CERRIX

ENG

Service Organization Control Report 2024

1st of January 2024 – 31st of December 2024
CERRIX B.V.

Statement of non-disclosure

This report is intended solely for the use of CERRIX, CERRIX clients and their related independent auditors. We expressly deny any liability, responsibility, or duty of care to any other third parties, whether in contract, or otherwise, who may gain access to this report.

This report includes confidential information which at all times remains the property of CERRIX. Clients and their related independent auditors may use this information to evaluate CERRIX given the services provided to its clients, as far as relevant for internal control over financial reporting. Clients and their related independent auditors may not copy, reproduce, sell or in any other way transfer this information, or provide it to a person, organization, or company.

CERRIX B.V.,
The Hague, 27th of May 2025.

Table of contents

SECTION 1: Management statement of CERRIX B.V.

The accompanying description has been prepared for customers who have used CERRIX's software and services and underlying IT management processes with respect to the CERRIX (GRCA) software suite of CERRIX B.V. , and their auditors who have a sufficient understanding to consider the description, along with other information including information about controls operated by customers themselves, when assessing the risks of material misstatements of customers' financial statements.

CERRIX B.V. confirms that:

(a) The accompanying descriptions in section 3 fairly presents CERRIX's description of the IT Management processes of the CERRIX system throughout the period 1 January 2024 to 31 December 2024 for the services provided with regards to the CERRIX system for customers in scope of this report. The criteria used in making this statement were that the accompanying description:

(i) Presents how the system was designed and implemented, including:

- The types of services provided, including, as appropriate, classes of transactions processed.
- The procedures, within both information technology and manual systems, by which those transactions were initiated, recorded, processed, corrected as necessary, and transferred to the reports prepared for customers.
- The related accounting records, supporting information and specific accounts that were used to initiate, record, process and report transactions; this includes the correction of incorrect information and how information was transferred to the reports prepared for user organizations.
- The related information used for providing the services;
- How the system dealt with significant events and conditions, other than transactions;
- The process used to prepare reports for customers;
- Relevant control objectives and controls designed to achieve those objectives;
- Controls that we assumed, in the design of the system, would be implemented by user entities, and which, if necessary to achieve control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved by ourselves alone;
- Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that were relevant to processing and reporting user organizations' transactions.

(ii) Includes relevant details of changes to the service organization's system during the period 1 of January 2024 to 31 December 2024.

(iii) Does not omit or distort information relevant to the scope of the system being described, while acknowledging that the description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in its own particular environment.

(b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period 1 January 2024 to 31 December 2024, except for the following matters:

- All changes are registered, classified, tested and approved prior to migration to the production environment;
- User access is limited to users based on their function;
- Information security policy / code of conduct is up to date and communicated to relevant parties;
- Suppliers are monitored on operational and information security aspects;
  Business disruptions are mitigated timely and completely.

The criteria used in making this statement were that:

(i) The risks that threatened achievement of the control objectives stated in the description were identified; and
(ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved and:
(iii) The controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period 1 January 2024 to 31 December 2024.

CERRIX,
The Hague, 27th of May 2025.

Niels van Weereld
CEO
CERRIX B.V.

Reasonable assurance report of the independent auditor

To: management of CERRIX B.V.

Assurance report on the description, design, implementation and operating effectiveness of internal controls (type II)

Our qualified opinion

In our opinion, except for the matter(s) described in the 'Basis for our qualified opinion' section, in all material respects,

- the description fairly presents the system that was designed and implemented throughout the period from 1 January 2024 to 31 December 2024;
- the controls related to the control objectives were suitably designed and implemented to achieve the control objectives if the controls operated effectively throughout the period from 1 January 2024 to 31 December 2024;
- the controls operated effectively to achieve the control objectives throughout the period from 1 January 2024 to 31 December 2024.

The criteria applied in forming our opinion are the criteria described in 'Section 1: Management statement of CERRIX B.V.' (hereafter: the management statement of the service organisation).

Our opinion has been formed based on the matters outlined in this assurance report. The specific controls tested and the nature, timing and results of those tests are described in the accompanying 'Section 4: Control framework, testing and results', with the control descriptions and results of testing containing controls objectives, internal controls and test procedures of the independent auditor and test results (hereafter: the description of test procedures and results).

