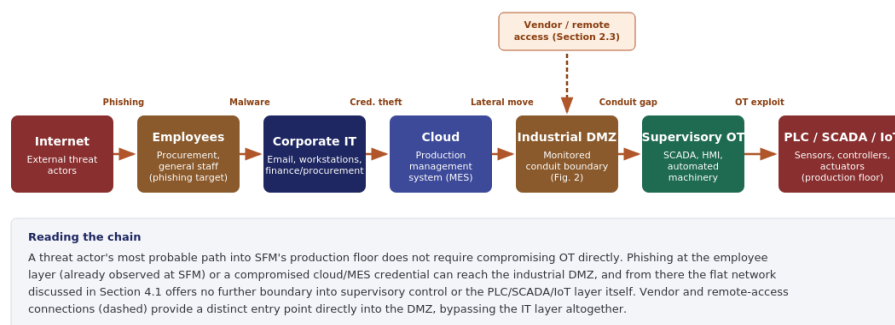


Figure 1. SFM cybersecurity risk landscape: attack-surface chain from external threat actor to production floor.

2.2 External Threats

Ransomware is a major concern because an attack could make production systems unavailable and could also involve theft of company data. Procurement phishing and business email compromise (BEC) deserve particular attention because procurement staff have already been targeted. Suppliers, maintenance companies and other third parties create additional attack paths, especially where remote access is available. Industrial espionage could expose engineering designs and other intellectual property. Vulnerable IoT and OT devices are also important because attacks against them may affect the integrity or availability of production. Credential attacks can support several of these threats by giving attackers access to legitimate accounts.

2.3 Internal Threats

Internal risks include mistakes by employees, weak or reused passwords, unauthorized software or devices, removable media, excessive privileges and deliberate misuse by an insider. These threats can be difficult to manage because the person involved may already have legitimate access. Vendor access is also important. Maintenance access may be necessary for production, but a permanent or over privileged account creates an avoidable route into the environment if it is not controlled and monitored.

2.4 CIA Analysis

The CIA triad provides a simple way to show what could be affected by each threat. Ransomware mainly affects availability because production may be stopped, although data may also be stolen. Phishing and stolen credentials can affect confidentiality and integrity. OT exploitation can affect the integrity and availability of production systems, while industrial espionage is mainly a confidentiality risk. This approach helps connect the risks to the controls recommended later in the report.

Threat	Origin	C	I	A	Notes
Ransomware (OT-affecting)	External	Y	Y	Y	May affect production and expose data
Phishing / BEC (procurement)	External	Y	Y	N	Already observed at SFM
Supply chain compromise	External	Y	N	Y	Impact depends on compromised party's access level
Industrial espionage / IP theft	External	Y	N	N	Mainly threatens engineering IP confidentiality

Threat	Origin	C	I	A	Notes
IoT/OT vulnerability exploitation	External	N	Y	Y	OT patching constrained by production stoppage risk
Credential-based attacks	External	Y	Y	N	Mitigated by MFA (Section 4.2)
Negligent employee error	Internal	Y	N	N	Circumvents controls rather than defeating them
Malicious insider	Internal	Y	Y	N	May be difficult to detect because access is legitimate
Weak passwords / shadow IT	Internal	Y	N	N	Precondition for several external threats above
Excessive privileges	Internal	Y	Y	N	Widens blast radius of other threats
Unmanaged vendor/third-party access	Internal/External boundary	Y	Y	Y	Now a primary breach pathway per sector evidence

2.5 Risk Assessment: Likelihood and Impact

The threats are ranked using a qualitative 5×5 likelihood and impact matrix. The scores are based on the information in the scenario and on the likely effect on production, information and customers. They are not measurements of SFM's actual incident frequency because no internal security data is provided.

