

# VinnizzZ: security audit report

Created on 05 November 2025 @ 18:44

VinnizzZ wants to build trust by giving you insight in how it builds software in a secure manner. The report details how software development at VinnizzZ is being monitored and safeguarded from the developer's computer all the way to the infrastructure used for delivery.

This security report has been generated by Aikido Security based on real-time monitoring of VinnizzZ code and infrastructure.

## Aikido benchmark

This percentage gives an indication of your security posture as a company, compared to all other Aikido customers.

Top  
**40%**  
of accounts

Section	Score
Score for code repositories	Top 50%
Score for cloud environment	N/A

## OWASP Top 10

This section details the OWASP risks for which the organization currently has active measures against.

Code	Title	Taken measures
A01:2021	Broken access control	<ul style="list-style-type: none"> <li><span style="color: green;">✓</span> Application is properly configured</li> <li><span style="color: green;">✓</span> Prevents unauthorized access to resources</li> </ul>
A02:2021	Cryptographic failures	<ul style="list-style-type: none"> <li><span style="color: green;">✓</span> Enforces encryption of data at rest</li> <li><span style="color: green;">✓</span> Enforces the use of secure connections</li> <li><span style="color: green;">✓</span> Prevents the exposure of secret keys</li> </ul>
A03:2021	Injection	<ul style="list-style-type: none"> <li><span style="color: green;">✓</span> App scanned for SQL injection attack</li> <li><span style="color: green;">✓</span> Prevents remote code execution</li> <li><span style="color: green;">✓</span> Prevents CSRF attacks</li> <li><span style="color: green;">✓</span> Prevents Cross Site Scripting (XSS)</li> <li><span style="color: green;">✓</span> Prevents command injection</li> </ul>
A04:2021	Insecure design	Monitoring, not fully compliant
A05:2021	Security misconfiguration	<ul style="list-style-type: none"> <li><span style="color: green;">✓</span> Application is properly configured</li> </ul>
A06:2021	Vulnerable and Outdated Components	Monitoring, not fully compliant
A07:2021	Identification and Authentication Failures	<ul style="list-style-type: none"> <li><span style="color: green;">✓</span> Prevents bypassing authorization controls</li> <li><span style="color: green;">✓</span> Prevents improper certificate validation</li> </ul>
A08:2021	Software and Data Integrity Failures	<ul style="list-style-type: none"> <li><span style="color: green;">✓</span> Takes measures to ensure proper deserialization</li> </ul>
A09:2021	Security Logging and Monitoring Failures	Monitoring, not fully compliant
A10:2021	Server-Side Request Forgery	<ul style="list-style-type: none"> <li><span style="color: green;">✓</span> App scanned for SSRF attack opportunities</li> </ul>

## ISO 27001:2022 compliance

A brief overview of the ISO 27001 requirements and any measures taken for these.

Title	Taken measures
A.8.2 - Privileged access rights	Monitoring, not fully compliant
A.8.3 - Information access restriction	Monitoring, not fully compliant
A.8.5 - Secure authentication	Monitoring, not fully compliant
A.8.6 - Capacity management	Monitoring, not fully compliant
A.8.7 - Protection against malware	<span data-bbox="638 709 682 745"></span> Prevents unwanted write operations to filesystems
A.8.8 - Management of technical vulnerabilities	Monitoring, not fully compliant
A.8.12 - Data leakage prevention	<span data-bbox="638 931 682 967"></span> Prevents remote code execution <span data-bbox="638 979 682 1015"></span> Has measures against SQL injection attacks <span data-bbox="638 1028 682 1064"></span> Prevents XSS attacks
A.8.13 - Backups	Monitoring, not fully compliant
A.8.15 - Logging	Monitoring, not fully compliant
A.8.18 - Use of privileged utility programs	Monitoring, not fully compliant
A.8.20 - Network security	Monitoring, not fully compliant
A.8.31 - Separation of development, test and production environments	Monitoring, not fully compliant
A.8.24 - Use of cryptography	<span data-bbox="638 1672 682 1708"></span> Uses secure cookies <span data-bbox="638 1721 682 1757"></span> Uses up-to-date cryptographic libraries
A.8.9 - Configuration management	Monitoring, not fully compliant
A.8.16 - Monitoring activities	Monitoring, not fully compliant

Title	Taken measures
A.8.25 - Secure development lifecycle	 Has connected a code repository
A.8.28 - Secure coding	Monitoring, not fully compliant
A.8.32 - Change management	Monitoring, not fully compliant
A.5.15 - Access control	Monitoring, not fully compliant
A.5.16 - Identity management	Monitoring, not fully compliant
A.5.28 - Collection of evidence	Monitoring, not fully compliant
A.5.33 - Protection of records	Monitoring, not fully compliant

## Esquema Nacional de Seguridad (ENS) compliance

A brief overview of the ENS requirements and any measures taken for these.