What we have examined

We have examined CERRIX B.V.'s description entitled the system description of the service organisation included in 'Section 3: Overview of CERRIX's system' of the IT management processes for processing of transactions of the user entities (hereafter: the system) throughout the period from 1 January 2024 to 31 December 2024 (hereafter: the description). We also examined the design, implementation and operating effectiveness of controls related to the control objectives stated in the description (hereafter: the control objectives).

'PwC' is the brand under which PricewaterhouseCoopers Accountants N.V. (Chamber of Commerce 34180285), PricewaterhouseCoopers Belastingadviseurs N.V. (Chamber of Commerce 34180284), PricewaterhouseCoopers Advisory N.V. (Chamber of Commerce 34180287), PricewaterhouseCoopers Compliance Services B.V. (Chamber of Commerce 51414406), PricewaterhouseCoopers Pensions, Actuarial & Insurance Services B.V. (Chamber of Commerce 54226368), PricewaterhouseCoopers B.V. (Chamber of Commerce 34180289) and other companies operate and provide services. These services are governed by General Terms and Conditions ('algemene voorwaarden'), which include provisions regarding our liability. Purchases by these companies are governed by General Terms and Conditions of Purchase ('algemene inkoopvoorwaarden'). At www.pwc.nl more detailed information on these companies is available, including these General Terms and Conditions and the General Terms and Conditions of Purchase, which have also been filed at the Amsterdam Chamber of Commerce.

The basis for our qualified opinion

1. Qualified opinion: internal controls were not sufficiently designed and implemented to provide reasonable assurance that internal controls that are included in the service organisation's description of its system will be achieved if internal controls are operating effectively:

CERRIX B.V. states in the description that the controls as mentioned in the table below are in place. We determined however that these controls are not suitably designed and implemented to achieve the related control objectives throughout the period from 1 January 2024 to 31 December 2024.

Proces: Security management

Control objective	Control number	Control description
User access is limited to users based on their function	C87	Whenever administrator actions are necessary on client environments, the DevOps team has to do a PIM request to elevate their user rights before they are allowed to access the client database. All PIM requests are reviewed by the CTO, logged and checked on validity. If necessary, appropriate actions are taken.
Information security policy / code of conduct is up to date and communicated to relevant parties	C7	Annually, or in case of significant changes to the ISMS, the Strategic Information Security Policy is reviewed by the CTO and updated if necessary. At least the following things will be checked: - The information security principles. - The information security objectives. - The key roles and responsibilities for information security. The high level information security policies. The new version is approved by the CERRIX CEO. The newly approved version is distributed to all personnel. All personnel will digitally confirm he/she has read and will comply to the Information Security Policy.
Information security policy / code of conduct is up to date and communicated to relevant parties	C22	Annually, the CTO reviews and updates the Code of Conduct according to the latest developments. The new version is approved by the CEO. The newly approved Code of Conduct is distributed to all CERRIX personnel and all CERRIX personnel need to digitally confirm he/she has read and will comply to the Code of Conduct.

Proces: Monitoring of external suppliers

Control objective	Control number	Control description
Suppliers are monitored on operational and information security aspects	C107	The Managing Director monitors the uptime of client environments quarterly via the uptime monitor. If uptime is outside parameters a message will be sent to the Slack channel. Azure will resolve as much issues as possible. Exception issues causing major time-outs will be added as an operational incident in the CERRIX event database and followed up.
Suppliers are monitored on operational and information security aspects	C42	Annually, all service providers that are labelled as 'Important' or 'Critical' are evaluated and reviewed by the CTO on operational- and information security performance. This may include: - SLA validity and performance - Security certifications e.g. ISO27001 - SOC 2 reports - Incidents

Proces: Business continuity

Control objective	Control number	Control description
Business disruptions are mitigated timely and completely	C47	Annually, the Information Security Officer and/or CTO reviews the Business Continuity Plan for changes based on outcomes of Business Recovery Tests, changes in best practices and changes within CERRIX. When necessary a new version is created and sent to the Managing Director for approval. After approval the new version of the Business Continuity Plan will be communicated to all relevant stakeholders within CERRIX.

