EN

Security Statement
CERRIX GRC PLATFORM

This document gives an overview of the implemented security measures relevant to the SaaS services of CERRIX.

Restricted

Document properties

Title:	Security Statement
Subject:	CERRIX SaaS Platform security measures
Author(s):	R.M. van der Horst
Current version:	2.2
Date:	3-6-2025
Audience:	Prospects and Clients

Version history

Version	Date	Author	Changes
1.0	07-03-2024	R.M. van der Horst	Initial document set-up
2.0	11-12-2024	R.M. van der Horst	Improved description of Security measures. Added description of critical third-parties.
2.1	18-12-2024	R.M. van der Horst	Added a description of our hosting environment. Textual improvements Added a Risk Management chapter Added an awareness training chapter
2.2	3-6-2025	R.M. van der Horst	Added a description of our backup & restore policy & practices.

CLASSIFICATION: CERRIX RESTRICTED

This document has been classified as CERRIX Restricted. The information contained within this document and any accompanying appendices is exclusively meant for the addressees that this document is directly distributed to. Further distribution of this document, its contents and attachments to any party or person other is prohibited unless explicit prior written permission is extended by CERRIX B.V. This document, its contents, attachments, and attachments are subject to a Non-Disclosure Agreement.

If you received this document in error and/or you do not have explicit permission in the sense stated above, CERRIX B.V. requests you close this document immediately and destroy it and any copies made.

Nothing in this document may be duplicated, in part or in its entirety, and/or made public by any means without prior written authorization of CERRIX B.V. No rights can be deduced from the content of this document.

Table of contents

Document properties **1**

Version history 1

1. Introduction **5**

1.1 ISO 27001 5

2. Information Security Principles **6**

3. Information Security Governance **7**

3.1 Policies 7

3.2 Procedures 7

4. Risk Management **8**

5. Cybersecurity **9**

5.1 Endpoint Security 9

5.2 Physical Security 9

5.3 Identity & Access Management 9

5.4 Hosting environment 9

5.5 Application Security 10

5.6 Security monitoring 10

6. Secure Software Development **11**

6.1 Security Requirements 11

6.2 Secure Design 11

6.3 Secure Development 11

6.4 Secure Testing 11

6.5 Secure Deployment 11

6.6 Asset Management 11

7. Business Continuity **12**

7.1 Business Continuity Plan 12

7.2 Business Continuity Scenarios 12

7.3 Business Continuity Testing 12

7.4 Backup & Restore 12

8. Awareness & Training 13
8.1 Awareness training 13
8.2 Training 13
8.2 Phishing Simulations 13
9. Third-Party Management 14
9.1. Supplier onboarding 14
9.2 Supplier evaluation 14
9.3 Supplier classification 15

1. Introduction

At CERRIX, we prioritize the security and privacy of our customers' data above all else. We understand the importance of safeguarding sensitive information and maintaining the trust of our clients. Therefore, we have implemented comprehensive security measures to protect against unauthorized access, data breaches, and other potential threats. The measures we have taken are described on a high level in this document.

1.1 ISO 27001

ISO 27001 is an international standard for managing information security. It provides a framework for establishing, implementing, maintaining, and continuously improving an Information Security Management System (ISMS). The standard helps organizations protect sensitive data by addressing risks related to information security, including data breaches, cyber-attacks, and unauthorized access.

Certification to ISO 27001 demonstrates that an organization follows best practices for managing information security.

CERRIX is ISO 27001: 2022 certified by BSI since August 2024.

2. Information Security Principles

To ensure safe and reliable SaaS-services for all its clients and to safeguard the information of clients, employees, and business partners, CERRIX B.V. recognizes the following fundamental principles, meant to fulfil the general and continuously improving aim of its security:

1. Security by design

To prevent security breaches and to safeguard the information of clients, employees, and business partners, CERRIX B.V. applies the security-by-design principle during development and deployment of new software and during the design and implementation of technical and physical infrastructure.

2. Zero trust

To enhance security, mitigate cyber risk and protect the information of clients, employees, and business partners, CERRIX B.V. applies the zero-trust principle regarding users, devices, network traffic, applications, and data.

3. Defense in depth

To establish and maintain a robust information security management system (ISMS), CERRIX B.V. applies the defense-in-depth principle that leverages security measures across multiple layers from policies & procedures up to endpoint devices.

4. Simplicity & proportionality

To prevent the needs and costs for additional security measures due to complex- organizational designs, processes, or architecture, CERRIX B.V. applies this principle with an aim for both operational and security efficiency.

3. Information Security Governance

This chapter describes the way in which information security is organized and steered on within CERRIX.

