ANDING & COMPANY

NIS2 Compliance for Medium-Sized Businesses

Playbook & Client Example

August 2026

NIS2 Compliance for MEs: Challenges and solution approach for an actionable compliance program

- **NIS2 Directive:**
  - EU directive from 2022 that **harmonizes and significantly tightens cybersecurity requirements** for organizations in the EU
  - Requires organizations to **establish and maintain an Information Security Management System (ISMS):** a structured framework covering risk management, incident response and business continuity
  - Violations can result in **fines of up to €10 million** or **2% of global annual revenue** (whichever is higher)
  - Management bears **formal responsibility for compliance** and **may be held accountable** in case of significant breaches
- **Challenges:**
  - The **complexity of the NIS2 requirements** leaves SMEs **without clear guidance** on the **measures required** and the appropriate **level of implementation**
  - Relevant **processes**, **workflows**, and **information** often already exist, but **remain informal and undocumented**
  - Once established, the ISMS often **lacks a clear maintenance plan** and dedicated **ownership by an ISMS representative**
- **Solution:**
  - A **structured**, **project-based implementation approach** that translates NIS2 requirements into clear policies, processes, and documented evidence
  - The result is a **right-sized ISMS** that can be **effectively maintained in day-to-day operations** and is supported by **organization-wide awareness**

Source: Anding Analysis

Agenda

- Intro NIS2 Compliance & Implementation Approach
- Client Example

NIS2 affects ~30,000 German companies: Broad and unclear scope make compliance a challenge

What is NIS2?

NIS2 (**Network and Information Security Directive 2**) is an EU directive that harmonizes and significantly tightens **cybersecurity requirements** for organizations across the EU

Key objectives:

- Strengthen the resilience of critical infrastructure: mandatory incident reporting within 24h/ 72h/ 1 month
- Harmonize **security standards** across the EU single market

Accountability & penalties:

- Violations can result in **fines of up to €10 million or 2% of global annual turnover** (whichever is higher)
- Management **bears formal responsibility** for compliance

Who is affected by NIS2?

~160,000 entities across the EU, incl. **~30,000 in Germany**, classified as **Essential** or **Important** based on **sector and size**

	Highly critical sectors*	Other critical sectors**
Large (250+ employees or >€50m turnover)	**Essential**	*Important*
Medium (50+ employees or >€10m turnover)	*Important*	*Important*

*Highly critical: energy, transport, banking, healthcare, water, digital infrastructure
**Other critical: postal, waste, food, chemicals, manufacturing, research

What is the challenge of NIS2?

- **Complex** and **broad requirements** make it difficult for MEs to identify **clear, actionable steps**
- The **absence of a formal certification** creates uncertainty around **how measures should be applied**
- **Unclear expectations** encourage **over-compliance** instead of **a pragmatic, balanced approach**
- Sustained compliance **requires continued effort** and **clear ownership over time**

Source: Anding Analysis, BSI, European Commission

Our NIS2 implementation approach is built on 3 core principles

Pragmatic: Implementation tailored to ME-specific context

Management-compatible: Progress, outcomes and implications communicated at management level

Sustainable: ISMS set up to be independently managed within ME

Source: Anding Analysis

Consolidation of complex, often ambiguous requirements into a single point of truth with clear measures for compliance

CLIENTCO EXTRACT

Regulatory baseline & assessment of relevance *controls derived from §30 BSIG and ISO 27001:2022, assessed for appropriate level of implementation*						**Client assessment** *current status, priority of implementation, effort associated and assessment maturity*				**Evidence** *concrete deliverables derived from abstract requirements, with clear ownership*			**Implications** *conclusion per control and resulting actions for the client*	
Control/ Clause No.	**Category**	**Topic/ Control Name**	**Official Description** (ISO 27001:2022)	**§30(2) No.**	**ME Relevance**	**Status** (Fulfilled / Partial / Planned / Open / n/A)	**Answer First Criticality** for our Project	**Easy to fix**	**Anding Confidence based on Evidence (1 - 5 Scale)**	**Typical evidence for ME Companies**	**ClientCo Evidence**	**Provided by Anding**	**Anding Assessment**	**Next Steps for ClientCo**
5.3	**Clause** *(Manage-ment System)*	**Organizational roles, responsibilities and authorities**	Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated	Nr. 1	◕	●			**5**	▪ RACI documentation about ISMS roles ▪ Role description in ISMS Handbook or organizational chart with security roles	RACI Table	ISMS Handbook	The ISMS Handbook and RACI sufficiently address the requirements of the clause	n/A