2. Qualified opinion: internal controls were not operating effectively throughout the period under review:

CERRIX B.V. states in the description that the controls as mentioned in the table below are implemented. However, as described in ‘Section 4: Control framework, testing and test results’ of the description, these controls were not operating effectively throughout the period from 1 January 2024 to 31 December 2024. This resulted in the non-achievement of the below stated control objectives throughout the period from 1 January 2024 to 31 December 2024.

Proces: Change / release management

Control objective	Control number	Control description
All changes are registered, classified, tested and approved prior to migration to the production environment	C103	Changes are requested via the ITSM system of CERRIX. Clients can request a change via the customer portal and involved CERRIX employees can request changes directly in the backend of the ITSM system. The customer support officer will validate the request and make sure the request is clear and updated with relevant information. Change Requests will be assessed and approved before they are executed. The assessment will contain an assessment of the impact on Information Security. The ticket is updated with applicable information security impact and the approval.

Proces: Security management

Control objective	Control number	Control description
User access is limited to users based on their function	C71	Every quarter, a check is performed on administrator accounts. Only the DevOps team and the CTO should have administrator rights.

Proces: Monitoring of external suppliers

Control objective	Control number	Control description
Suppliers are monitored on operational and information security aspects	C44	Azure reports general Service incidents & Security advisories via their Service Health dashboard. The CTO analyses quarterly if there are important items and performs follow up if necessary.

Further details with regards to our tests of controls and findings are described in ‘Section 4: Control framework, testing and test results’.

We performed our examination in accordance with Dutch law, including Dutch Standard 3402 ‘Assurancerapporten betreffende interne beheersingsmaatregelen bij een serviceorganisatie’ (assurance reports on controls at a service organisation).

This engagement is aimed to obtain reasonable assurance. Our responsibilities in this regard are further described in the section ‘Our responsibilities for the examination’ of this assurance report.

We believe that the assurance evidence we have obtained is sufficient and appropriate to provide a basis for our qualified opinion.

Independence and quality control

We are independent of CERRIX B.V. in accordance with the 'Verordening inzake de onafhankelijkheid van accountants bij assuranceopdrachten' (ViO, Code of Ethics for Professional Accountants, a regulation with respect to independence) and other relevant independence requirements in the Netherlands. Furthermore, we have complied with the 'Verordening gedrags- en beroepsregels accountants' (VGBA, Dutch Code of Ethics for Professional Accountants, a regulation with respect to rules of professional conduct).

PwC applies the applicable quality management requirements pursuant to the 'Nadere voorschriften kwaliteitsmanagement' (NVKM, regulations for quality management) and the International Standard on Quality Management (ISQM) 1, and accordingly, maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Matters related to the scope of our examination

The description indicates that certain control objectives can only be achieved if complementary controls at user entities, assumed in the design and implementation of CERRIX B.V.'s controls are suitably designed, implemented and operating effectively, along with related controls at the service organisation. Our examination did not extend to such complementary controls at user entities, and we have not evaluated the suitability of the design, implementation or operating effectiveness of such controls.

CERRIX B.V. uses Microsoft Azure for datacenter services and Platform as a Service (PaaS) solutions, Microsoft Azure DevOps for the internal ticketing system, HaloPSA for its IT service management system, EightFence for the management of Microsoft Sentinel SIEM solution, and Netrom for sourcing of their development team. The description includes only the control objectives and related controls of CERRIX B.V. and excludes the control objectives and related controls of Microsoft Azure, Microsoft Azure DevOps, HaloPSA, EightFence and Netrom. Our examination did not extend to controls of Microsoft Azure, Microsoft Azure DevOps, HaloPSA, EightFence and Netrom, and we have not evaluated the suitability of the design, implementation operating effectiveness of such controls.

The information included in 'Section 5: Management response on auditor findings' is presented by management of CERRIX B.V. to provide additional information and is not part of the description. This information has not been part of our examination of the description of the system and the design, implementation and operating effectiveness of controls to achieve the related control objectives, and accordingly we express no opinion thereon.

Our opinion is not modified in respect of these matters.

Limitations of a description and to controls at a service organisation

The description is prepared to meet the common needs of a broad range of user entities and their auditors and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment.