3.1 Policies

Relevant security policies include, but are not limited to:

- **Physical Security Policies**
- **Employee Security Policies**
- **Access Control Policies**
- **Data Security Policies**

3.2 Procedures

Relevant security procedures include, but are not limited to:

- **Change Management**
- **Incident Management**
- **Improvement Management**
- **Information Security Risk Management**
- **Back-up & Restore**
- **Disaster Recovery Management**
- **Supplier Management**

4. Risk Management

CERRIX prioritizes the security and integrity of your data through a comprehensive and proactive risk management process. Our approach is designed to identify, assess, and mitigate potential threats, and ensuring the resilience and reliability of our Software as a Service (SaaS) offerings.

1. Risk Identification and Assessment

We begin by systematically identifying assets, including data, applications, and infrastructure components. This process involves evaluating their value and potential impact on your operations. We conduct thorough threat assessments to understand potential risks, such as natural disasters, cyberattacks, and system failures. Additionally, we perform vulnerability assessments to identify weaknesses within our systems that could be exploited.

2. Implementation of Control Measures

Based on our assessments, we implement appropriate control measures to mitigate identified risks. These measures are designed to provide cost-effective protection without compromising productivity. We continuously evaluate the effectiveness of these controls to ensure they meet our security objectives.

3. Continuous Monitoring and Improvement

Our commitment to security is ongoing. We continuously monitor our systems for emerging threats and vulnerabilities, adapting our risk management strategies as needed. This proactive approach ensures that we maintain a secure environment for your data and operations.

4. Compliance with Industry Standards

We adhere to industry best practices and regulatory requirements, including ISO 27001 and the Digital Operational Resilience Act (DORA), to ensure our risk management processes meet the highest standards of security and compliance.

5. Cybersecurity

Cyber security measures are in place to ensure a solid and resilient security posture.

5.1 Endpoint Security

Relevant endpoint security measures include, but are not limited to:

- **Disk Encryption**
- **Anti-virus & Anti-malware**
- **Mobile Device Management**
- **Patch Management**
- **Remote Wipe**
- **Conditional Access Policies**

5.2 Physical Security

Relevant physical security measures include, but are not limited to:

- **Access logging**
- **Electronic keys**
- **Video surveillance**
- **Alarming systems/Physical security monitoring**

5.3 Identity & Access Management

Relevant identity & access measures include, but are not limited to:

- **Single Sign On**
- **Multi Factor Authentication**
- **Privileged Identity Management**
- **Roll Based Access**

5.4 Hosting environment

CERRIX applications are exclusively hosted on Microsoft Azure, in the Western Europe region.
When hosting data on Microsoft Azure in the Western Europe region, the data is stored and processed in Microsoft's datacenters located in the Netherlands. Azure ensures that all data remains within the geographic boundaries of the European Union (EU), which is critical for compliance with the General Data Protection Regulation (GDPR).

GDPR mandates that organizations must handle personal data with care and ensure that data resides within jurisdictions that uphold equivalent data protection standards. By selecting the Western Europe region, we can meet GDPR requirements for data residency and sovereignty, benefiting from Azure's robust security measures, certifications, and transparency regarding data processing practices. Microsoft also commits to not transferring customer data outside the selected region without explicit authorization, providing an additional layer of trust and control for organizations operating under GDPR compliance obligations.

Microsoft Azure ensures redundancy in the Western Europe region through its Availability Zones and multi-datacenter infrastructure. Within the region, multiple physically separate datacenters operate in tandem to ensure high availability, data durability, and business continuity. Each datacenter is equipped with independent power, cooling, and networking systems to minimize the risk of simultaneous failures. Azure's zone-redundancy allows critical applications and data to be replicated across these datacenters, ensuring that if one datacenter experiences an outage, the others within the same region can take over seamlessly.
We utilize Microsoft Azure's backup services. Your data backup is stored in Recovery Services vaults, which are specialized storage entities within Azure designed to house backup data securely. These vaults are also located in the Azure region Western Europe but in a different Availability Zone to ensure compliance with data residency requirements and to facilitate efficient backup and restore operations.

Relevant hosting environment security measures include, but are not limited to:

- **(Security) Architecture Design & Reviews**
- **DDoS Protection**
- **Network segmentation**
- **Firewall with IDS & IPS**
- **Vulnerability Assessments**
- **Redundancy**
- **Back-up & Restore**

5.5 Application Security

Relevant application security measures include, but are not limited to:

- **Encryption at Rest**
- **Encryption in Transit**
- **Secure Authentication**
- **Role Based Access Control**
- **User Provisioning (SCIM)**
- **IP Whitelisting**
- **Virus Scanning**
- **Separate Customer Environments**

5.6 Security monitoring

Relevant security monitoring measures include, but are not limited to:

- **SOC/SIEM**
- **Application Insights**
- **Security Assessments**
- **Secure Score Monitoring**
- **Threat Intelligence**

6. Secure Software Development

Secure development measures are in place to ensure a safe and reliable SaaS product.

