# 

[**Fabricon - Backstory - Short**](#_kv3o2ojur15e) **2**

[**Fabricon - Backstory - Extended**](#_mlk3pcibz7vv) **3**

[Company Overview](#_b6oevpsmv2j) 3

[Industry Focus and Supply Chain Position](#_klm63prtna5f) 3

[Fabricon’s Customers and Cybersecurity Expectations](#_jywxuu6pgdy1) 3

[Fabricon’s Suppliers and Supply Chain Risks](#_gx8mscztsxj) 3

[Suppliers](#_hwdetzraus63) 3

[Supplier Risks](#_zd2f6neqnbye) 4

[Manufacturing Technologies and Cybersecurity Challenges](#_twmv747wbhbq) 4

[Key Equipment and Technologies:](#_pejpcxw506q4) 4

[Key Roles and Responsibilities](#_fm8acl40rky6) 4

[Leadership Team Overseeing Cybersecurity:](#_896cte22ocar) 4

[**Fabricon’s Journey: Protecting the Value Chain**](#_rt8tkgv7pp7i) **5**

[**Fabricon’s Compliance Journey with Norm Ninja**](#_pmc9x4edtxbf) **8**

[Key Features Used:](#_4p65ainkfzqe) 8

[**Future Goals and Investments**](#_zfpz2d5v8pj3) **8**

# 

# Fabricon - Backstory - Short

Fabricon, a 120-person manufacturing company producing precision components for the automotive and aerospace sectors, operates within Europe’s critical supply chain infrastructure, which makes it subject to the NIS2 directive.

Although GDPR applies to some client and supplier data, Fabricon’s primary focus is on safeguarding production systems and sensitive operational data, which is essential to meeting client expectations for quality and reliability.

To meet these regulatory needs, Fabricon has established a unified cybersecurity framework combining ISO 27001 (for general information security), NIST CSF (for a structured cybersecurity approach), and IEC 62443 (to secure industrial control systems).

These frameworks help Fabricon address NIS2’s requirements for securing essential services, while ISO 27701 adds light but sufficient privacy management, aligning with GDPR on data protection basics.

Fabricon’s manufacturing operations rely on legacy production equipment, including CNC machines and SCADA systems, that lack built-in cybersecurity features, creating vulnerabilities. The company’s reliance on remote maintenance systems increases its risk level.   
Additionally, the company collaborates with multiple suppliers, increasing its exposure to third-party risks. Despite these challenges, Fabricon’s leadership is committed to elevating cybersecurity and compliance to protect its clients and maintain competitive positioning.

Fabricon Solutions operates in Europe’s critical supply chain, making compliance with NIS2 essential to safeguard production systems against cyber threats. NIS2 mandates strict cybersecurity practices for essential service providers, including manufacturers serving sectors like automotive and aerospace.

To meet these requirements, Fabricon uses NIST CSF to structure its cybersecurity approach, focusing on identification, protection, detection, response, and recovery.

ISO 27001 supports general information security, aligning well with NIS2’s requirements for protecting critical assets, while IEC 62443 is tailored to secure industrial control systems, covering Fabricon’s legacy manufacturing equipment vulnerabilities.

For handling client and supplier data, GDPR applies, and ISO 27701 extends Fabricon’s framework to address basic data privacy requirements.

Together, these standards create a unified reference model that meets both cybersecurity and data privacy needs, covering Fabricon’s critical assets and third-party interactions under one comprehensive compliance strategy. This integrated approach reduces complexity, ensuring effective alignment with regulatory demands.

# 

# Fabricon - Backstory - Extended

## Company Overview

# 

Fabricon is a Belgium-based medium-sized manufacturer with 120 employees, specializing in precision components for the automotive and aerospace industries. Established over 30 years ago, Fabricon has built a reputation for engineering excellence and reliable delivery, serving both Tier 1 and Tier 2 suppliers in Europe and the United States.