Total of 110 Clauses and Controls

Source: Anding Analysis

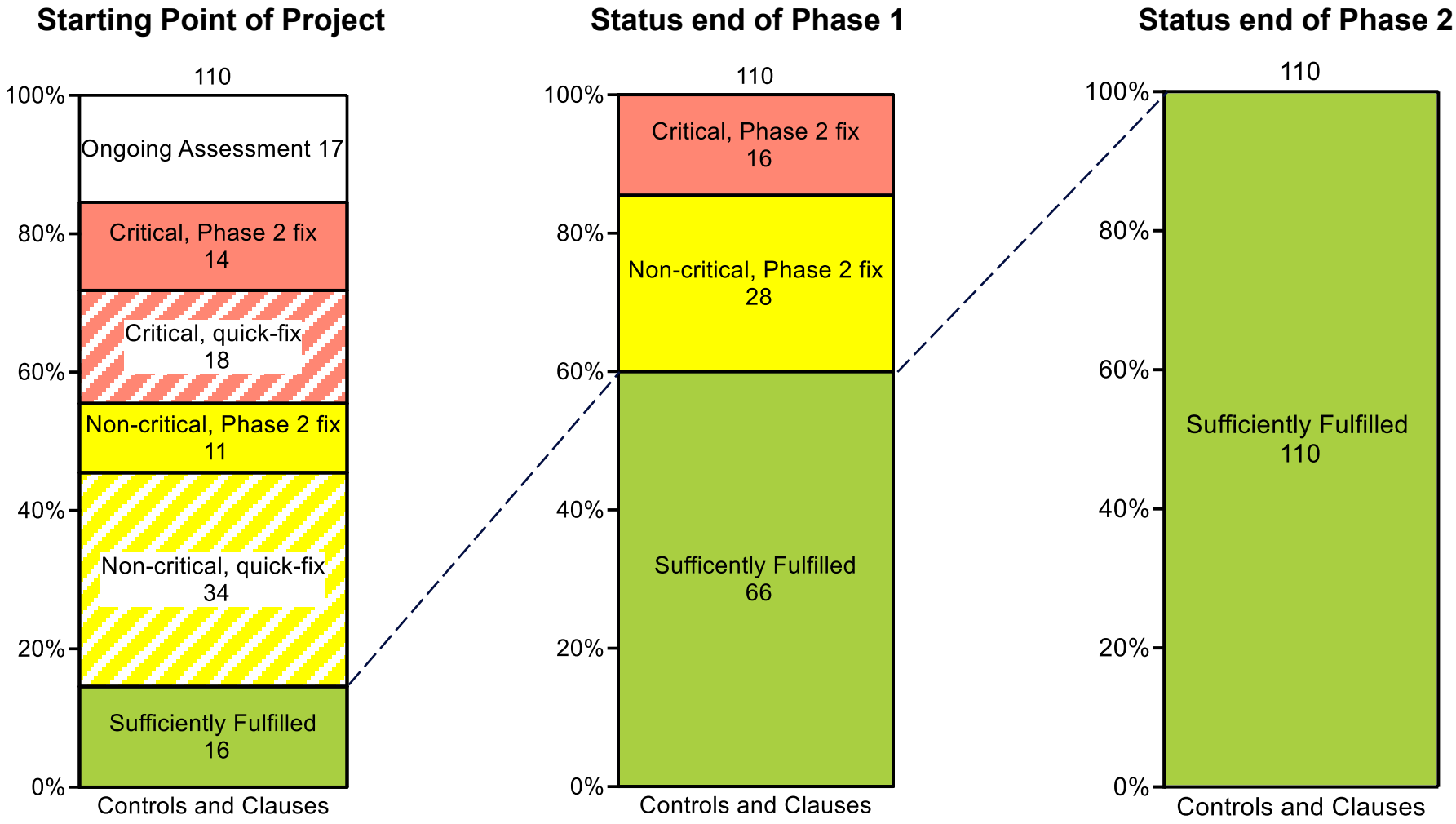
Deliberate reduction of underlying complexity to provide management with a clear view of progress and direction