Because of their nature, controls at a service organisation may not prevent, or detect and correct, all errors or omissions. Also, the projection to the future of conclusions about the suitability of the design, implementation or operating effectiveness of the controls to achieve the control objectives is subject to the risk that controls at a service organisation may become ineffective.

Restriction on use and distribution

Our assurance report and the description of test procedures and results is addressed to and intended for the exclusive use of CERRIX B.V., user entities of CERRIX B.V.'s system during the period from 1 January 2024 to 31 December 2024, and their auditors, who have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organisations and user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not to be relied on by any third party (other parties) as such parties are not aware of the purpose of the assessment and they could interpret the results incorrectly. Our assurance report (or any part of it) may therefore not be made available in any form to third parties without our prior written consent. We do not accept or assume and deny any liability, duty of care or responsibility to any parties other than CERRIX B.V. and the user entities of CERRIX B.V.'s system and their auditors.

Responsibilities

Responsibilities of management of the service organisation

Management has provided the accompanying management statement of the service organisation about the fairness of the presentation of the system in the description and the design, implementation and operating effectiveness of the controls described therein to achieve the related control objectives. Management is responsible for:

- preparing the description and the management statement of the service organisation, in accordance with the criteria described in the management statement of the service organisation, including the completeness, accuracy, and method of presentation of the description and the management statement of the service organisation;
- providing the services covered by the description;
- specifying the control objectives and stating them in the description;
- identifying the risks that threaten the achievement of the control objectives; and
- suitably designing, implementing, and documenting controls to achieve the related control objectives.

Furthermore, management is responsible for such internal control as it determines is necessary to enable the preparation of the description that is free from material misstatement, whether due to fraud or error and for monitoring of controls to assess their effectiveness, to identify deficiencies and to take corrective actions.

Our responsibilities for the examination

Our responsibility is to plan and perform our examination in a manner that allows us to obtain sufficient and appropriate assurance evidence for our opinion.

Our opinion provides reasonable assurance on the fairness of the description and on the design, implementation and operating effectiveness of the controls described therein to achieve the related control objectives in accordance with the criteria described in the management statement of the service organisation.

Our examination has been performed with a high, but not absolute, level of assurance, which means we may not detect all material errors and fraud during our examination. Reasonable assurance is a high but not absolute level of assurance, which makes it possible that we may not detect all material misstatements.

Deviations may arise as a result of fraud or errors. Deviations are material if it can reasonably be expected that they, individually or collectively, can influence the economic decisions that users make based on the description. The materiality influences the nature, timing and extent of our work and the evaluation of the effect of identified deviations on our opinion.

Procedures performed

Our examination of the description of the system and the design, implementation and operating effectiveness of controls consisted, among other things, of the following:

- identifying and assessing the risks that the description is not fairly presented and that the controls are not suitably designed, implemented or operating effectively to achieve the control objectives throughout the period from 1 January 2024 to 31 December 2024, whether due to errors or fraud, designing assurance procedures responsive to those risks in order to obtain assurance evidence that is sufficient and appropriate to provide a basis for our opinion;
- evaluating the overall presentation of the description, the suitability of the control objectives, and the suitability of the criteria described by the service organisation in the management statement of the service organisation;
- performing procedures to obtain assurance evidence about the fair presentation of the description of the controls to achieve the control objectives;
- testing the operating effectiveness of those controls necessary to provide reasonable assurance that the control objectives were achieved.

Amsterdam, 27 mei 2025
PricewaterhouseCoopers Accountants N.V.

Jasmijn van Dieren

J. van Dieren RA
partner

SECTION 3: Overview of CERRIX's system

The following section describes:

- Introduction of CERRIX
- The scope of this report
- An overview of CERRIX's risk and control system
- CERRIX's relevant processes
- Client responsibilities

3.1 Introduction of CERRIX

CERRIX is a supplier of Governance, Risk and Compliance and audit (GRCA) software (hereafter CERRIX software suite). In addition, we provide consulting services in the area of Governance, Risk management, Compliance and IT-audit related to the CERRIX software. With our dedicated workforce we develop and implement the CERRIX software suite and help clients to reach a higher level of risk maturity. The CERRIX software suite is designed to support every aspect of the risk management and control cycle of our clients. We believe in a joint effort between business consultants and our clients to constantly improve and optimize the CERRIX software suite. Our offices are located in The Hague, The Netherlands and Antwerp, Belgium.