Título	Medidas Tomadas
[op.pl.4] Planificación\Dimensionamiento - gestión de la capacidad	No se han tomado medidas activas
[op.acc.1] Control de accesos\Identificación	No se han tomado medidas activas
[op.acc.2] Control de accesos\Requisitos de acceso a la información	No se han tomado medidas activas
[op.acc.2] Control de accesos\Requisitos de acceso - programas utilitarios privilegiados.	No se han tomado medidas activas
[op.acc.2] Control de accesos\Requisitos de acceso - acceso a la información - mínimo privilegio	No se han tomado medidas activas
[op.acc.4] Control de acceso\Proceso de gestión de derechos de acceso privilegiados	No se han tomado medidas activas
[op.acc.6] Control de accesos\Mecanismo de autenticación (usuarios de la organización)	No se han tomado medidas activas
[op.exp.3] Explotación\Gestión de la configuración	No se han tomado medidas activas
[op.exp.4] Explotación\Mantenimiento y actualizaciones de seguridad - Gestión de vulnerabilidades técnicas	No se han tomado medidas activas
[op.exp.5] Explotación\Gestión de cambios en sistemas y aplicaciones	No se han tomado medidas activas
[op.exp.6] Explotación\Protección frente a código dañino	 Prevención de operaciones de escritura no deseadas en sistemas de archivos

Título	Medidas Tomadas
[op.exp.8] Explotación\Registro de la actividad y eventos de seguridad	No se han tomado medidas activas
[op.exp.8] Explotación\Registro de la actividad y logs de actividad	No se han tomado medidas activas
[op.exp.9] Explotación\Registro de la gestión de incidencias - recolección de evidencia	No se han tomado medidas activas
[op.mon.3] Monitorización del sistema\Vigilancia - monitoreo de actividades y eventos de seguridad	No se han tomado medidas activas
[mp.com.1] Protección de las comunicaciones\Perímetro seguro - medidas de seguridad para proteger la red	No se han tomado medidas activas
[mp.si.2] Protección de los soportes de información\Criptografía	<ul style="list-style-type: none"> <li> Uso seguro de cookies</li> <li> Uso de librerías criptográficas actualizadas</li> </ul>
[mp.sw.1] Protección de las aplicaciones informáticas\Desarrollo de aplicaciones - separación de los entornos	No se han tomado medidas activas
[mp.sw.1] Protección de las aplicaciones informáticas\Ciclo de vida de desarrollo seguro de aplicaciones	<ul style="list-style-type: none"> <li> Ha conectado un repositorio de código</li> </ul>
[mp.info.6] Protección de la información\Copias de seguridad	No se han tomado medidas activas
[mp.s.1] Protección de los servicios\correo electrónico - medidas prevenir la fuga de datos	<ul style="list-style-type: none"> <li> Prevención de ejecución remota de código</li> <li> Se tienen medidas para proteger contra ataques de inyección de SQL</li> <li> Prevención contra ataques de Cross-Site Scripting (XSS)</li> </ul>

## SOC2 compliance

A brief overview of the SOC2 requirements and any measures taken for these.

Title	Taken measures
CC3.3: Consider the potential for fraud	Monitoring, not fully compliant
CC3.2: Estimate Significance of Risks Identified	<ul style="list-style-type: none"> <li><span data-bbox="644 466 693 502">✓</span> Does not have any severe surface monitoring issues</li> <li><span data-bbox="644 508 693 544">✓</span> Does not have any severe open source dependency issues</li> <li><span data-bbox="644 551 693 587">✓</span> Configured monitoring for code repositories</li> <li><span data-bbox="644 593 693 629">✓</span> Configured monitoring for container images</li> </ul>
CC5.2: The entity selects and develops general control activities over technology to support the achievement of objectives	<ul style="list-style-type: none"> <li><span data-bbox="644 741 693 777">✓</span> Does not have any severe infrastructure as code issues</li> </ul>
CC6.1: Restricts logical access	<ul style="list-style-type: none"> <li><span data-bbox="644 889 693 925">✓</span> Has measures against SQL injection attacks</li> <li><span data-bbox="644 931 693 967">✓</span> Is protected against SSRF attacks</li> <li><span data-bbox="644 973 693 1009">✓</span> Is protected against command injections attacks</li> <li><span data-bbox="644 1015 693 1051">✓</span> Prevents XSS attacks</li> </ul>
CC6.1: Consider network segmentation	Monitoring, not fully compliant
CC6.1: Restrict access to information assets	Monitoring, not fully compliant
CC6.1: Manages credentials for infrastructure and software	Monitoring, not fully compliant
CC6.1: Use encryption to protect data	<ul style="list-style-type: none"> <li><span data-bbox="644 1529 693 1564">✓</span> Enforces encryption of data in transit</li> <li><span data-bbox="644 1571 693 1607">✓</span> Uses up to date cryptography libraries</li> </ul>
CC6.6: Restrict Access	Monitoring, not fully compliant
CC6.6: Require additional authentication or credentials	Monitoring, not fully compliant
CC6.6: Implement boundary protection system	Monitoring, not fully compliant