CLIENTCO EXAMPLE

Critical:
little to nothing in place yet; critical to address

Non-critical:
- less relevant for MEs
- already largely in place; "full compliance" requires additional steps

Sufficiently Fulfilled:
Effectively completed; only limited minor actions remain in a few cases on ClientCo's side



Source: Anding Analysis

Structured handover of ownership and recurring activities to embed the ISMS in operations and sustain compliance

Risks
Top risks
New risks
Risk development

Emergency management
Emergency plans
Fire drill / exercises

Audits
internal Audits
external Audits
non-conformities

Measures
Open measures
Overdue measures

Security incidents
Quantity
Criticality
Causes

Security incidents
Risk management
Number of fulfilled controls
Number of incidents
Status of recurring audits

Suppliers
Critical service providers
Relevant incidents

Annual management report
ISMS report summarizing key activities and developments for management briefing

Source: Anding Analysis, mv it

Our implementation approach builds on translating §30 BSIG NIS2 requirements into actionable security controls

Influenced by the ME-specific relevance of each control

§30 BSIG Risk Management Measures

1. **Risk Management**
   (establishing a methodology to identify, assess, and treat security risks)
2. **Incident Response**
   (processes to detect, respond to, and report incidents)
3. **Business Continuity**
   (backup management, disaster recovery, and crisis)
4. **Supply Chain Security**
   (assessing and managing security risks from suppliers and service providers)
5. **Security Acquisition, Development & Maintenance**
   (including vulnerability management and disclosure throughout the IT lifecycle)
6. **Policies for assessing risk management effectiveness**
   (regular review of whether security measures actually work)
7. **Cybersecurity Training & Awareness**
   (educating staff on cyber hygiene and threats)
8. **Cryptography**
   (policies and processes for encryption and key management)
9. **Access Control & Asset Management**
   (defining who can access what, and how systems/products are managed)
10. **Multi-Factor Authentication & Secure Communications**
    (including secure emergency communication channels where applicable)

Mapping

Source: Anding Analysis

Leveraging client knowledge and existing assets, our approach translates NIS2 requirements into a tailored ISMS

ILLUSTRATIVE

Baseline Assessment

Establish a comprehensive view of the status quo through structured stakeholder interviews:

- Capture existing **documentation and evidence**
- Formalize **undocumented processes and practices**

Anding NIS2 Framework

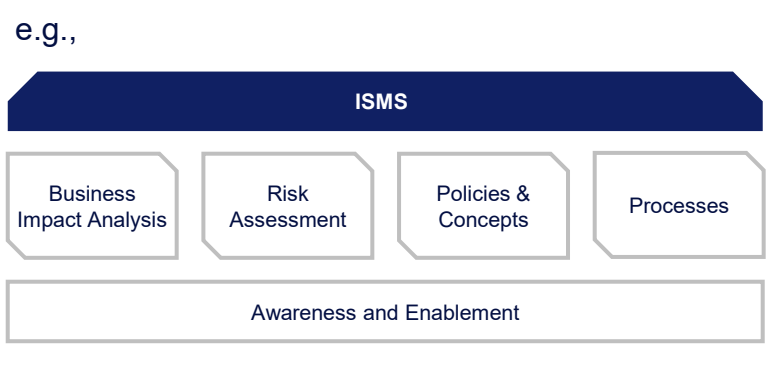
Assess the status quo against the defined NIS2 security controls:

- Consolidate inputs into a **single assessment framework**
- Derive **gaps, priorities and required actions**

ISMS Implementation

Implement a tailored ISMS:

- Address prioritized gaps through **policies, concepts and**, where needed, **technical measures**
- Establish the ISMS as the **central structure** consolidating NIS2-related activities



Source: Anding Analysis

Operational challenge: Aligning diverse stakeholders with the right level of involvement alongside day-to-day operations

Managing Director

Interaction needs to be selective, while ensuring sufficient transparency and enablement for the MD to fulfill their accountability