Threat	Likelihood (1-5)	Impact (1-5)	Score	Band
Ransomware (OT-affecting)	4	5	20	Critical
Phishing / BEC (procurement)	5	4	20	Critical
Unmanaged vendor/third-party access	3	5	15	High
Supply chain compromise	3	4	12	High
Industrial espionage / IP theft	3	4	12	High
IoT/OT vulnerability exploitation	3	4	12	High
Credential-based attacks	3	3	9	Medium
Malicious insider	2	4	8	Medium
Negligent employee error	4	2	8	Medium
Weak passwords / shadow IT	3	2	6	Low-Medium
Excessive privileges	2	3	6	Low-Medium

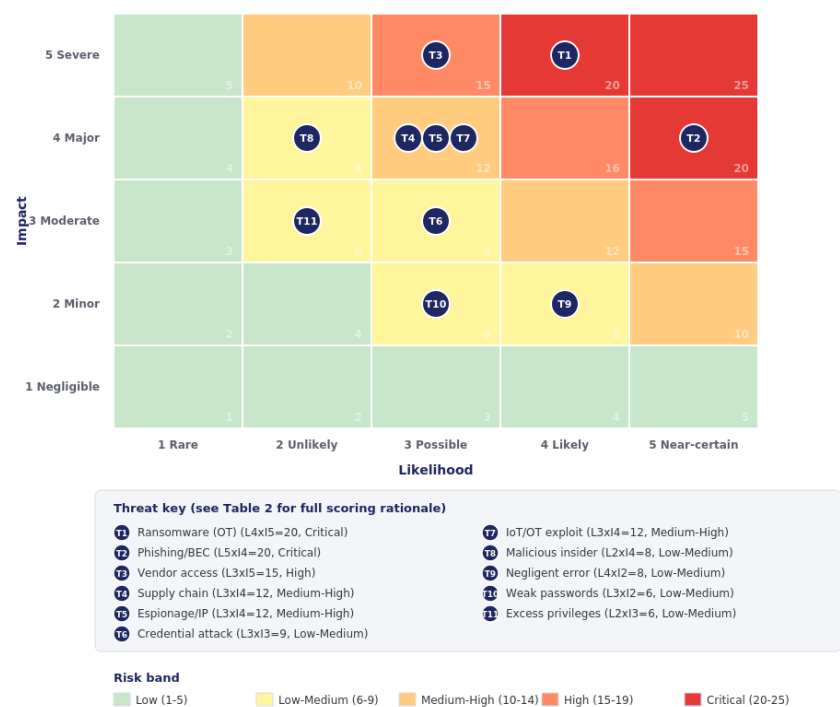


Figure 3. SFM cyber risk heat map, plotting Table 2 scores by likelihood and impact.

3. Security Policy Framework

No single standard covers all of SFM's needs. NIST CSF 2.0 is useful for overall risk management, ISO/IEC 27001 supports information security governance, IEC 62443 is focused on industrial control systems, and UK data protection law sets legal requirements for personal data. Using them together makes sense, but SFM should avoid creating duplicate processes that add work without reducing risk.

Policy	Purpose	Requirements	Owner	Review	Enforcement
Acceptable Use	Govern appropriate IT/OT and device use	Prohibited activities defined; onboarding acknowledgement	IT Security	Annual	HR disciplinary process; access revocation
Access Control	Match access to role, re-verify periodically	RBAC + least privilege; MFA on remote/privileged; recertification	IT Security & HR	Bi-annual	Automated access reviews; suspension on failure
Network Segmentation	Separate IT/OT to limit lateral movement	Defined zones/conduits; firewall rules; no direct IT-OT traffic	IT Security & Ops	Annual / on change	Firewall audits; review sign-off before deployment
Data Classification & Governance	Classify data by sensitivity	4-tier classification; encryption/retention per tier	Data Protection Officer	Annual	DLP flags violations; classification audits

Policy	Purpose	Requirements	Owner	Review	Enforcement
Third-Party & Vendor Security	Manage supplier/contractor/MSP risk	Due diligence at onboarding; contractual clauses; time-limited access	Procurement & IT Security	Annual / renewal	Onboarding gate; quarterly PAM log review
Patch & Vulnerability Management	Timely remediation of vulnerabilities	Differentiated IT/OT timelines; coordinated OT maintenance windows	IT Security & Ops	Quarterly	Scan reports tracked to closure; overdue escalation
Incident Response	Define detection, containment, recovery	IR Team defined; escalation thresholds; mandatory post-review	IT Security	Annual / post-incident	Mandatory tabletop attendance; tested twice yearly
Remote Access & BYOD	Secure remote/third-party connections	VPN + MFA mandatory; BYOD baseline before connecting	IT Security	Annual	NAC blocks non-compliant devices