Title	Taken measures
CC6.7: Use encryption technologies or secure communication channels to protect data	 Uses up to date cryptography libraries
CC6.8: Restrict application and software installation	 Protects unauthorized runtime access  Prevents container orchestration takeover
CC6.8: Detect unauthorized changes to software and configuration parameters	Monitoring, not fully compliant
CC6.8 Use anti-virus and anti-malware software	 Aikido Malware Scanner is enabled
CC7.1: Monitor infrastructure and software	 Connected code repositories
CC7.1: Implement change detection mechanism	Monitoring, not fully compliant
CC7.1: Detect unknown or unauthorized components	 Does not have risky licenses
CC7.1: Conduct vulnerability scans	 Connected code repositories
CC7.1: Implement filters to analyze anomalies	 Connected code repositories
CC7.1: Restores the affected environments	 Has no critical open source dependency issues
CC8.1: Protect confidential information	Monitoring, not fully compliant
CC8.1: Track system changes	Monitoring, not fully compliant
CC10.3: Tests integrity and completeness of backup data	Monitoring, not fully compliant

## CIS Controls compliance

A brief overview of the CIS controls and any measures taken for these.

Title	Taken measures
2.2 Ensure Authorized Software is Currently Supported	Monitoring, not fully compliant
3.3 Configure Data Access Control Lists	Monitoring, not fully compliant
3.4 Enforce Data Retention	 Enabled security logging for cloud instances
3.10 Encrypt Sensitive Data in Transit	 Enforces encryption of data in transit
3.11 Encrypt Sensitive Data at Rest	 Encrypts data at rest
3.14 Log Sensitive Data Access	 Enabled security logging for cloud instances
4.4 Implement and Manage a Firewall on Servers	 Prevents unauthorized public access to file storage
4.6 Securely Manage Enterprise Assets and Software	 Enforces latest TLS version  Enforces encryption of data in transit
4.9 Configure Trusted DNS Servers on Enterprise Assets	 Uses DNSSEC extensions
5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts	Monitoring, not fully compliant
6.5 Require MFA for Administrative Access	Monitoring, not fully compliant
6.4 Require MFA for Remote Network Access	Monitoring, not fully compliant
7.1 Establish and Maintain a Vulnerability Management Process	Monitoring, not fully compliant
8.2 Collect Audit Logs	 Enabled security logging for cloud instances

Title	Taken measures
10.1 Deploy and Maintain Anti-Malware Software	<ul style="list-style-type: none"><li data-bbox="638 202 882 234"> No malware issues</li><li data-bbox="638 255 1176 287"> Prevents unwanted write operations to filesystems</li></ul>
11.2 Perform Automated Backups	<ul style="list-style-type: none"><li data-bbox="638 356 1078 388"> Has backups for stateful cloud resources</li></ul>
12.3 Securely Manage Network Infrastructure	<ul style="list-style-type: none"><li data-bbox="638 483 1299 515"> Prevents unauthorized public access to networks and instances</li></ul>
12.6 Use of Secure Network Management and Communication Protocols	<ul style="list-style-type: none"><li data-bbox="638 599 1299 631"> Prevents unauthorized public access to networks and instances</li><li data-bbox="638 652 1054 684"> Enforces encryption of data in transit</li><li data-bbox="638 705 1070 737"> Uses secure communications protocols</li></ul>
13.6 Collect Network Traffic Flow Logs	<ul style="list-style-type: none"><li data-bbox="638 800 1119 832"> Enabled security logging for cloud instances</li></ul>
16.2 Establish and Maintain a Process to Accept and Address Software Vulnerabilities	<p data-bbox="638 948 980 979">Monitoring, not fully compliant</p>
16.5 Use Up-to-Date and Trusted Third-Party Software Components	<ul style="list-style-type: none"><li data-bbox="638 1096 1119 1127"> No risky licenses in 3rd party dependencies</li></ul>
16.8 Separate Production and Non-Production Systems	<p data-bbox="638 1224 980 1256">Monitoring, not fully compliant</p>
16.12 Implement Code-Level Security Checks	<p data-bbox="638 1351 980 1383">Monitoring, not fully compliant</p>