* Tier 1 Suppliers: Deliver finished systems or subassemblies directly to OEMs like Airbus, Boeing, Volkswagen, and BMW. Examples include brake systems, hydraulics, or engine modules.
* Tier 2 Suppliers: Provide individual components or materials to Tier 1 suppliers. Fabricon fits this role, producing precision parts such as fuel injectors, turbine blades, and sensor housings that are later integrated into larger systems.

Fabricon operates two production facilities near Antwerp, strategically positioned to leverage major European logistics hubs and international ports for seamless export.

The company supplies critical components to OEMs (Original Equipment Manufacturers) and defense contractors, making it a key player in Europe’s critical infrastructure and subject to the NIS2 Directive for cybersecurity compliance.

## Industry Focus and Supply Chain Position

### Fabricon’s Customers and Cybersecurity Expectations

Fabricon’s Tier 1 customers, including Bosch, ZF Friedrichshafen, Collins Aerospace, and Safran, demand strict cybersecurity standards aligned with:

* TISAX for automotive data protection (ISO 27K+ Automotive controls).
* AS9100D for aerospace quality standards (Quality Mgt).
* NIST SP 800-171 for securing defense-related data (Wetgeving).
* CMMC (Cybersecurity Maturity Model Certification) for US defense contractors (Wetgeving).

These customers expect end-to-end data protection, incident response plans, and supply chain security compliance in line with NIS2 and GDPR.

## Fabricon’s Suppliers and Supply Chain Risks

Fabricon depends on a global supplier network for raw materials, custom tooling, and software systems.

### Suppliers

* Material Providers:
  + Thyssenkrupp (Germany): High-performance metals for aerospace components.
  + BASF (Germany): Advanced polymers for injection molding.
  + Tooling and Equipment Vendors:
  + Mazak Europe: Supplies CNC machinery with remote diagnostic capabilities.
  + ABB Robotics (Switzerland): Provides automation systems integrated with Siemens PLCs.
* Software Vendors:
  + SAP S/4HANA ERP Platform: Manages inventory, production planning, and supplier data.
  + Siemens TIA Portal: Programs and manages PLC controllers.

### Supplier Risks

* Third-Party Access Risks: Vendors use remote tools like TeamViewer, creating vulnerabilities if access controls fail.
* Data Leakage Risks: Shared design files and CAD data require encryption to avoid theft or tampering.
* Compliance Gaps: Suppliers not meeting ISO 27001 standards can introduce weaknesses into Fabricon’s systems.

Fabricon mitigates these risks through vendor audits, contract clauses, and supply chain monitoring to enforce compliance.

## Manufacturing Technologies and Cybersecurity Challenges

Fabricon combines traditional manufacturing equipment with modern technologies, exposing it to cybersecurity risks.

### Key Equipment and Technologies:

* Production Equipment:
  + Mazak Integrex i-400 (5-axis CNC): Produces high-precision aerospace parts but operates on Windows XP Embedded, making it vulnerable to malware and ransomware attacks.
  + Trumpf TruLaser 3030 (Laser Cutting): Processes metal sheets for engine brackets but depends on networked SCADA controls, susceptible to command injection attacks.
* Industrial Control Systems (ICS):
  + Siemens SIMATIC S7-300 PLCs: Automates robotic assembly lines but lacks encryption, risking unauthorized access.
  + GE iFIX SCADA Systems: Monitors machine performance but is vulnerable to man-in-the-middle attacks without network segmentation.
* IT Infrastructure:
  + Cisco Meraki Firewalls: Protects network traffic but must be continually updated to resist evolving phishing attacks.
  + Splunk Enterprise Security: Provides real-time monitoring but requires ongoing rule updates to detect advanced threats.

