Machine Security Compliance Framework

This framework details key security considerations for Machine Builders to develop and commission secure machines that remain secure throughout their lifecycle. We believe this is only possible with a comprehensive strategy that ensures security is ingrained throughout the entire organisation. This framework details six steps and should be read from left-to-right. Each step builds on the knowledge gained from the previous steps.

1 Management commitment

Security starts with commitment from the highest level of the organisation and must be part of the foundation throughout the entire organisation.

Set security goals
Define ambitious security goals to determine your aim, e.g:
- No security incidents for any comissioned machine
- No incidents for internal confidential information related to data alteration or loss
- Deliver only IEC 62443-certified machines

Allocate resources
Management needs to allocate appropriate resources (time, money, people) to achieve these security goals.

Promote *security by design*
Management needs to ensure security is ingrained throughout the organisation.

Review
At least once a year perform a **management review** looking at the security status of the entire organisation with all security-related personnel and management. Discuss the following:
- Measurable data regarding security goals
- Significant security risks and plans to address them
- Number and type of security incidents
- Planning of security related events
- Resources and capacity
- Audit results (internal/external)

2 Risk management

To measure is to knowing. Developing a mindset for assessing risks vs. benefits ensures objectivity and helps you set your priorities straight.

Mapping

Inventory of risks
Make a comprehensive list of all security risks. Choose a method to systematically assess everything, e.g. by looking at each process or asset individually.

Scoring

Risk scoring
Score each risk based on the likelihood and impact of it happening.

Benefit scoring
Score each risk for the benefit of having the item.

Cost-benefit analysis
Weigh risks against benefits to determine which items contain *unacceptable risks*.

Treating

Risk treatment
Prepare detailed plans on how to mitigate these risks, based on the following strategies.

- **Reduce**
  Lower the likelihood of it happening or the impact when it happens.
- **Avoid**
  Not performing the activity that creates the risk.
- **Insure**
  Remove the impact of the risk by insuring your organisation for the damages if it occurs.

3 Internal organisation

The importance of a secure internal organisation cannot be overstated. It is the foundation upon which to grow and build. There are three key goals:
- Ensuring your **people** are knowledgeable
- Incorporating security throughout all **processes**
- Using industry-standard **technology**

People

Background checks
Investigate applicants for red flags.

Competencies
Ensure applicants are capable of upholding security standards related to their role.

Responsibilities
Define roles and assign responsibilities to maintain security.

Start of employment

Employee lifecycle

End of employment

Revocation
Remove access to services and information.

Training
Provide appropriate education opportunities.

Awareness
Ensure security is top-of-mind for all employees.

Assessment
Regularly review employees' performance and growth.

Processes

Document

Access control
Restrict who can access systems and information.

Information levels
Define information confidentiality levels and their appropriate security guidelines.

Supplier security
Design, evaluate and review security requirements for your suppliers.

Security policies
Create strong security policies to uphold availability, integrity and confidentiality of systems and information.

Incident management
Describe how to treat and learn from security incidents.

Internal audits
Regularly review your organisation's adherence to security policies and procedures.

Technology

Engineering lifecycle

1. **Requirements**
   Explicitly define security requirements early in the project.
2. **Development**
   Develop using secure (coding) standards.
3. **Testing**
   Perform thorough testing from the perspective of a hacker.
4. **Peer review**
   Ensure at least one independent person reviews the changes.
5. **Documentation**
   Provide thorough documentation for future reference.
6. **Commisioning**
   Commission the changes.

Backups
Create regular backups of critical data.

Internal network
Design a secure internal network.

4 Machine & Cloud

After creating a strong security foundation for your organisation, you are ready to provide customers with secure machines and connectivity solutions. You are also in a position to assess the security maturity of your cloud providers and other suppliers. You are only as strong as your weakest link.

Machine architecture

Topology
Describe the machine topology.

Firmware upgrades
If feasible, update the firmware of all machine components.

Inventory of components
List and describe all used components in the machine.

Component lifecycle
Consider when to replace or update specific components.

Documentation
Document all relevant machine information, e.g:
- Electrical diagrams
- Machine manuals
- Service reports

Firewall
Separate your machine network from the factory network using a strict firewall.

Machine data
Only store relevant machine data and transfer it in a secure manner.

Remote access
Incorporate a secure tool to provide remote access to your machine.

OT / IT network

Network architecture
Integrate your machine into the factory network using segmentation (VLANs, DMZs).

Cloud

Encryption
Ensure all communication is encrypted using strong algorithms.

User management
Allow admins to restrict users with access permissions.

Terms of Service / Privacy
Protect your and your users' rights with terms of service and privacy statements.

Authentication
Enforce strong authentication methods (e.g. password requirements, 2FA).

Cloud architecture
A cloud platform can be simplified as a number of servers and a number of databases that are accessible from the Internet. Ensure these servers are configured with security in mind, e.g:
- Restrict access to servers
- Configure strict firewalls
- Use modern supported software

Patch management
Update all server and database applications when feasible.

Vulnerability assessment
Perform regular vulnerability assessments or pentests.

Monitoring
Employ automated monitoring to assess your cloud environment's health.

Automated backups
Create regular backups of critical data.

5 External communication

Detailing every security rule, policy and process is essential for a multitude of reasons. Good documentation makes it clear to your partners who holds what responsibilities, it builds trust and guarantees you can provide everything described. Well-written documents also improve clarity between you, your customers and suppliers and it will preempt questions they might have.

Writing tips

Just write
Writing everything down helps you organise information, and helps bring details to the surface you may not have considered before.

Templating
Write everything down using a template to ensure you do not forget crucial steps and make it easily shareable.

Start early
Start documenting early on in the process.

Use it as a discussion
Writing down your requirements and wishes helps you guide conversations with your customer.

Example documents

Not every detail has to be documented, but here are some examples that can help you decide what to document.

Security whitepaper
Describes, at a high-level, all security related aspects of your organisation, machine and/or cloud solution.

Terms of service
Describes all legal rights and obligations you and your customers have in relation to the services provided.

Privacy statement
Describes how you handle personal information, as well as who people can contact for further questions.

Machine connectivity
Describes the network connectivity requirements the machine has.

Supplier security
Describes the suppliers you use, as well as relevant security requirements they have.

Non-disclosure agreement
Describes what information can and can't be shared.

6 Certification

Once you have implemented, formalized and documented security solutions for the previous steps, you can consider certifying your organisation against a security standard. Complying with one of these standards ensures your security management system is thorough and well-thought-out. The certification audit will validate your documentation and force the entire organisation to follow your security policies. The certificate itself will be a guarantee to any interested party that you are committed to security.

Relevant standards

ISO 27001
Comprehensive cybersecurity standard, focussed on general or cloud companies.

IEC 62443
Comprehensive cybersecurity standard, focussed on machine security and industrial sites.

ISO 9001
Quality management standard, focussed on processes to maintain quality standards.

ISO 27701
Privacy standard, focussed on keeping personal information private.

And more...

Key parts of any standard

Scope
Describes what sites, products, departments or processes follow the standards.

External audit
An approved auditing agency will perform an audit on all requirements of the standard.

Proof
You must be able to prove that every rule, policy and process is performed as documented.