## CIS AWS benchmark compliance

A brief overview of the CIS AWS benchmark and any measures taken for these.

Title	Taken measures
2.3 No root user account access key exists	Monitoring, not fully compliant
2.4 MFA is enabled for the root user account	Monitoring, not fully compliant
2.7 IAM password policy requires minimum length of 14 or greater	Monitoring, not fully compliant
2.8 IAM password policy prevents password reuse	Monitoring, not fully compliant
2.9 MFA is enabled for all IAM users with console access	Monitoring, not fully compliant
2.11 Credentials unused for 45 days are disabled	Monitoring, not fully compliant
2.12 There is only one active access key per IAM user	Monitoring, not fully compliant
2.13 Access keys should be rotated every 90 days	Monitoring, not fully compliant
2.14 IAM users receive permissions only through groups	Monitoring, not fully compliant
2.15 IAM policies allowing full administrative privileges are not attached	Monitoring, not fully compliant
2.16 Support role has been created to manage incidents with AWS Support	Monitoring, not fully compliant
2.17 IAM instance roles are used for AS resources access from instances	Monitoring, not fully compliant
2.18 IAM SSL/TLS certificates are not expired	Monitoring, not fully compliant

Title	Taken measures
2.19 IAM External Access Analyzer is enabled for all regions	Monitoring, not fully compliant
2.21 Access to CloudShell is restricted	Monitoring, not fully compliant
3.1.1 S3 Bucket Policy denies HTTP requests	Monitoring, not fully compliant
3.1.2 MFA delete is enabled on S3 buckets	Monitoring, not fully compliant
3.1.4 S3 is configured with 'Block Public Access' enabled	Monitoring, not fully compliant
3.2.1 RDS data is encrypted at rest	Monitoring, not fully compliant
3.2.2 'Auto Minor Version Upgrade' is enabled for RDS instances	Monitoring, not fully compliant
3.2.3 RDS instances are not publicly accessible	Monitoring, not fully compliant
3.2.4 RDS clusters use Multi-AZ for enhanced availability	Monitoring, not fully compliant
3.3.1 EFS file systems are encrypted at rest	Monitoring, not fully compliant
4.1 Cloudtrail enabled in all regions	Monitoring, not fully compliant
4.2 Cloudtrail log validation is enabled	Monitoring, not fully compliant
4.3 AWS Config enabled in all regions	Monitoring, not fully compliant
4.4 Cloudtrail logs have server access logging enabled	Monitoring, not fully compliant
4.5 Cloudtrail logs are encrypted at rest using a CMK	Monitoring, not fully compliant

Title	Taken measures
4.6 Symmetric CMKs rotation is enabled	Monitoring, not fully compliant
4.7 VPC flow logging is enabled in all regions	Monitoring, not fully compliant
4.8 Ensure object-level logging for S3 write events is enabled	Monitoring, not fully compliant
4.9 Ensure object level logging for S3 read events is enabled	Monitoring, not fully compliant
6.1.1 EBS volumes are encrypted by default	Monitoring, not fully compliant
6.1.2 CIFS access is restricted to trusted networks	Monitoring, not fully compliant
6.3 Security groups do not allow ingress from 0.0.0.0/0 on server admin ports	Monitoring, not fully compliant
6.4 Security groups do not allow ingress from ::/0 on server admin ports	Monitoring, not fully compliant
6.5 Default security groups restricts all traffic	Monitoring, not fully compliant
6.7 EC2 metadata service only allows IMDSv2	Monitoring, not fully compliant

## NIS2 compliance

A brief overview of the NIS2 directive and any measures taken for these.

Title	Taken measures
Policies on risk analysis and information system security	 Configured monitoring for code repositories
Incident handling	Monitoring, not fully compliant
Business continuity	Monitoring, not fully compliant
Supply chain security	Monitoring, not fully compliant
Security in network and information systems acquisition	Monitoring, not fully compliant
Policies and procedures regarding the use of cryptography	 Uses secure cookies  Uses up-to-date cryptographic libraries
Access control policies and asset management	Monitoring, not fully compliant
The use of multi-factor authentication	Monitoring, not fully compliant

## NIST 800-53 compliance

A brief overview of the NIST directive and any measures taken for these.