## Key Roles and Responsibilities

### Leadership Team Overseeing Cybersecurity:

* Elena Rousseau – CEO:
  + Leads compliance with NIS2, focusing on risk governance and supply chain security.
* Marco De Wit – Head of Operations:
  + Secures production processes and enforces IEC 62443 for ICS systems.
* Pieter De Smet – IT Manager:
  + Implements ISO 27001 controls, manages network defenses, and responds to cyber incidents.
* Annelies Janssen – Compliance Officer:
  + Tracks GDPR and NIS2 compliance using Norm Ninja for risk assessments and action tracking.
* Ellen Vervoort – HR Manager:
  + Oversees employee training, including phishing simulations and awareness programs.

# 

# Fabricon’s Journey: Protecting the Value Chain

Fabricon, a 120-person manufacturing company in Europe, is an expert in producing precision components for the automotive and aerospace sectors.

As a critical link in Europe’s supply chain, they faced new regulatory challenges with the introduction of the NIS2 directive.

One morning, CEO Elena gathered her leadership team: “With NIS2 now in effect, we have significant cybersecurity obligations,” she began. “We must safeguard our production systems and sensitive operational data. Our legacy equipment and extensive supplier network add complexity, but we can’t ignore this.”

**1. Organizational Scoping: Discovering Standards and Mapping Capabilities**

Seeking a solution, Fabricon adopted a compliance platform designed for SMEs, called SimplTrust.

They started with **Organizational Scoping**, using industry-based templates provided by the platform. Through a plain-language questionnaire, they identified applicable regulations and standards: NIS2, GDPR, ISO 27001, NIST CSF, IEC 62443, and ISO 27701.

The platform generated a **business capability map**, outlining key functions like manufacturing processes, quality control, and supply chain management. The team tweaked the templates to reflect their unique operations.

“This map shows how regulations apply directly to our business functions,” noted Marco, the Head of Operations. “It gives us clarity on where to focus our compliance efforts.”

**2. Unified Control Framework: Automated Mapping and Simplification**

Next, they moved to the **Unified Control Framework**. Leveraging its extensive library of templates, the platform automatically mapped the regulatory requirements to the selected industry standards. Overlapping controls were identified and consolidated.

“Look, the platform suggests how to address multiple regulations with unified controls,” Elena observed. “We don’t have to do the mapping ourselves.”

This automated approach streamlined their compliance efforts, reducing redundancy and complexity.

**3. Asset Management: Linking Assets to Regulations and Capabilities**

In the **Asset Management** phase, they cataloged all their assets:

• **Processes**: Manufacturing workflows, quality assurance procedures.

• **Teams**: Engineering, procurement, IT support.

• **Data Objects**: Client specifications, production data, supplier contracts.

• **Physical Devices**: Legacy machines, control systems, assembly lines.

Each asset was linked to the regulatory requirements and business capabilities identified earlier. This established clear connections between their assets, the applicable regulations, and their operational functions.

“By linking assets to both regulations and capabilities, we see how vulnerabilities could impact our entire operation,” Marco commented

.

**4. Assessment Planning and Execution: Engaging the Team**

They proceeded to **Assessment Planning**, scheduling evaluations based on asset criticality. High-priority assets like production systems were slated for frequent reviews. The platform synced these schedules with team calendars and sent automated reminders.

During **Assessment Execution**, teams across the company used provided templates and checklists to evaluate controls, collect evidence, and document findings. The user-friendly tools made it easy for everyone to participate, not just compliance experts.

**5. Gap Analysis & Reporting: Identifying and Prioritizing Risks**

After assessments, the platform performed a **Gap Analysis**, highlighting critical vulnerabilities:

• **Unsecured Legacy Equipment**: Lack of modern cybersecurity features.

• **Supplier Risks**: No formal evaluation of supplier cybersecurity practices.

• **Employee Training Gaps**: Inconsistent cybersecurity awareness.

Gaps were prioritized based on their potential impact on the value chain. The platform offered actionable recommendations for each issue.

“Now we know exactly where to focus our efforts,” Elena said. “The risks are clear, and so are the solutions.”