Process Owners

Required input needs to be collected despite limited availability and competing day-to-day priorities

Management Team

Results need to be consolidated into a management-level view to support informed decision-making

ISMS Representative

The role often needs to be newly established and efficiently enabled alongside day-to-day responsibilities

Internal IT

Measures need to be feasible within existing IT structures and capabilities

Anding Team

Our approach **orchestrates stakeholder involvement** throughout the implementation, balancing **efficient input collection**, **management transparency** and **clear ownership** while **minimizing time and effort** required from ME

Source: Anding Analysis

Agenda

- Intro NIS2 Compliance & Implementation Approach
- Client Example

Client example: Building a standalone, ME-compatible ISMS following a corporate carve-out

CLIENT EXAMPLE

Situation

- ClientCo is a carved-out, PE-backed consumer electronics company, previously part of a global technology group
- As an independent legal entity, ClientCo must establish its own NIS2 compliance and governance setup previously provided at group level
- ClientCo is subject to NIS2 as a manufacturer of electronic and optical products meeting the applicable size criteria
- Project objective: Implement NIS2 and establish an ME-compatible ISMS

Challenges

- Limited internal expertise and dedicated resources to address NIS2 independently
- Relevant processes and practices often existed informally, but lacked formal documentation
- Existing group-level policies did not fit ClientCo's less complex, mid-sized setup
- Ongoing transformation meant that the organizational setup continued to evolve throughout the project
- No clear setup for ongoing ISMS management or dedicated ISMS representative in place

Results

- Comprehensive NIS2 compliance baseline established across all applicable controls
- Existing practices formalized and tailored policies, concepts and processes established for ClientCo's setup
- Management involvement and company-wide NIS2 awareness established
- ME-compatible ISMS set up for independent ownership and ongoing management

Source: Anding Analysis

~10 weeks NIS2 Project covering status quo assessment to operational documentation and ISMS set-up

SIMPLIFIED OVERVIEW

1 week → | 6 weeks → | 3 weeks →

Kick-Off & Status Quo

1.1 Kickoff
- Alignment on objectives, scope and timeline
- Initial review of current NIS2 status

1.2 Identification of Process Owners
- Identification of relevant process owners and subject-matter experts
- Preparation of interview schedule

1.3 Assessment of existing documentation
- Review of available policies and documentation

Interviews & Documentation

2.1 Execution of Interviews
- Execution of structured interviews with relevant subject-matter experts
- Capture of existing processes, practices and related risks

2.2 Gap Assessment & Prioritization
- Assessment of the status quo against defined NIS2 controls
- Identification and prioritization of gaps and required actions

2.3 Addressing of Initial Gaps
- Creation of required policies, process descriptions and other ISMS documentation (e.g., BIA, Risk Register, Statement of Applicability…)

ISMS Setup & Enablement

Optional

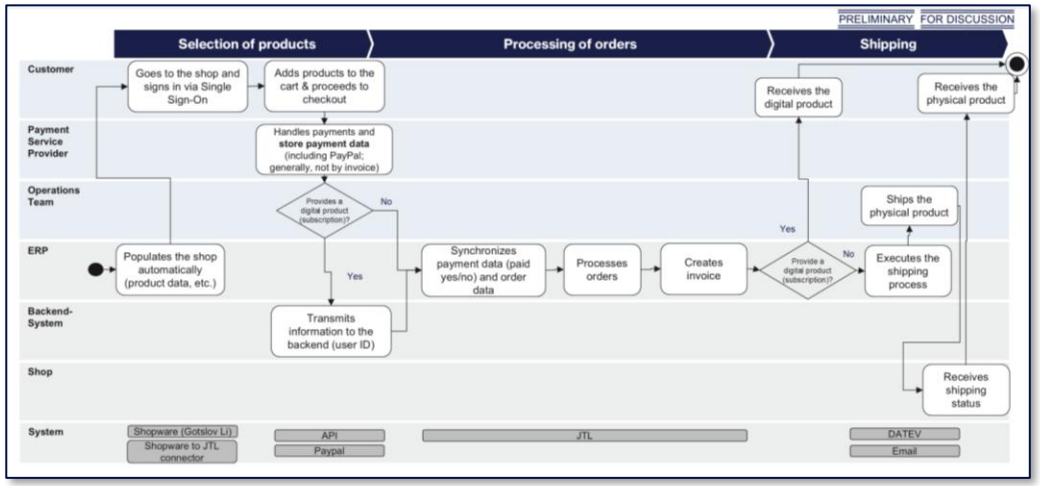
3.1 Information Security Management Setup
- Set-up of a pragmatic and automated ISMS, e.g., in SharePoint