Title	Taken measures
1.2.4 Account Management   Disable Accounts	Monitoring, not fully compliant
1.2.5 Account Management   Automated Audit Actions	Monitoring, not fully compliant
1.2.8 Account Management   Privileged User Accounts	Monitoring, not fully compliant
1.2.13 Account Management   Account Monitoring for Atypical Usage	Monitoring, not fully compliant
1.3.8 Access Enforcement   Role-based access control	Monitoring, not fully compliant
1.4.22 Information Flow Enforcement   Physical or Logical Separation of Information Flows	<ul style="list-style-type: none"> <li> Enforces safe SSL protocol usage</li> <li> Prevents abuse of cookies</li> <li> Uses up to date cryptography libraries</li> </ul>
1.6.2 Least Privilege   Authorize Access to Security Functions	<ul style="list-style-type: none"> <li> Enforces safe SSL protocol usage</li> </ul>
1.17.2 Remote Access   Monitoring and Control	Monitoring, not fully compliant
1.17.6 Remote Access   Monitoring for Unauthorized Connections	Monitoring, not fully compliant
1.23.1 Data Mining Protection	<ul style="list-style-type: none"> <li> Restrict excessive or unauthorized data mining queries.</li> </ul>
3.6.2 Audit Record Review, Analysis, and Reporting   Automated Process Integration	<ul style="list-style-type: none"> <li> Limit access to sensitive data based on user roles and responsibilities.</li> </ul>
3.9.4 Protection of Audit Information   Cryptographic Protection	<ul style="list-style-type: none"> <li> Enforces safe SSL protocol usage</li> <li> Prevents abuse of cookies</li> </ul>

Title	Taken measures
3.9.5 Protection of Audit Information   Access by Subset of Privileged Users	Monitoring, not fully compliant
3.11.2 Audit Record Retention   Long-term Retrieval Capability	Monitoring, not fully compliant
3.12.2 Audit Record Generation   System-wide and Time-correlated Audit Trail	Monitoring, not fully compliant
4.7.7 Continuous Monitoring   Automation Support for Monitoring	Monitoring, not fully compliant
5.5.2 Access Restrictions for Change   Automated Access Enforcement and Audit Records	 Enforces safe SSL protocol usage
5.7.9 Least Functionality   Binary or Machine Executable Code	Monitoring, not fully compliant
6.9.6 System Backup   Transfer to Alternate Storage Site	Monitoring, not fully compliant
7.2.2 Identification and Authentication (organizational Users)   Multi-factor Authentication to Privileged Accounts	Monitoring, not fully compliant
7.2.3 Identification and Authentication (organizational Users)   Multi-factor Authentication to Non-privileged Accounts	Monitoring, not fully compliant
7.5.2 Authenticator Management   Password-based Authentication	Monitoring, not fully compliant
7.5.7 Authenticator Management   Protection of Authenticators	Monitoring, not fully compliant
7.10.1 Adaptive Authentication	Monitoring, not fully compliant

Title	Taken measures
8.5.2 Incident Monitoring   Automated Tracking, Data Collection, and Analysis	Monitoring, not fully compliant
13.12.1 Insider Threat Program	 Enforces safe SSL protocol usage
16.10.1 Threat Hunting	Monitoring, not fully compliant
17.3.2 System Development Life Cycle   Manage Preproduction Environment	 Enforces safe SSL protocol usage  Prevents abuse of cookies  Uses up to date cryptography libraries
18.5.2 Denial-of-service Protection   Restrict Ability to Attack Other Systems	Monitoring, not fully compliant
18.5.3 Denial-of-service Protection   Capacity, Bandwidth, and Redundancy	 Enforces safe SSL protocol usage
18.7.6 Boundary Protection   Deny by Default Allow by Exception	 Enforces safe SSL protocol usage  Prevents abuse of cookies
18.7.8 Boundary Protection   Split Tunneling for Remote Devices	Monitoring, not fully compliant
18.7.11 Boundary Protection   Prevent Exfiltration	 Restrict excessive or unauthorized data mining queries.  Enforces safe SSL protocol usage
18.7.16 Boundary Protection   Networked Privileged Accesses	Monitoring, not fully compliant
18.12.2 Cryptographic Key Establishment and Management   Availability	 Enforces safe SSL protocol usage
18.16.3 Transmission of Security and Privacy Attributes   Anti-spoofing Mechanisms	Monitoring, not fully compliant