**6. Risk Assessment and Action Planning: Focusing on What Matters**

They conducted a **Risk Assessment**, evaluating the impact and likelihood of each identified gap. With the platform’s guidance, they developed action plans:

• **Secure Legacy Equipment**: Implement network segmentation and update security protocols.

• **Enhance Supplier Management**: Establish a supplier risk assessment program.

• **Improve Employee Training**: Roll out comprehensive cybersecurity training modules.

Tasks were assigned to specific teams, resources were allocated, and timelines were established.

**7. Implementation Tracking and Continuous Monitoring**

As they began implementing solutions, the platform provided **Implementation Tracking** through visual dashboards and progress indicators. Automated alerts reminded teams of upcoming deadlines and flagged any delays.

Simultaneously, **Continuous Monitoring** kept an eye on key compliance and risk metrics. One day, the platform’s AI-powered detection alerted them to unusual activity in their data systems.

“Thanks to this alert, we caught a potential issue early,” Marco reported. “We addressed it before it became a serious problem.”

**8. Training and Awareness: Empowering Employees**

Understanding that technology alone wasn’t enough, they utilized the platform’s **Training and Awareness** programs.

Customized modules educated employees on cybersecurity best practices relevant to their roles.

• **Production Teams** learned about securing legacy equipment.

• **Procurement Staff** received training on supplier risk management.

• **All Employees** completed courses on data protection and phishing awareness.

“Our team’s cybersecurity awareness has significantly improved,” Elena remarked. “They’re now an active part of our defense.”

**9. Effectiveness Evaluation and Strategic Review**

Using the **Effectiveness Evaluation** tool, they measured the impact of their actions:

• **Reduced High-Risk Vulnerabilities**: Legacy equipment was secured.

• **Strengthened Supplier Security**: Supplier assessments were implemented.

• **Enhanced Employee Competence**: Training completion rates increased.

In a strategic review meeting, they aligned compliance efforts with business goals. Protecting their value chain not only met regulatory requirements but also enhanced client trust and competitiveness.

“We’ve turned compliance into a strategic asset,” Elena concluded. “It supports our growth and solidifies our market position.”

**10. Regulatory Updates: Staying Ahead**

Finally, the platform’s **Regulatory Update** feature kept them informed of any changes in relevant regulations. Updates to NIS2 or GDPR were automatically reflected in their Unified Control Framework, ensuring continuous compliance.

“We no longer need to constantly monitor for regulatory changes,” Marco said. “The platform does it for us.”

**Conclusion: Turning Compliance into Competitive Advantage**

Fabricon’s journey transformed their approach to compliance and cybersecurity. By leveraging the platform’s automated guidance and integrating compliance into every aspect of their business—from assets and processes to teams and data—they protected their value chain effectively.

“Compliance isn’t just about avoiding fines,” Elena addressed her team. “It’s about building trust, ensuring quality, and driving our company forward.”

Through a user-friendly platform, Fabricon turned complex regulatory demands into manageable actions, safeguarding their business and turning compliance into a competitive advantage.

# Fabricon’s Compliance Journey with Norm Ninja

Fabricon adopted Norm Ninja to simplify cyber compliance and manage its NIS2 and GDPR obligations.

## Key Features Used:

* Organizational Scoping: Maps vulnerabilities in legacy systems and PLC networks.
* Risk Assessments: Evaluates threats in remote access tools and data storage systems.
* Action suggestion and tracking: Assigns tasks for upgrading firewalls, implementing encryption, and segmenting SCADA systems.
* Training Programs: Delivers e-learning modules and tests employee preparedness through simulated attacks.

# Future Goals and Investments

Fabricon is investing in:

* Modernizing Equipment: Replacing older Windows XP-based controllers with secure Linux systems.
* Zero-Trust Architecture: Enforcing multi-factor authentication (MFA) and role-based access controls (RBAC).
* AI-Based Monitoring Tools: Deploying Darktrace AI for behavioral anomaly detection and threat hunting.
* Supply Chain Security Audits: Ensuring ISO 27001 compliance among suppliers.