

GOVERNANCE DOCS

BSI C5:2026

Gap Assessment Report

BSI Cloud Computing Compliance Criteria Catalogue C5:2026

Nordlicht Cloud Services (sample)

The managed Kubernetes platform and its two German data centre regions.

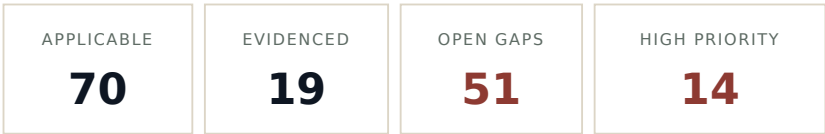
ASSESSED	25 September 2026
EDITION	C5:2026, published 7 April 2026, applies to engagements from 1 June 2027
IN SCOPE	73 requirements, 70 applicable
PROFILE	Technology, software and SaaS · 50 to 249 people · BSI
PREPARED BY	Governance Docs

CONTENTS

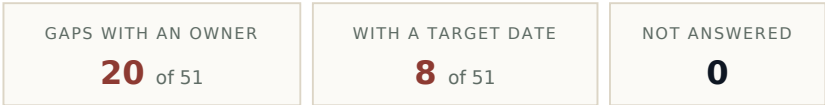
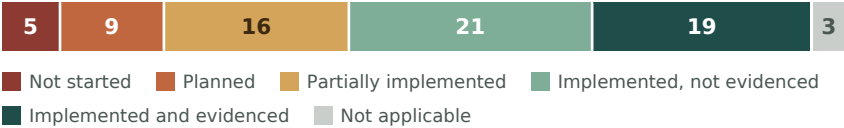
- 1 Executive summary
- 2 Readiness by area and where the next points come from
- 3 Remediation plan
- A About this report

Confidential. Prepared for Nordlicht Cloud Services (sample) from its own self-assessment; not independently verified by Governance Docs (see section A). Share on a need-to-know basis.

Where Nordlicht Cloud Services (sample) stands against BSI C5



STATUS OF EVERY REQUIREMENT



WHAT THIS ASSESSMENT TELLS YOU

- Overall readiness is 64.3% against BSI C5 across 70 applicable controls. 19 of them are implemented and evidenced.
- Most open gaps: Operations, with 9 at 69%. Strongest area: Identity and cryptography at 88%.
- 21 controls are operating but not evidenced. Collecting their records alone lifts the score to 71.8% (+7.5 points), the cheapest gain available.
- 14 gaps are high priority (not started or only planned); 4 of them are in Incidents, continuity, compliance and investigations.

DO THESE FIRST

	PRIORITY	ACTION	OWNER	START FROM
1	HIGH	Put an owner and date against the 4 high-priority gaps in Incidents, continuity, compliance and investigations	Risk Manager	Post-Incident Review & Lessons Learned Template
2	MEDIUM	Adopt and tailor the Client (Tenant) Separation & Isolation Standard, which closes 3 open gaps	To assign	Client (Tenant) Separation & Isolation Standard
3	LOW	Evidence the 21 controls that already operate (+7.5 points)	To assign	Records the controls already produce

Analysis and priorities

IN ONE SENTENCE

You stand at Developing with 51 open gaps, and you should focus first on resolving high-priority software development controls.

AI-assisted analysis, generated from the information the organization provided and checked automatically against the scores and findings in this report. It supports planning and is not an audit opinion; see "Basis of this report and limitation of liability".

FOR SENIOR MANAGEMENT AND THE BOARD

We stand at readiness level 2 of 4, Developing, with an overall score of 64.3% across 70 applicable requirements. Our main exposures lie in development and continuity planning, where critical safeguards have not started. While many technical measures are in place, 21 controls lack formal audit evidence. We need executive leadership to require named owners and target dates for all 51 open gaps, and to allocate team time to formalize secure development and continuity procedures immediately.

WHERE YOU STAND

Your self-assessment places the organization at readiness level 2 of 4, named Developing, with an overall score of 64.3%. Out of 70 applicable requirements, you recorded 51 open gaps and 14 high priority gaps. While 19 requirements are implemented and evidenced, 21 are implemented without evidence, and 5 have not started. Furthermore, 20 gaps have an assigned owner and 8 have a target date. The assessment shows that foundational practices exist, but operational consistency and formal tracking remain limited across several departments.