3.2 Scope of the report

3.2.1 General scope

The general scope of this report is determined by the products and services that CERRIX delivers to its clients.

The following product is in scope:

- CERRIX (GRCA) software suite, consisting of process management, risk management, control testing, improvement management, incident management, data management, KRI/KPI management, third party management, flexible forms, audit management and embedded PowerBi reporting options.

For this product, the following services are in scope:

- CERRIX GRCA software is offered as Software as a Service accessible via Internet
- SaaS license grants frequent release updates to clients and first line support
- Available 24 hours a day, 7 days a week (except for maintenance hours)
- Automated back-up of client production and acceptation environments
- Secure connections and additional security measures

3.2.2 Processes in scope

In order to determine the processes in scope, CERRIX reviews the existing SLA's that are agreed with its clients for the products and services in scope of this report.

The following processes are considered relevant and are therefore in scope of this report:

Processes in scope of this report
Availability Management, consisting of the following subprocesses: • External backup & restore
Change/release management
Incident/problem management
Security management, consisting of the following subprocesses: • Maintain Information Security Policy • Physical Access control • Logical Access control • Network & Infrastructure security • Endpoint Security
Monitoring of external suppliers
Business Continuity Management

3.2.3 Systems in scope

A table of identified systems CERRIX uses in their day-to-day operations is listed below.

System	*Hosting*
CERRIX (GRCA) software suite	Azure, Western Europe
Azure DevOps	Azure, Western Europe
HaloPSA, Professional Service Automation	AWS, Frankfurt

3.2.4 Processes outsourced to external suppliers

CERRIX outsources several processes to external suppliers. Final responsibility for these outsourced processes remains with CERRIX. To assess adequacy of control objectives and controls of external suppliers, the carve-out method is used. The description in this report includes only the control objectives and related controls of CERRIX and excludes the control objectives and related controls at Microsoft. Instead CERRIX has implemented the process "monitoring of external suppliers." Via this process CERRIX reviews and monitors the adequacy of the key external suppliers' control objectives and controls to mitigate client risks. The following key external suppliers are identified:

.

- **Microsoft Azure:** Provides Datacenter services and Platform as a Service (PaaS) solutions which are used to host CERRIX SaaS applications. The maintenance of the PaaS platform and datacenter is fully managed by Microsoft while the full management of the GRCA suite, data and databases is managed by CERRIX.

- **Microsoft Azure DevOps:** Internal ticketing systems used by the software development department. DevOps is hosted by Microsoft on its Azure platform and has its own SOC 1 and SOC 2 assurance reports. CERRIX monitors the SOC 2 report as the controls between the SOC1 and SOC2 reports are the same. The reason for monitoring the SOC 2 is that it focuses on IT-specific controls.

- **HaloPSA:** In 2024, CERRIX implemented HaloPSA as its IT Service Management system. This system provides a client portal for all customers where they can report tickets (e.g. Incidents, bugs, Service Requests, etc). While Halo is considered a valuable system in the service chain of CERRIX, it is not deemed high risk and CERRIX's service delivery can continue to function without it. Halo is ISO 27001 certified.

- **Eightfence:** In 2024, CERRIX implemented Microsoft Sentinel, a SIEM solution which is managed and monitored by Eightfence. Eightfence runs a 24x7 Security Operations Center. Each month a service review takes place to monitor the performance of Eightfence. Eightfence is ISO 27001 certified.

- **Netrom:** In 2024, CERRIX hired two external developers from Netrom. These developers work in the Dutch development teams under the daily supervision of CERRIX. These developers have access to our source code and therefore Netrom is deemed a high risk supplier. Their developers however, have no access to customer environments and/or customer data. Netrom is ISO 27001 certified. The development activities performed by Netrom are monitored by Cerrix via the monitoring controls over the change management activities, as found in section 4.1.2 Change / Release Management.