3.1 NIST CSF 2.0

NIST CSF 2.0 gives SFM a clear structure for managing cybersecurity through Govern, Identify, Protect, Detect, Respond and Recover. Its main benefit is that it gives management and technical teams a common way to discuss risk. However, it does not provide the detailed design rules needed for an industrial control network. SFM should therefore use NIST as the overall framework rather than as its OT engineering standard [3].

3.2 ISO/IEC 27001

ISO/IEC 27001:2022 provides the basis for an information-security management system and continual improvement [4]. For SFM, it can help assign responsibility, record risk decisions

and show customers that security is being managed systematically. Its limitation is that an ISMS does not tell SFM how to segment PLCs or safely connect OT systems. Certification or alignment should therefore not be treated as proof that technical risks have been removed.

3.3 ISA/IEC 62443

IEC 62443 is the most directly relevant of these standards to SFM's production environment. IEC 62443-3-2 uses zones and conduits as part of a risk based approach to industrial control systems [5]. This supports the proposed IT/OT segmentation. The main challenge is implementation: SFM will need input from OT engineers and carefully planned maintenance windows so that security changes do not disrupt production.

3.4 UK GDPR and the Data Protection Act 2018

The UK GDPR and Data Protection Act 2018 set the legal requirements for protecting personal data. Where a personal data breach is reportable, the ICO states that the organization should notify the regulator without undue delay and, where feasible, within 72 hours of becoming aware of the breach [6]. This is a legal requirement rather than a cybersecurity framework, so it needs to sit alongside the technical and governance controls.

3.5 Core Security Policy Suite

These policies turn the main security requirements into responsibilities that staff and managers can be held accountable for. Access control and segmentation reduce the chance of unauthorized movement, vendor controls reduce third party risk, and patching needs to take account of OT maintenance windows. The main practical issue is the time needed to manage reviews, suppliers and maintenance changes, so responsibility should be shared between IT, Operations, Procurement and HR.

4. Mitigation Measures and Implementation

4.1 Network Segmentation (Priority Control)

Network segmentation should be one of SFM's first major architectural changes because it can limit movement from the office network towards production. Complete OT isolation would reduce some risks, but it would not fit SFM's connected manufacturing model. A better option is separate zones with controlled and monitored connections between corporate IT, an industrial DMZ and OT. This follows IEC 62443 [1], [5]. The design can be prepared in Phase 2 and deployed in Phase 3 with Operations involved. Segmentation still needs MFA and privileged access controls because it does not prevent stolen credentials from being used.

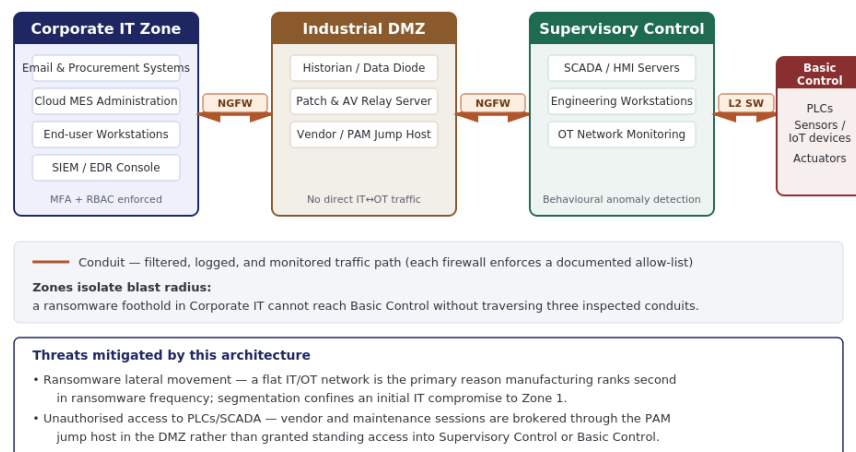


Figure 2. Target IT/OT network segmentation using the IEC 62443 zone-and-conduit model.