WHAT IT MEANS FOR THE ORGANIZATION

The pattern indicates that technical controls operate in daily routines but lack documentation and verifiable proof. Development scored lowest at 25%, while Incidents, continuity, compliance and investigations reached 31.3%. This creates business exposure because external reviewers and the BSI expect documented evidence for essential workflows. Evidencing what already runs would increase your overall score to 71.8%. Without systematic governance, however, unevidenced controls leave you vulnerable to operational disruption, and the absence of development policies directly weakens your security architecture.

WHERE TO FOCUS FIRST

You should focus first on high priority gaps in software engineering and continuity planning to establish basic control boundaries. Formalizing policies for development, change management, and disaster recovery will resolve your most severe exposures. Next, assemble records for the 21 controls that are implemented but not evidenced to raise your score quickly. Ensure every open gap receives an assigned owner and completion date to establish internal accountability. Standardizing client isolation and access procedures will help you address several shared operational requirements efficiently.

PRIORITIES

PRIORITY	WHY IT MATTERS	FIRST STEP	START FROM	WITHIN	
1	Establish secure software development policies and change approvals DEV-01/02/14 Development policy, outsourcing and third-party components · DEV-09/10/15 Version control, production approval and exceptions	Development scored lowest at 25% with core controls not started. Unvetted third-party components and unapproved code changes expose services to operational failure and regulator scrutiny.	Draft the baseline software development policy covering third-party components and production release approval criteria.	Secure Software Development Lifecycle (SDLC) Policy Comprehensive BSI C5:2026 Cloud Toolkit – 107 Compliance Templates	30 DAYS
2	Formalize disaster recovery plans and post-incident learning SIM-06 Evaluation and learning · BCM-03/04 Continuity plans and testing	Incidents and continuity scored 31.3% with no formal continuity plans active. Untested recovery procedures leave systems unable to demonstrate resilience during major operational outages.	Document the core disaster recovery plan and outline procedures for post-incident reviews.	Disaster Recovery Plan Comprehensive BSI C5:2026 Cloud Toolkit – 107 Compliance Templates	30 DAYS
3	Implement internal audit procedures and security governance COM-02/03 Audit planning and internal audit · OIS-01/02 ISMS and information security policy	A planned governance structure and missing audit routines leave internal control deficiencies undetected. Regular audit routines are essential to meet baseline supervisory expectations.	Adopt the internal audit procedure and establish an audit findings register.	C5 Internal Audit Procedure Comprehensive BSI C5:2026 Cloud Toolkit – 107 Compliance Templates	60 DAYS
4	Standardize backup verification and cross-network administration access OPS-06/07/08/09 Backup and recovery · COS-04/05 Cross-network and administration access	Unverified recovery routines and administrative network access gaps jeopardize core infrastructure integrity. Securing administrative channels prevents unauthorized operational changes across segmented environments.	Define testing intervals for backup recovery and formalize remote administration access rules.	Backup & Recovery Procedure Comprehensive BSI C5:2026 Cloud Toolkit – 107 Compliance Templates	60 DAYS
5	Evidence client tenant separation and isolation standards COS-06/07 Traffic separation and topology documentation · OPS-30/31 Separation of datasets	Proving tenant separation resolves multiple open findings across operations and communications. Providing evidence for already running controls lifts your score to 71.8%.	Assemble network architecture diagrams and isolation rules that demonstrate client dataset segregation.	Client (Tenant) Separation & Isolation Standard Comprehensive BSI C5:2026 Cloud Toolkit – 107 Compliance Templates	90 DAYS

30 / 60 / 90-DAY ROADMAP**FIRST 30 DAYS**

- Assign owners and target dates to all 51 open gaps across the organization.
- Draft the secure software development lifecycle policy covering third-party components.
- Document the disaster recovery plan and testing procedures.

DAYS 31 TO 60

- Establish the internal audit procedure and corrective action tracking register.
- Formalize backup recovery procedures and review remote administration access controls.
- Implement change management and application security testing procedures.

DAYS 61 TO 90

- Gather audit evidence for the 21 controls already operating in daily workflows.
- Document the client tenant separation and isolation standard across environments.
- Conduct business impact analyses and record recovery time objectives.