3.2 Addressing of More Extensive Controls
- Development of required concepts and collection of additional evidence

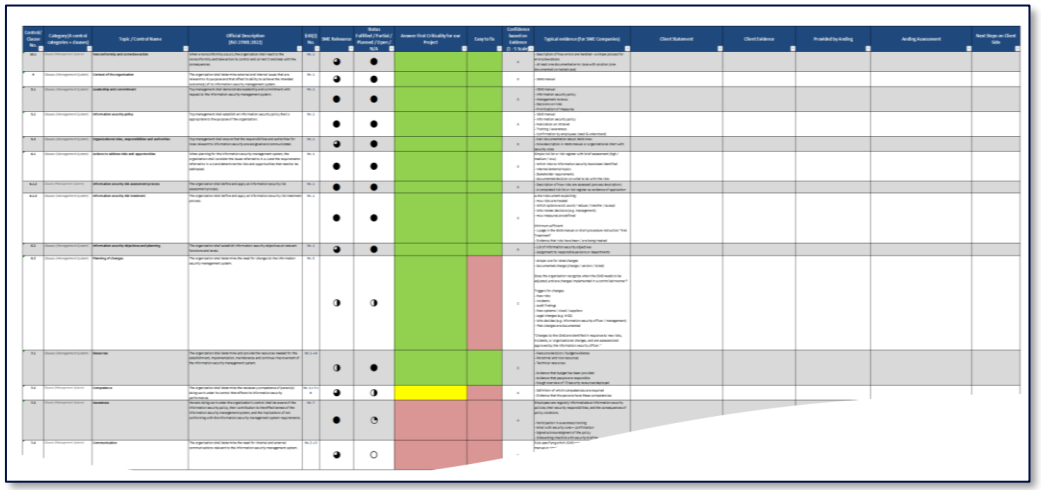
3.3 Communication, Awareness and Enablement
- Preparation of management report and review
- Communication of the new ISMS and related documentation
- Handover and enablement for ongoing compliance activities

Source: Anding Analysis

Typical outputs: Translating stakeholder input into structured assessment and documentation