Title	Taken measures
18.16.4 Transmission of Security and Privacy Attributes   Cryptographic Binding	 Enforces safe SSL protocol usage
18.20.3 Secure Name/address Resolution Service (authoritative Source)   Data Origin and Integrity	Monitoring, not fully compliant
18.21.2 Secure Name/address Resolution Service (recursive or Caching Resolver)   Data Origin and Integrity	Monitoring, not fully compliant
18.22.1 Architecture and Provisioning for Name/address Resolution Service	Monitoring, not fully compliant
18.23.4 Session Authenticity   Unique System-generated Session Identifiers	Monitoring, not fully compliant
18.24.1 Fail in Known State	Monitoring, not fully compliant
18.28.2 Protection of Information at Rest   Cryptographic Protection	 Enforces safe SSL protocol usage  Prevents abuse of cookies
18.34.2 Non-modifiable Executable Programs   No Writable Storage	Monitoring, not fully compliant

## PCI compliance

A brief overview of the PCI Data Security Standards and any measures taken for these.

Title	Taken measures
1.2 Network security controls (NSCs) are configured and maintained.	Monitoring, not fully compliant
1.3 Network access to and from the cardholder data environment is restricted.	<ul style="list-style-type: none"><li>✓ Enforces connections to use the latest SSL version</li><li>✓ Prevents abuse of cookies</li></ul>
3.4 Access to displays of full PAN and ability to copy cardholder data are restricted.	Monitoring, not fully compliant
3.5 Primary account number (PAN) is secured wherever it is stored.	Monitoring, not fully compliant
4.2 PAN is protected with strong cryptography during transmission.	<ul style="list-style-type: none"><li>✓ Enforces connections to use the latest SSL version</li><li>✓ Prevents abuse of cookies</li><li>✓ Enforces encryption of data in transit</li></ul>
5.2 Malicious software (malware) is prevented, or detected and addressed.	<ul style="list-style-type: none"><li>✓ No malware issues</li></ul>
6.4 Public-facing web applications are protected against attacks.	<ul style="list-style-type: none"><li>✓ App scanned for SQL injection attack</li><li>✓ Prevents CSRF attacks</li><li>✓ Prevents Cross Site Scripting (XSS)</li></ul>
7.2.2 Access is assigned to users, including privileged users.	Monitoring, not fully compliant
7.2.5 All application and system accounts and related access privileges are assigned and managed.	Monitoring, not fully compliant
7.3 Access to system components and data is managed via an access control system(s).	Monitoring, not fully compliant
8.4 Multi-factor authentication (MFA) is implemented to secure access into	Monitoring, not fully compliant

Title	Taken measures
the CDE.	
10.2.1 Audit logs are enabled and active for all system components and cardholder data.	Monitoring, not fully compliant
10.3.3 Audit log files are promptly backed up to a secure, central, internal log server(s).	Monitoring, not fully compliant
10.7.2 Failures of critical security control systems are detected, alerted, and addressed promptly.	Monitoring, not fully compliant
11.3.2 External vulnerability scans are performed.	Monitoring, not fully compliant
11.3.1 Internal vulnerability scans are performed.	<ul style="list-style-type: none"><li><input checked="" type="checkbox"/> Configured monitoring for code repositories</li><li><input checked="" type="checkbox"/> Configured monitoring for container images</li></ul>

## HIPAA compliance

A brief overview of the HIPAA Compliance Checklist and any measures taken for these.

Title	Taken measures
1.3.1 Security Standards: General Requirements	<ul style="list-style-type: none"><li><span style="color: green;">✓</span> Enforces safe SSL protocol usage</li><li><span style="color: green;">✓</span> Prevents abuse of cookies</li><li><span style="color: green;">✓</span> Uses up to date cryptography libraries</li></ul>
1.4.1 Administrative Safeguards: Security management process	Monitoring, not fully compliant
1.4.4 Administrative Safeguards: Information access management	Monitoring, not fully compliant
1.4.5 Administrative Safeguards: Security awareness and training	Monitoring, not fully compliant
1.4.7 Administrative Safeguards: Contingency plan	Monitoring, not fully compliant
1.6.1 Technical Safeguards: Access control	Monitoring, not fully compliant
1.6.2 Technical Safeguards: Audit controls	Monitoring, not fully compliant
1.6.3 Technical Safeguards: Integrity	<ul style="list-style-type: none"><li><span style="color: green;">✓</span> Uses up to date cryptography libraries</li></ul>
1.6.4 Technical Safeguards: Person or entity authentication	Monitoring, not fully compliant
1.6.5 Technical Safeguards: Transmission Security	<ul style="list-style-type: none"><li><span style="color: green;">✓</span> Uses up to date cryptography libraries</li><li><span style="color: green;">✓</span> Enforces safe SSL protocol usage</li><li><span style="color: green;">✓</span> Prevents abuse of cookies</li></ul>

## HITRUST LVL3 Compliance

A brief overview of the HITRUST LVL3 framework and any measures taken for these.