4.2 Identity, Access, and Detection Controls

MFA and privileged-access management should be applied first to remote and privileged accounts. MFA makes stolen passwords less useful, while PAM can reduce permanent administrator access and limit vendor sessions. Procurement staff also need a clear process for checking payment or bank-detail changes rather than relying on email alone. EDR and a maintained OT asset inventory will improve detection and visibility. These controls can start in Phase 1 and expand during Phase 2.

4.3 Resilience and Data Protection Measures

SFM should maintain offline or immutable backups of critical business data and important OT configurations and test restoration at least twice a year. Backups improve recovery from

ransomware, but they do not stop data theft, so DLP should also protect sensitive CAD files, specifications and production information. Critical suppliers should undergo security checks and accept suitable security requirements in their contracts. Measures should include restore test success, DLP coverage and the percentage of critical suppliers assessed.

Threat	Control	Implementation	Owner	KPI
Ransomware / lateral movement	IT/OT network segmentation	Zone-and-conduit architecture, NGFWs at boundaries	IT Security & Ops	% zones with validated conduit rules
Credential / vendor access	MFA + Privileged Access Mgmt	MFA on remote/privileged accounts; PAM brokers vendor sessions	IT Security	MFA coverage % (target 100%)
Procurement phishing / BEC	Email authentication + callback	DMARC/DKIM/SPF; mandatory callback for payment changes	IT Security & Procurement	Phishing click rate (downward)
Malware / unauthorized access	EDR + OT-aware asset inventory	Endpoint detection; full PLC/sensor inventory	IT Security	% assets in maintained inventory
Ransomware downtime	Immutable, tested backups	Air-gapped IT+OT backups; biannual restore test	IT Security & Ops	Backup restoration success rate
Espionage / IP (possession) loss	Data loss prevention (DLP)	DLP on CAD files, specs, production data	IT Security	% restricted data covered by DLP
Supply chain compromise	Formal vendor risk assessment	Security questionnaire; certification evidence for critical suppliers	Procurement	% suppliers with completed assessment

4.4 Phased Implementation Roadmap

The controls should not all be introduced at once. Measures that can reduce the risks already seen at SFM should come first, while changes to OT networks should be designed and tested before they are introduced into production.

In the first 30 days, SFM should introduce email authentication, payment change verification and MFA for privileged accounts. During months 1 to 3, it should complete MFA and PAM, design the segmentation model, establish reliable backups and build the OT asset inventory. During months 3 to 6, the company can deploy segmentation, expand EDR and DLP, and run a ransomware exercise. During months 6 to 12, the focus should move to supplier assurance, a second exercise and regular Board review of the security KPIs.

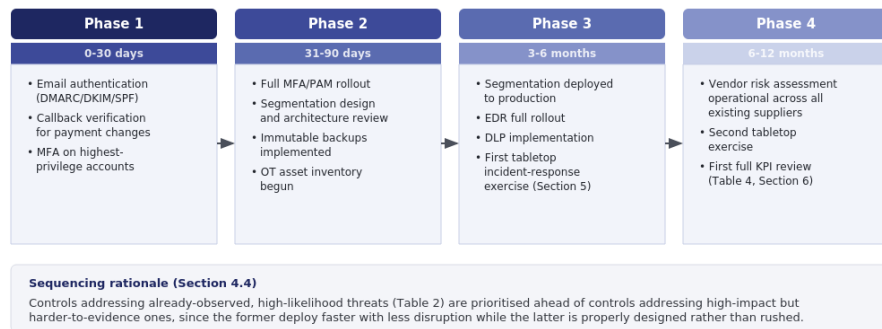


Figure 6. Cybersecurity implementation roadmap: four-phase sequencing per Table 2 risk priority.