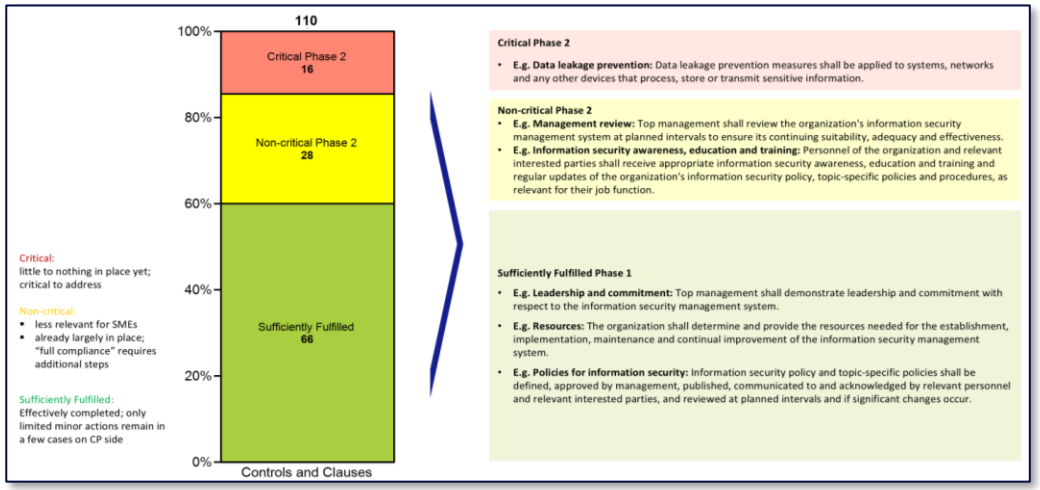


Capture of existing processes based on interviews

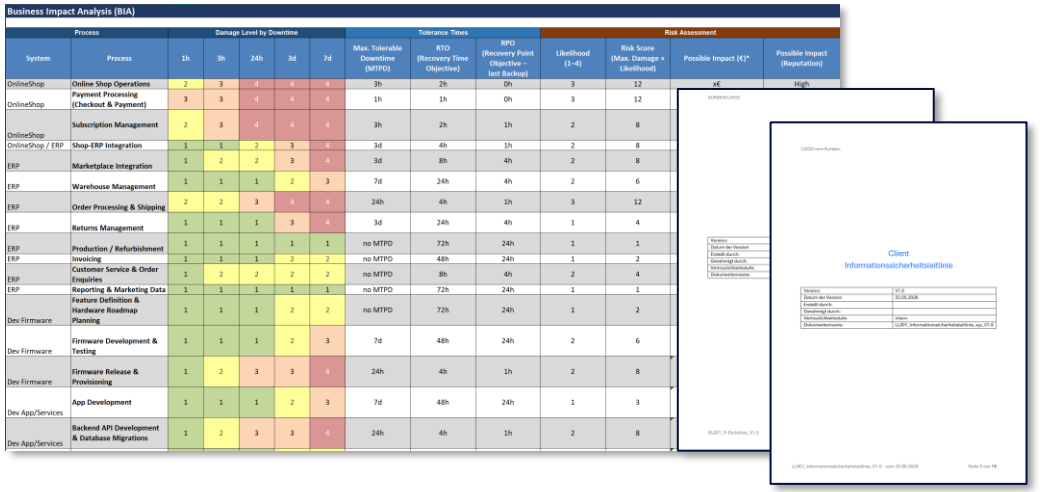


SELECTION

Assessment of the status quo against NIS2 controls



Identification and prioritization of gaps and required actions

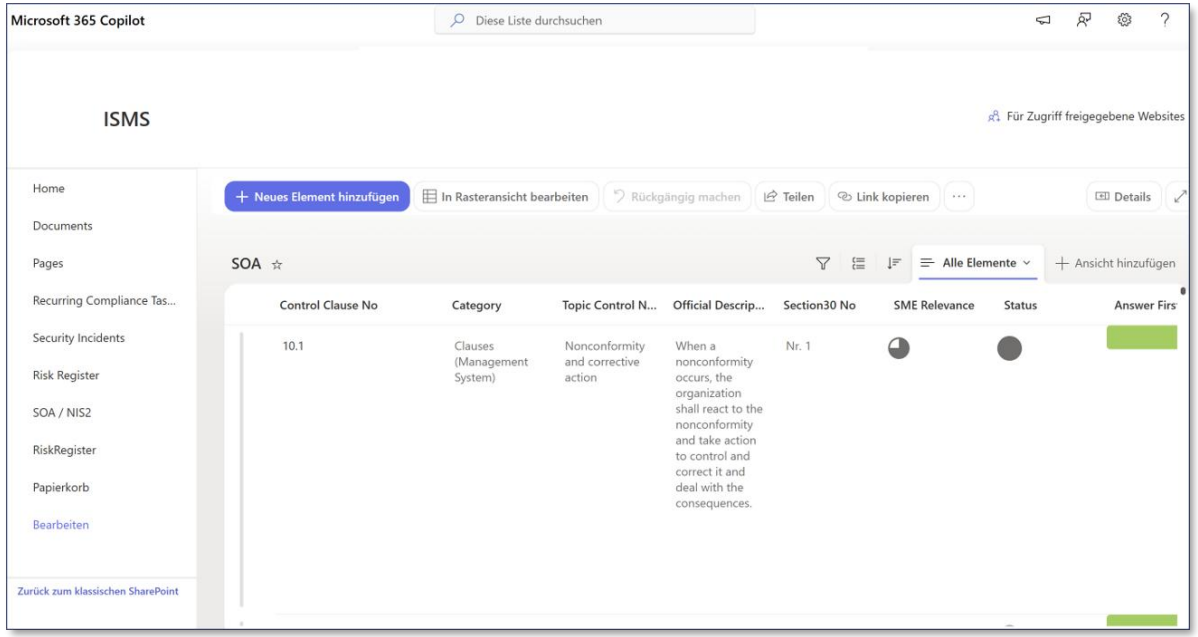


Creation of policies and other ISMS documentation (e.g., BIA)