Maturity across the standard

Each bar shows how the requirements in one area break down by status, weakest on the left. The score is the average across applicable requirements; the chips count open gaps by priority.

AREAS	STATUS MIX	SCORE	GAPS H · M · L
Governance, policy and people		70%	
Assets and physical security		67%	
Operations		69%	
Identity and cryptography		88%	
Communications, portability and suppliers		59%	
Development		25%	
Incidents, continuity, compliance and investigations		31%	
Product security and the attestation		78%	

■ Not started
 ■ Planned
 ■ Partially implemented
 ■ Implemented, not evidenced
 ■ Implemented and evidenced
 ■ Not applicable

WHERE THE NEXT POINTS COME FROM

The score after each kind of work, cheapest first. Gold is what that step adds.

Today		64.3%
Evidence what already runs 21 requirements		71.8% +7.5
Finish what is partly in place 16 requirements		83.2% +11.4
Implement what is planned 9 requirements		92.9% +9.7
Start what has not begun 5 requirements		100.0% +7.1

DOCUMENTS THAT CLOSE THE MOST GAPS

Each bar counts the open gaps that name the document as the way to close them.

Client (Tenant) Separation & Isolation Standard		3
Cryptography and Key Management Policy		3
Network Security Policy		3
Information Security Governance Framework		2
Information Security Risk Management Procedure		2
Information Security Risk Register		2

All of these are in the BSI C5:2026 Cloud Toolkit (107 documents).

Every open gap, grouped by what has to happen next

Work from the top. Requirements not yet started or only planned are the ones a certification auditor reaches first; the last group already operates and needs only its records.

HIGH Not started · 5

Start from a documented baseline: adopt and tailor the document named below, then put it into operation.

Ref	Requirement	Area	Owner · target	Closes it
DEV-01/02/14	Development policy, outsourcing and third-party components	Development	To assign	Secure Software Development Lifecycle (SDLC) Policy · Procurement & Supply Chain Security Policy
DEV-09/10/15	Version control, production approval and exceptions	Development	HR Manager	DevSecOps & CI/CD Security Procedure · Change Management Procedure
SIM-06	Evaluation and learning	Incidents, continuity, compliance and investigations	Risk Manager	Post-Incident Review & Lessons Learned Template
BCM-03/04	Continuity plans and testing	Incidents, continuity, compliance and investigations	Compliance Lead 4 Feb 2027	Disaster Recovery Plan · BC/DR Testing & Exercise Procedure
COM-02/03	Audit planning and internal audit	Incidents, continuity, compliance and investigations	To assign	C5 Internal Audit Procedure · C5 Audit Findings & Corrective Action Register

HIGH Planned · 9

Move from plan to implementation. Assign an owner and a date, then put the control into operation.

Ref	Requirement	Area	Owner · target	Closes it
OIS-01/02	ISMS and information security policy	Governance, policy and people	Risk Manager	Information Security Management Policy · Information Security Governance Framework
OIS-10	Information security in project management	Governance, policy and people	To assign	Information Security Governance Framework · Management Commitment & Review Procedure

SP-01/02	Policy documentation, communication and review	Governance, policy and people	Operations Manager	Security Policy Framework & Master Policy · Security Policy Review & Communication Procedure +1 more
AM-06/07/10/11	Commissioning, decommissioning and transfer	Assets and physical security	HR Manager	Media Handling & Disposal Procedure · Equipment Security & Maintenance Procedure
OPS-06/07/08/09	Backup and recovery	Operations	HR Manager	Backup & Recovery Procedure · Disaster Recovery Plan
COS-04/05	Cross-network and administration access	Communications, portability and suppliers	To assign	Remote Access & VPN Security Procedure · Network Segmentation & Firewall Management Procedure
DEV-03/06/07/08	Change policy, risk assessment, testing and logging	Development	Compliance Lead	Change Management Procedure · Application Security Testing Procedure
COM-01/04	Legal requirements and security performance	Incidents, continuity, compliance and investigations	HR Manager	Legal & Regulatory Requirements Register · Compliance Management Policy
PSS-11/12	Images and data location	Product security and the attestation	Operations Manager	Container Security & Orchestration Standard · Data Location & Jurisdiction Register +1 more

MEDIUM Partially implemented · 16

Extend the existing approach to the whole scope and apply it consistently, then evidence it.