5. Monitoring and Incident Response

5.1 Continuous Monitoring

SFM needs visibility across both IT and OT. A SIEM or managed detection and response service should collect useful information from firewalls, EDR, the cloud production system and relevant OT monitoring tools. NCSC guidance also stresses the importance of understanding and monitoring OT connectivity [1].

This matters because normal IT monitoring may not show unusual activity inside an industrial network.

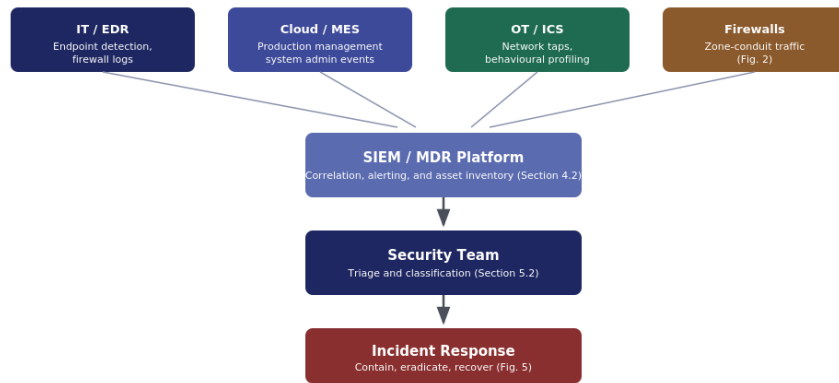


Figure 4. Security monitoring architecture: log sources feeding SIEM/MDR through to incident response.

5.2 Incident Response

SFM should use a simple incident process: Detect, Triage and Classify, Contain, Eradicate, Recover, and then review what happened. This is consistent with current NIST incident-response guidance [7].

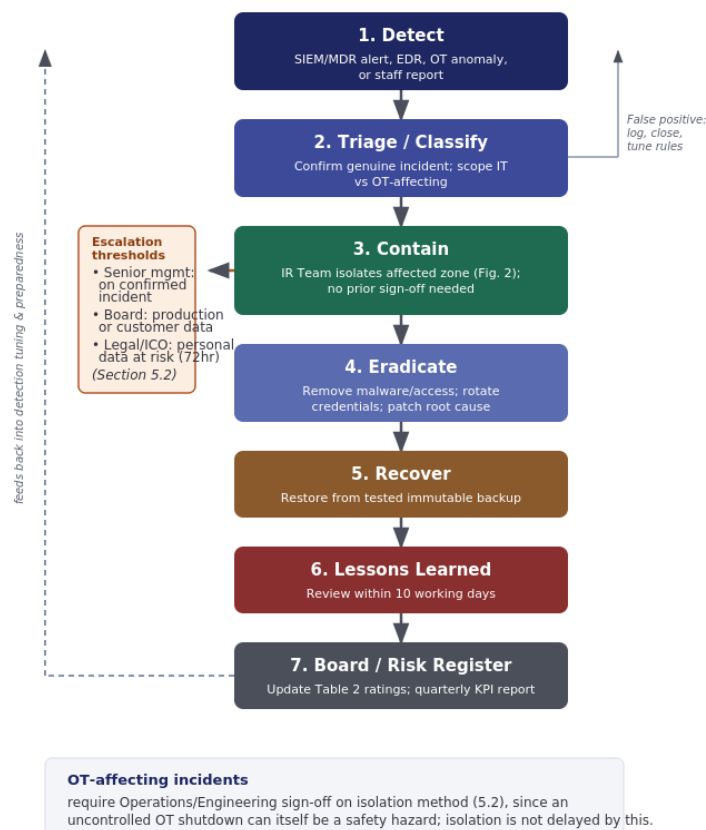


Figure 5. Incident response flowchart: seven-step sequence with escalation thresholds.

The escalation rules should be agreed in advance. Senior management should be informed when an incident is confirmed. The Board should be involved when production, important customer information or engineering IP is seriously affected. Legal and the Data Protection Officer should be involved where personal data or contractual reporting duties may apply. Where a personal data breach is reportable, the ICO's applicable notification period must be followed [6].