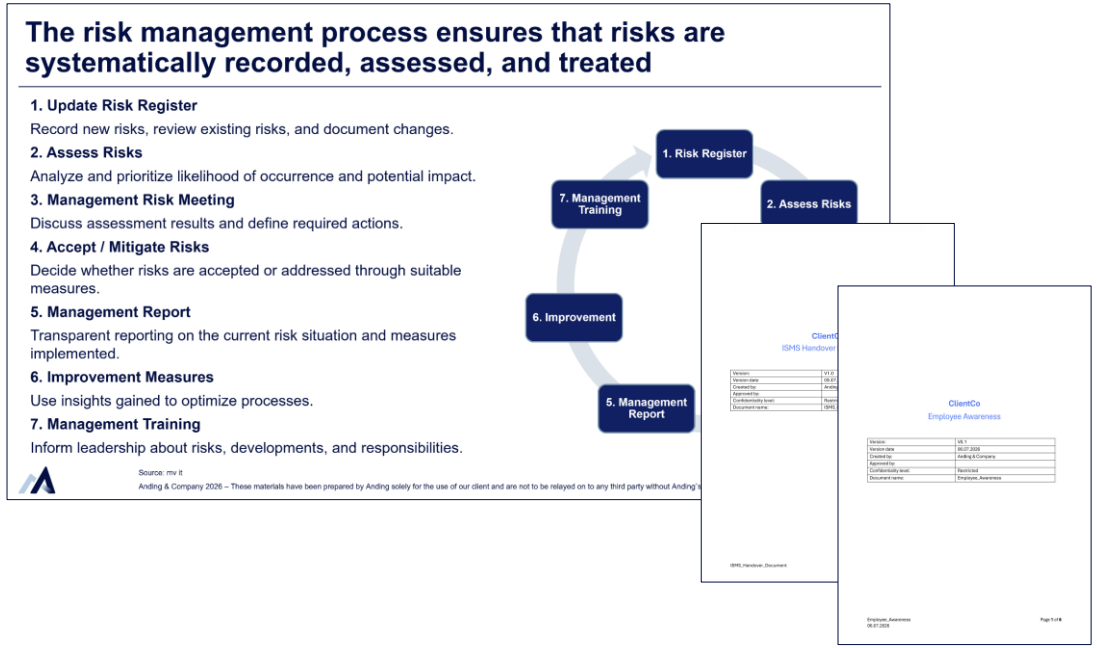
Source: Anding Analysis

Typical outputs: Pragmatic ISMS setup and enablement for ongoing compliance management

SELECTION



Set-up of a pragmatic and automated ISMS, e.g., in SharePoint



Enablement for ongoing compliance activities and communication of ISMS and relevant documentation

Source: Anding Analysis

Effective working mode combining Anding's NIS2 expertise with focused client involvement

FOR DISCUSSION

ANDING & COMPANY x IT Partner

- **Provide expertise** for NIS2 assessment and implementation based on experience from comparable client projects
- **Bring the right framework** to structure the implementation and enable the client team
- **Orchestrate stakeholder involvement** to ensure efficient input collection, clear ownership and management transparency
- **Do the heavy lifting** on interviews, evidence collection, analysis and results documentation
- **Create clarity in a complex regulatory environment** and provide management with a **transparent view of status and gaps**
- **Provide seamless control documentation** and lay the foundation for a **client-owned, living ISMS**

Client

- **Set us up for success** with relevant documentation and insights to quickly understand the starting point
- **Connect us with relevant stakeholders** and facilitate interview scheduling
- **Provide access to required data and information** *(e.g., evidence, existing policies)*
- **Share technical expertise** on existing concepts, identified risks and the current compliance setup
- **Give timely feedback** on deliverables, frameworks and proposed direction
- **Engage in the knowledge transfer** to enable independent ongoing management of the ISMS

Source: Anding Analysis


ANDING
& COMPANY