Ref	Requirement	Area	Owner · target	Closes it
AM-12	Removable media and endpoints	Assets and physical security	To assign	Media Handling & Disposal Procedure · Asset Management Policy
PS-03/04/08	Perimeter, site access and workplace	Assets and physical security	IT Manager 24 Dec 2026	Data Center Physical Access Control Procedure · Visitor Management Procedure +1 more
OPS-04/05	Malware protection	Operations	IT Manager	Malware Protection Procedure
OPS-10/11/12	Logging policy, derived data and retention	Operations	Risk Manager 26 Nov 2026	Logging & Monitoring Procedure

OPS-14/15/16	Log retention, accountability and configuration	Operations	Compliance Lead	Logging & Monitoring Procedure · Clock Synchronization & Log Integrity Standard
OPS-18/25/26	Vulnerability management, scanning and hardening	Operations	Risk Manager	Vulnerability Management Procedure
COS-06/07	Traffic separation and topology documentation	Communications, portability and suppliers	To assign	Client (Tenant) Separation & Isolation Standard · Network Security Policy
PI-01/02/03	Portability, contractual provision and deletion	Communications, portability and suppliers	To assign	Data Portability and Interoperability Policy · Service Migration & Exit Procedure +1 more
SSO-06/08	Supplier exit and functional components	Communications, portability and suppliers	Operations Manager 21 Jan 2027	Subservice Organization Assessment Procedure · Software Bill of Materials (SBOM) Management Procedure
DEV-04/05/13	Secure development competence, design and transparency	Development	To assign	Secure Coding Standards · Software Bill of Materials (SBOM) Management Procedure +1 more
DEV-11/12	Development and test environments	Development	Operations Manager 21 Jan 2027	DevSecOps & CI/CD Security Procedure · Client (Tenant) Separation & Isolation Standard
SIM-04/05	Documentation, reporting and staff duty	Incidents, continuity, compliance and investigations	HR Manager 29 Oct 2026	Incident Severity Classification Matrix · Incident Notification & Escalation Procedure
BCM-01/02	Continuity management and business impact analysis	Incidents, continuity, compliance and investigations	Risk Manager 7 Jan 2027	Business Continuity Management Policy · Business Impact Analysis (BIA) Procedure +1 more
INQ-01/02/03/04	Government investigation requests	Incidents, continuity, compliance and investigations	To assign	Government Investigative Request Policy · Investigative Request Handling Procedure +1 more
ATT-SD	System description	Product security and the attestation	To assign	C5:2026 System Description Template · C5 Boundary Conditions Documentation

ATT-GAP

Readiness and improvement

Product security
and the attestationRisk Manager
21 Jan 2027C5 Gap Analysis
Workbook Template ·
C5 Continual
Improvement
Procedure +1 more

LOW Implemented, not evidenced · 21

Collect and file evidence an auditor can sample. The control is operating; what is missing is the record of it.

Ref	Requirement	Area	Owner · target	Closes it
OIS-03/04	Interfaces, dependencies and segregation of duties	Governance, policy and people	To assign	Cloud Security RACI Matrix · Cloud Security Organization Structure & Roles
OIS-05/06	Threat intelligence and external contacts	Governance, policy and people	To assign	Information Security Risk Management Procedure · Information Security Risk Register
OIS-07/08/09	Risk management policy, assessment and treatment	Governance, policy and people	To assign	Information Security Risk Management Procedure · Information Security Risk Register +1 more
HR-05	Termination and role change	Governance, policy and people	To assign	Role Change & Termination Security Procedure
PS-05/06/07	Environmental threats, supply and monitoring	Assets and physical security	To assign	Environmental Protection & Monitoring Procedure · Equipment Security & Maintenance Procedure
OPS-01/02/03	Capacity management	Operations	To assign	Capacity Management Procedure
OPS-19/20/21/24	Incidents, crashes and customer involvement	Operations	To assign	Incident Detection & Classification Procedure · Incident Notification & Escalation Procedure
OPS-30/31	Separation of datasets	Operations	To assign	Client (Tenant) Separation & Isolation Standard
OPS-34/35	Container management	Operations	To assign	Container Management & Security Procedure · Container Security & Orchestration Standard
IAM-03/04/05	Locking, withdrawal and review	Identity and cryptography	To assign	Access Review & Recertification Procedure · Role Change & Termination Security Procedure