The incident team should include IT Security, Operations or Engineering for OT incidents, Legal, and a Board sponsor. The team should have agreed authority to isolate affected systems, but OT containment must be planned carefully because shutting down or disconnecting equipment can itself affect production or safety.

An IT workstation can often be isolated quickly. An OT system needs more care because an incorrect shutdown could interrupt production. The proposed segmentation should make it possible to isolate a smaller affected zone rather than taking the whole production environment offline. Twice yearly tabletop exercises should test this process and the results should be added to the risk register.

6. Training and Awareness

Because procurement staff have already been targeted, SFM should use role based security training rather than relying only on one annual awareness session.

Role	Training	Frequency	Method	KPI
All employees	Phishing recognition, MFA hygiene, blame-free reporting	Onboarding + annual	Instructor-led + micro-learning + simulated phishing	Completion; click rate; reporting rate
Procurement / Finance	BEC patterns; callback-verification procedure	Onboarding + annual + post-incident	Targeted session + simulated BEC scenarios	Callback-verification compliance rate
Production / OT Engineers	OT safety implications; vendor remote-access hygiene	Onboarding + annual	Practical OT exercises + instructor-led	Exercise participation; media-policy adherence
IT / Security Staff	SIEM/MDR alerting, EDR triage, PAM administration	Onboarding + per tool update	Technical instructor-led + hands-on	Mean time to triage/containment
Senior Management / Board	Governance obligations; escalation role	Onboarding + annual briefing	Condensed governance briefing (Appendix A)	Quarterly dashboard review attendance

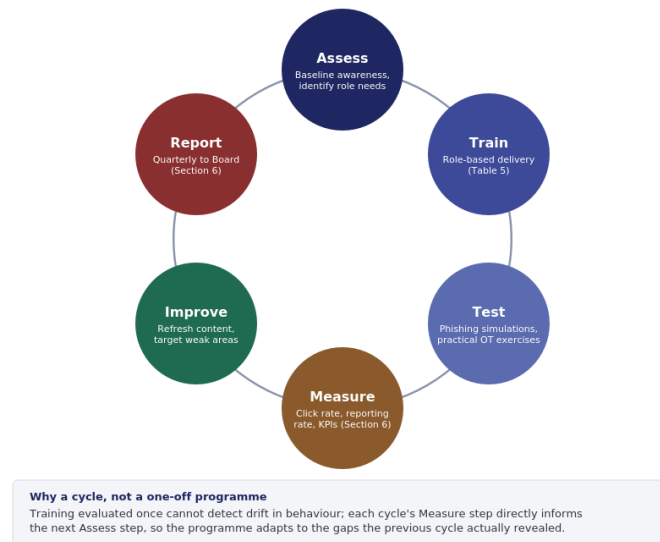


Figure 7. Training and awareness cycle underpinning the role based programme.

All employees should receive training when they join SFM and an annual refresher covering phishing, MFA and incident reporting. Procurement and Finance should have extra exercises on BEC and checking payment changes. OT engineers need practical training on safe remote access and responding to OT incidents. IT and Security staff need more technical training on SIEM, EDR and PAM. The Board needs shorter briefings focused on governance, risk and escalation.

Training should combine short online modules with instructor led sessions, phishing simulations and practical exercises. Staff also need an easy, blame free way to report suspicious emails or activity. Early reporting can give the security team more time to contain an incident.

The programme should be measured using completion rates, phishing click rates, phishing reporting rates, MFA coverage and incident detection and containment performance. Completion alone only shows that training was attended. Behavioural measures give SFM better evidence that the training is changing how people respond to threats. Results should be reported to the Board each quarter.

7. Conclusion

SFM's most important risks are ransomware and procurement phishing/BEC, followed by vendor access, supply chain compromise, IP theft and OT exploitation. The recommended response focuses on segmentation, MFA and PAM, stronger email controls, monitoring, reliable backups, protection of sensitive data and better supplier security.