Title	Taken measures
2.3 Privilege Management	Monitoring, not fully compliant
2.4 User Password Management	 Prevents Exposed Secrets
2.9 User Authentication for External Connections	Monitoring, not fully compliant
2.10 Equipment Identification in Networks	Monitoring, not fully compliant
2.11 Remote Diagnostic and Configuration Port Protection	Monitoring, not fully compliant
2.12 Segregation in Networks	Monitoring, not fully compliant
2.13 Network Connection Control	 Use of Cryptography: Enforces SSL
2.14 Networking Routing Control	Monitoring, not fully compliant
2.16 Secure Log-on Procedures	 Use of Cryptography: Secure Cookies  Use of Cryptography: Enforces SSL
2.17 User Identification and Authentication	Monitoring, not fully compliant
2.18 Password Management System	 Prevents Exposed Secrets
2.22 Information Access restriction	 Prevents SQL Injection Attacks  Prevents CSRF Attacks  Prevents Cross-Site Scripting Attacks
2.23 Sensitive System Isolation	Monitoring, not fully compliant

Title	Taken measures
7.3 Protection of Organizational Records	<ul style="list-style-type: none"><li><span data-bbox="638 202 687 255">✓</span> Prevents Exposed Secrets</li><li><span data-bbox="638 255 687 308">✓</span> Prevents SQL Injection Attacks</li><li><span data-bbox="638 308 687 361">✓</span> Prevent Root Access</li></ul>
7.4 Data Protection and Privacy of Covered Information	<ul style="list-style-type: none"><li><span data-bbox="638 407 687 460">✓</span> Use of Cryptography: Enforces SSL</li><li><span data-bbox="638 460 687 513">✓</span> Use of Cryptography: Secure Cookies</li><li><span data-bbox="638 513 687 566">✓</span> Prevents SQL Injection Attacks</li><li><span data-bbox="638 566 687 618">✓</span> Prevent Root Access</li></ul>
7.6 Regulation of Cryptographic Controls	<ul style="list-style-type: none"><li><span data-bbox="638 639 687 692">✓</span> Use of Cryptography: Enforces SSL</li><li><span data-bbox="638 692 687 745">✓</span> Use of Cryptography: Secure Cookies</li><li><span data-bbox="638 745 687 798">✓</span> Use of Cryptography Libraries</li></ul>
10.12 Back-up	Monitoring, not fully compliant
10.13 Network Controls	Monitoring, not fully compliant
10.17 Information Handling Procedures	<ul style="list-style-type: none"><li><span data-bbox="638 1011 687 1064">✓</span> Use of Cryptography: Enforces SSL</li><li><span data-bbox="638 1064 687 1117">✓</span> Use of Cryptography: Secure Cookies</li><li><span data-bbox="638 1117 687 1170">✓</span> Use of Cryptography Libraries</li></ul>
10.18 Security of System Documentation	<ul style="list-style-type: none"><li><span data-bbox="638 1201 687 1254">✓</span> Configured Monitoring for Code Repositories</li></ul>
10.19 Information Exchange Policies and Procedures	<ul style="list-style-type: none"><li><span data-bbox="638 1322 687 1374">✓</span> Use of Cryptography: Enforces SSL</li></ul>
10.26 Publicly Available Information	Monitoring, not fully compliant
10.27 Audit Logging	Monitoring, not fully compliant
11.2 Input Data Validation	<ul style="list-style-type: none"><li><span data-bbox="638 1630 687 1683">✓</span> Prevents SQL Injection Attacks</li><li><span data-bbox="638 1683 687 1736">✓</span> Cross-Site Scripting (XSS) Prevention</li><li><span data-bbox="638 1736 687 1788">✓</span> Server-Side Request Forgery (SSRF) Prevention</li></ul>
11.6 Policy on the Use of Cryptographic Controls	<ul style="list-style-type: none"><li><span data-bbox="638 1841 687 1894">✓</span> Use of Cryptography: Enforces SSL</li><li><span data-bbox="638 1894 687 1947">✓</span> Use of Cryptography Libraries</li></ul>