6.1 Security Requirements

Relevant measures include, but are not limited to:

- **Coding Standards**
- **Code Reviews**

6.2 Secure Design

Relevant secure design measures include, but are not limited to:

- **Security by Design**

6.3 Secure Development

Relevant secure development measures include, but are not limited to:

- **OWASP and other best practices**

6.4 Secure Testing

Relevant security testing measures include, but are not limited to:

- **Manual Software Testing**
- **Automated testing**

6.5 Secure Deployment

Relevant secure deployment measures include, but are not limited to:

- **Repository Security**
- **Secure Pipelines**

6.6 Asset Management

Relevant asset management measures include, but are not limited to:

- **Inventory of software libraries and components**
- **Inventory of Infrastructure components**
- **Inventory of Data**

7. Business Continuity

As a Software-as-a-Service provider, we understand the critical role our platform plays in your business operations. Our Business Continuity strategy is designed to mitigate risks, maintain service integrity, and ensure that your access to our platform remains uninterrupted, even in the event of unforeseen events.

7.1 Business Continuity Plan

Our comprehensive Business Continuity Plan (BCP) is aligned with industry best practices and is regularly reviewed and tested to address potential disruptions, such as natural disasters, cyberattacks, or technical failures. By leveraging resilient infrastructure, robust recovery protocols, and proactive risk management, we are committed to safeguarding the availability of our services and minimizing any operational impact on your business.

7.2 Business Continuity Scenarios

Business continuity scenarios refer to the different types of events or disruptions that a business might plan for to ensure operations continue smoothly. These scenarios help identify risks and prepare strategies to mitigate them. CERRIX has defined scenarios for the following situations:

7.3 Business Continuity Testing

Regular testing of the business continuity plan is conducted to ensure readiness for unforeseen events. Based on a Business Impact Analysis (BIA) , the most likely scenarios and/or scenarios with the highest impact are selected for Business Continuity Testing.

7.4 Backup & Restore

Client production environments are backed-up continuously for 14 days so that we can meet our RPO of 1 hour and RTO of 8 hours. Full back-ups are performed on a weekly basis by Azure with a retention period of one month and Monthly full back-ups are performed with a retention period of 6 months.

Twice a year we test if backups can be successfully restored in line with out defined RPO and RTO.

8. Awareness & Training

8.1 Awareness training

All CERRIX employees have to conduct mandatory security awareness training. Every quarter, three awareness modules are published and have to be completed that quarter. The security officer monitors compliance with this requirement.

8.2 Training

Employees that are involved in the software development lifecycle, also have to conduct specific trainings with regards to secure software development, including the training Secure Software Development LifeCycle and the training Master the OWASP Top 10.

8.2 Phishing Simulations

At least once a year, CERRIX conducts a phishing simulation to assess and enhance our employees' ability to recognize and respond to phishing attacks.

9. Third-Party Management

9.1. Supplier onboarding

All suppliers must undergo a formal assessment process before they are approved. The assessment will include:

- **Security Questionaire**
  Suppliers must complete a security questionnaire to provide information about their security practices.
- **Risk Assessment**
  Our security team will conduct a risk assessment based on the supplier's responses and the nature of the service provided.
- **Contracts**
  All suppliers must sign contracts that include specific security requirements and clauses.
- **Audits**
  For high-risk suppliers, an optional audit may be part of the onboarding process.

9.2 Supplier evaluation

Approved suppliers will be subject to ongoing monitoring and periodic reassessment to ensure continued compliance with security requirements. This will include:

- **Regular reviews**
  Regular review of security practices and controls.
- **Annual reassessment**
  Annual reassessment for high-risk suppliers.
- **Immediate reassessment**
  Immediate reassessments in case of security incidents or changes in the supplier's operations.

9.3 Supplier classification

CERRIX is reliant on a few suppliers for our core service, the development and delivery of a GRCA platform. The critical and high importance suppliers have been listed in the table below:

#	Supplier	Service	Description	Classification	Data processor
1	Microsoft	Hosting Services	MS Azure Hosting platform	High risk	Yes
2	Halo Service Solutions Limited	ITSM platform	Halo PSA platform. IT Service Management System for ticket registration and resolution.	Medium risk	Yes
3	EightFence B.V.	Security Operations Center	Managed Security Information and Event Management (SIEM).	Medium risk	Yes
4	BSI	ISO 27001	ISO 27001 external auditor	Low risk	No
5	Securesult	Pentesting	Outsourced pentesting	Low risk	No