The proposed standards work together because they cover different parts of the problem:

NIST supports overall risk management,

ISO/IEC 27001 supports security governance,

IEC 62443 addresses OT,

and UK data protection law covers personal information.

The controls are phased so that SFM can reduce immediate risks while introducing OT changes carefully. Some residual risk will remain because no single control can prevent every type of attack.

The Board should review the main security measures and KPIs regularly as SFM's technology and threat environment change. Before major investment decisions, the risk scores should be checked against the company's actual asset inventory, network design and incident data. This assessment is a practical starting point, not a substitute for a live security assessment.

References

- [1] National Cyber Security Centre, CISA, ASD, BSI, and partner agencies, “Secure connectivity principles for operational technology,” Jan. 2026.
- [2] National Institute of Standards and Technology, “Guide for Conducting Risk Assessments,” NIST SP 800-30 Rev. 1, Sep. 2012.
- [3] National Institute of Standards and Technology, “The NIST Cybersecurity Framework (CSF) 2.0,” NIST CSWP 29, Feb. 2024.
- [4] International Organization for Standardization and International Electrotechnical Commission, “ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements,” 2022.
- [5] International Electrotechnical Commission, “IEC 62443-3-2:2020 — Security for industrial automation and control systems — Security risk assessment for system design,” 2020.
- [6] Information Commissioner’s Office, “Personal data breaches: a guide,” updated 2025.
- [7] National Institute of Standards and Technology, “Incident Response Recommendations and Considerations for Cybersecurity Risk Management,” NIST SP 800-61 Rev. 3, Apr. 2025.

Appendix : Presentation



WHY THIS MATTERS NOW

WHY THIS MATTERS NOW

SFM has already seen malware, procurement phishing and unauthorised access attempts. The risk is therefore already present, not just a future possibility.



3

recent security
incident types
reported in the SFM
scenario



IT + OT
connected
production
environment
can increase the
impact of an attack



Board risk

possible production
downtime, data loss
and industrial
espionage

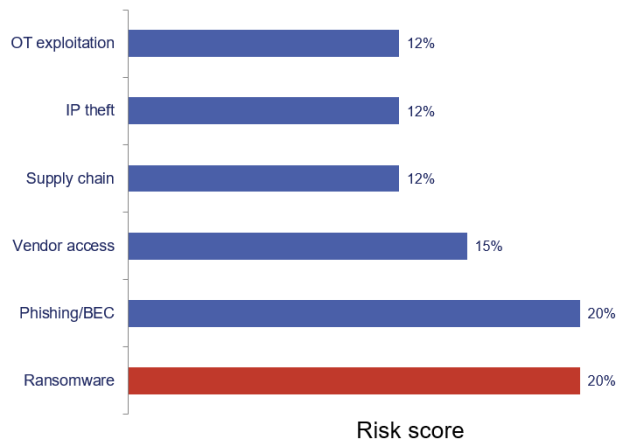


1 goal

protect production
continuity,
engineering IP, and
customer trust

THREAT LANDSCAPE

Ransomware is one of SFM's main risks



What's driving it

- OT systems may be difficult to patch without affecting production
- Suppliers and remote access create extra routes into the business
- Ransomware, phishing, stolen credentials and OT weaknesses can be linked in one attack

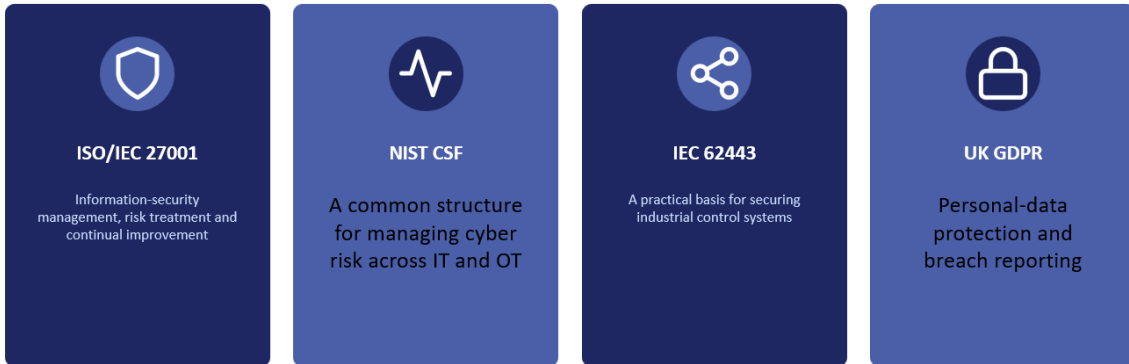
The main internal and external threats facing SFM