CRY-01/02/03	Cryptography policy, change and review	Identity and cryptography	To assign	Cryptography and Key Management Policy · Cryptographic Algorithm Selection Standard +1 more
CRY-04/05	Transport and at-rest protection	Identity and cryptography	To assign	Encryption Standard (Data at Rest & in Transit)
CRY-06/09/10/11	Key generation, provisioning, storage and archival	Identity and cryptography	To assign	Key Lifecycle Management Procedure · Cryptography and Key Management Policy
CRY-17/18/19	Lifecycle management, external KMS and customer keys	Identity and cryptography	To assign	Key Lifecycle Management Procedure · Cryptography and Key Management Policy
COS-01/02/03	Technical safeguards and connection monitoring	Communications, portability and suppliers	To assign	Network Security Policy · Network Segmentation & Firewall Management Procedure
COS-08	Data transmission policies	Communications, portability and suppliers	To assign	Secure Data Transfer & Communication Standard
SSO-01/02/04	Supplier policy, risk assessment and register	Communications, portability and suppliers	To assign	Procurement & Supply Chain Security Policy · Subservice Organization Assessment Procedure +1 more
SSO-03/05/07	Supplier data processing, monitoring and transparency	Communications, portability and suppliers	To assign	Supplier Security Requirements Specification · Supply Chain Risk Assessment Procedure
SIM-01/02/03	Incident policy, plans and processing	Incidents, continuity, compliance and investigations	To assign	Security Incident Management Policy · Incident Response Procedure +1 more
PSS-02/04	Vulnerability identification and error handling	Product security and the attestation	To assign	Vulnerability Disclosure & Response Procedure · Application Security Testing Procedure
PSS-08/09/10	Roles, authorisation and software defined networking	Product security and the attestation	To assign	Identity and Access Management Policy · Network Security Policy

How it was scored

STATUS WEIGHTS

Status	Weight	Meaning
■ Not started	0.00	No policy, process or activity exists for this requirement.
■ Planned	0.25	Approach agreed and scheduled, but nothing is in place yet.
■ Partially implemented	0.50	In place for part of the scope, or inconsistently applied.
■ Implemented, not evidenced	0.75	Operating as intended, but you could not prove it to an auditor today.
■ Implemented and evidenced	1.00	Operating as intended, with records an auditor can sample.
■ Not applicable	—	A justified exclusion. Removed from the score - record why in your notes.

READINESS LEVELS

1 • Initial (0%+)

Most requirements are not yet in place. Build the foundations before thinking about an audit.

2 • Developing (40%+)

The programme is under way, with material gaps an auditor would find.

3 • Established (65%+)

Most controls operate. Remaining work is closing specific gaps and evidencing what runs.

4 • Audit-ready (85%+)

Controls operate and are evidenced. Ready for an internal audit and a certification body.

WHAT THIS REPORT IS

BASIS OF THIS REPORT AND LIMITATION OF LIABILITY

This report is the output of a self-assessment. The scores, readiness levels, gaps, analysis and recommendations in this report are derived solely from the information entered by the organization, and have not been independently reviewed, verified, tested or audited by Governance Docs. Governance Docs did not conduct an independent assessment of the organization, its controls or its operations.

The accuracy and completeness of the results depend entirely on the accuracy and completeness of the information provided. Governance Docs gives no assurance, certification or audit opinion, and accepts no liability for any inaccuracy, omission or deviation arising from that information, or for any decision taken, or not taken, in reliance on this report.

The report, including any AI-assisted analysis, is provided for guidance and planning only. It does not constitute legal, regulatory or other professional advice, and it does not replace an independent assessment or a certification audit.

A control that is running but cannot be evidenced scores 0.75, not 1.00. Auditors sample records, not intentions. Closing that distance is usually the fastest route to a higher score.

All assessment questions and guidance are original wording by Governance Docs. Clause and control references are used as identifiers; no text from the standard is reproduced. You need your own licensed copy of the standard to implement it.

YOUR WORKBOOK

The Excel workbook that comes with this report follows the same sections and colours. Dashboard: sections 1 and 2, recalculated live. Assessment: every requirement; change a status and every score, chart and level updates. Remediation Plan: section 3, with owners, dates and progress since this report. How it was scored: this page.

Governance Docs · governancedocs.com