Title	Taken measures
11.7 Key Management	 Prevents Exposed Secrets
11.8 Control of Operational Software	 No Open End-of-Life (EOL) Issues  No Open DAST Issues  No Open OSS Security Issues  Configured Monitoring for Code Repositories  Configured Monitoring for Containers
11.12 Outsourced Software Development	 No Open SCM Security Issues
11.13 Control of Technical Vulnerabilities	Monitoring, not fully compliant

## GDPR compliance

A brief overview of GDPR rules and any measures taken for these.

Title	Taken measures
2.1 Principles Relating to Processing of Personal Data	<ul style="list-style-type: none"><li>✓ Use of Cryptography: Enforces SSL</li><li>✓ Use of Cryptography: Secure Cookies</li><li>✓ Use of Cryptography Libraries</li></ul>
4.2 Data Protection by Design	Monitoring, not fully compliant
4.5 Processor	<ul style="list-style-type: none"><li>✓ Use of Cryptography: Enforces SSL</li><li>✓ Use of Cryptography: Secure Cookies</li><li>✓ Use of Cryptography Libraries</li></ul>
4.7 Records of Processing Activities	Monitoring, not fully compliant
4.9 Security of Processing	<ul style="list-style-type: none"><li>✓ Use of Cryptography: Enforces SSL</li><li>✓ Use of Cryptography: Secure Cookies</li><li>✓ Use of Cryptography Libraries</li></ul>

## DORA compliance

A brief overview of the DORA Compliance Checklist and any measures taken for these.

Title	Taken measures
Article 7, ICT Risk Management: Systems, Protocols, and Tools	Monitoring, not fully compliant
Article 8, ICT Risk Management: Identification	 Has connected code repositories
Article 9, ICT Risk Management: Protection and prevention	 Use of Cryptography: Enforces SSL  Use of Cryptography: Secure Cookies
Article 10, ICT Risk Management: Detection	Monitoring, not fully compliant
Article 11, ICT Risk Management: Response and Recovery	Monitoring, not fully compliant
Article 12, ICT Risk Management: Backup	Monitoring, not fully compliant
Article 15, Harmonization With Other Regulations	Monitoring, not fully compliant
Article 17, Incident Management Process	Monitoring, not fully compliant
Article 18, Classification of Incidents and Cyber Threats	 Configured monitoring for code repositories  Configured monitoring for container images

## Scan history report

This section details all company assets that are being monitored and how often scans are performed.

Kind	Frequency	Last occurrence
Open-source dependencies:	Daily	2025-11-05
OSS licenses: 0 monitored for compliance	Weekly	2025-11-05
Static app security testing: 1 repository monitored	Daily	2025-11-05
Infrastructure as code: monitored for misconfigurations	Daily	2025-11-05
Exposed secrets: history of 1 repository scanned	Daily	2025-11-05

## Issue insights over the past 3 months

The table below gives an overview of new findings in a 3 month rolling window. A triaged finding is one that has been either been solved, ignored after analysis or planned in a task management system for resolution.

Issue kind	New	False positives	Handled
Open-source Dependencies	0	0	0
Container Images	0	0	0
Cloud Configurations	0	0	0
Virtual Machines	0	0	0
Secrets in source code history	2	1	0
DAST/Surface Monitoring	0	0	0
SAST/Static App Security Testing	2	1	0
Infrastructure As Code	0	0	0
Mobile	0	0	0
End-of-life Runtimes	0	0	0
Access Controls	0	0	0
Licenses	0	0	0
Malware Issues	0	0	0
AI Pentest Issues	0	0	0

## Open Issues Snapshot

The table below gives an overview of all findings that were open Nov 5th 2025.

Issue type	Critical	High	Medium	Low
Open-source Dependencies	0	0	0	0
Container Images	0	0	0	0
Cloud Configurations	0	0	0	0
Virtual Machines	0	0	0	0
Secrets in source code history	0	0	1	0
DAST/Surface Monitoring	0	0	0	0
SAST/Static App Security Testing	1	0	0	0
Infrastructure As Code	0	0	0	0
Mobile	0	0	0	0
End-of-life Runtimes	0	0	0	0
Access Controls	0	0	0	0
Licenses	0	0	0	0
Malware Issues	0	0	0	0
AI Pentest Issues	0	0	0	0