INTERNAL	EXTERNAL
Malicious insider or misuse of legitimate access	Ransomware
Human error, misconfiguration or unsafe USB use	Phishing targeting procurement staff
Weak or reused passwords	Supply-chain / third-party compromise
Unmanaged or unauthorised IoT devices	Industrial espionage and OT vulnerabilities

GOVERNANCE

A policy framework built on recognised standards

The standards give SFM a common approach to governance, information security, OT security and data protection.



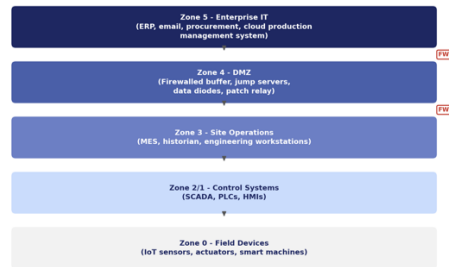
Core policies: Acceptable Use · Access Control · Network Segmentation · Data Classification · Incident Response · Third-Party Security · Patch Management · Backup & Continuity

MITIGATION — ARCHITECTURE

Keeping a problem in IT from becoming a factory-floor problem

If an office account is compromised, the attacker should not be able to move straight to a PLC. Separate IT, DMZ and OT zones with controlled firewall rules reduce that risk.

- Firewalls and access controls between zones
- Only required traffic is allowed and monitored
- IoT devices and smart machines are placed in controlled zones
- Changes are tested and agreed with Operations before deployment



IEC 62443 zone-and-conduit model; full detail in written report

MITIGATION MEASURES

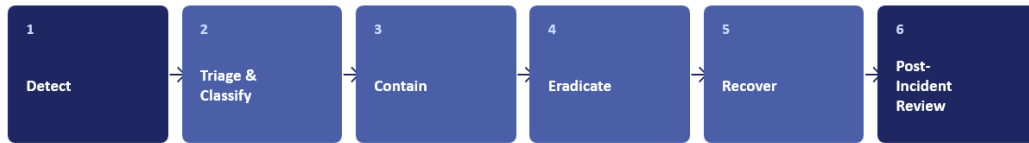
Five controls to prioritise in the first six months

1		Network segmentation	IT/DMZ/OT zoning with firewalls
2		Multi-factor authentication	Remote and privileged accounts
3		Email & phishing defence	Filtering plus DMARC/DKIM/SPF
4		Encrypted, tested backups	Offline or immutable backups with regular restore tests
5		Supply-chain risk controls	Security requirements in supplier contracts

MONITORING & RESPONSE

Detect early and contain safely

An IT device can often be isolated quickly. OT incidents need Operations and Engineering involved because the wrong action could interrupt production or create a safety issue.



Serious incidents go to Senior Management and the Board. Legal/DPO are involved where required, including applicable data-breach reporting.

Making security part of everyday work

	All staff	Induction and annual refresher
	Procurement & finance	Targeted workshops and regular phishing tests
	OT / production engineers	Hands-on OT session twice a year
	IT / security team	Ongoing technical training and twice-yearly exercises
	Senior management / Board	Annual Board briefing linked to the risk register

Approve and fund the first stage now

Endorse

the core policies and standards approach

Fund

segmentation, MFA, monitoring and backup improvements

Mandate

role-based training and quarterly Board reporting

Review

the programme each quarter using the cyber risk and KPI dashboard

No single control will stop every attack. The aim is to make sure one failure does not become a major production or data-loss event.