3.3 Internal control system

The products and services in scope of this report are in many cases linked to the financial reporting process of CERRIX's clients. Consequently, CERRIX's clients and their external auditors are dependent on an evaluation of CERRIX's internal control system by an independent external service auditor. CERRIX therefore provides insight in its organisation and the quality of its internal control system by means of this report.

CERRIX seeks after the highest possible quality of service for its clients. Therefore, it is important to control client risks for their financial reporting that are related to CERRIX's processes, systems and external suppliers. In order to adequately control risks, CERRIX has set up an internal control system based on COSO (see figure 1).

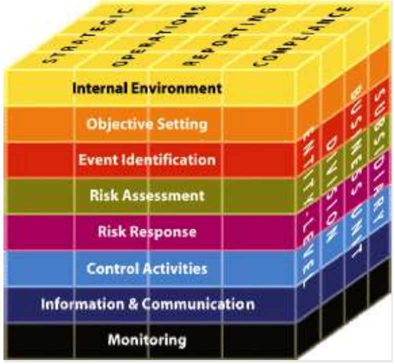

Figure 1: Internal control system based on COSO II.

The following paragraphs provide a description of:

- *The internal environment:* Describes CERRIX's organisation, its risk appetite, the way it manages risk awareness and employee integrity, the way risk management is governed.
- *Objective setting*: Describes CERRIX's business objectives and related risk management objectives.
- *Event identification and risk assessment:* Identifies events (risks) that can have a negative effect on CERRIX' objectives and scores these events (risks) on likelihood and impact.
- *Risk response:* Describes CERRIX's possible risk responses to identified risks.
- *Control activities:* Describes CERRIX's control activities.
- *Information & communication:* Describes how CERRIX communicates about risk management.
- *Monitoring*: Describes how CERRIX monitors its risks and controls.

3.3.1 Internal environment

The internal environment consists of CERRIX's organisation and general framework of processes and controls in which it operates. This paragraph describes CERRIX's risk appetite, risk awareness, risk governance and responsibility, employee integrity and CERRIX´s organisational structure.

Risk appetite

CERRIX deems the security of its systems and client data of the utmost importance. CERRIX strives to stay ahead of increasing compliance and customer demands. Therefore, CERRIX's risk appetite can be characterised as risk averse. The risk appetite is reviewed periodically as part of the Risk Assessment.

Risk awareness

CERRIX demands of its employees to be highly risk aware. This is done by:

- Performing periodic risk assessments.
- Security awareness program (Awaretrain)
- Periodic communication of security policies and code of conduct.
- Communication of key risk, events, and measures of improvement to related departments.

Risk governance and responsibility
CERRIX is a small organization and therefore cannot implement the 3-lines of defense model. To adequately implement risk governance and responsibility, CERRIX uses the following risk governance model.

Within CERRIX, the departments are primarily responsible for managing risks within the processes executed and systems used. Management of risks is executed by:

- Evaluating risk by the execution of periodic risk assessments.
- The (day to day) execution of controls.
- The implementation and/or improvement of controls.

The Chief Information Security Officer (CISO) and the Information Security Officer (ISO) execute the monitoring function. The CEO is accountable for the proper execution of internal control system within CERRIX. The CISO is responsible for facilitating the risk management process within CERRIX.

Considering business economics, CERRIX has not implemented an independent 2nd (risk management and compliance department) or 3rd line of defense (internal audit department). It is foreseen that every year, an independent service auditor will audit the design, implementation, and the operational effectiveness (in the form of an assurance report in line with Dutch Standard 3402) of CERRIX's risk and control system. During the audit, the service auditor will perform test activities (i.e., sample testing, walk troughs, etc.). During the execution of these test activities, the departments will provide the evidence of controls executed.

Employee integrity
Screening of new personnel is standard procedure within CERRIX. The following screening activities are executed:

- ***Identity control:*** New employees of CERRIX must identify themselves by providing CERRIX with a copy of their passport or driving license before employment contracts are signed to determine the identity of the employee.
- ***Screening:*** All employees must be screened within reasonable time after start of employment. As part of this screening the employee must provide CERRIX with a so called "Verklaring Omtrent Gedrag (VOG)" and relevant school diplomas and past work references may be verified by CERRIX.

CERRIX's organisation

The organisational structure is shown in figure 2. The departments in scope are marked in red.

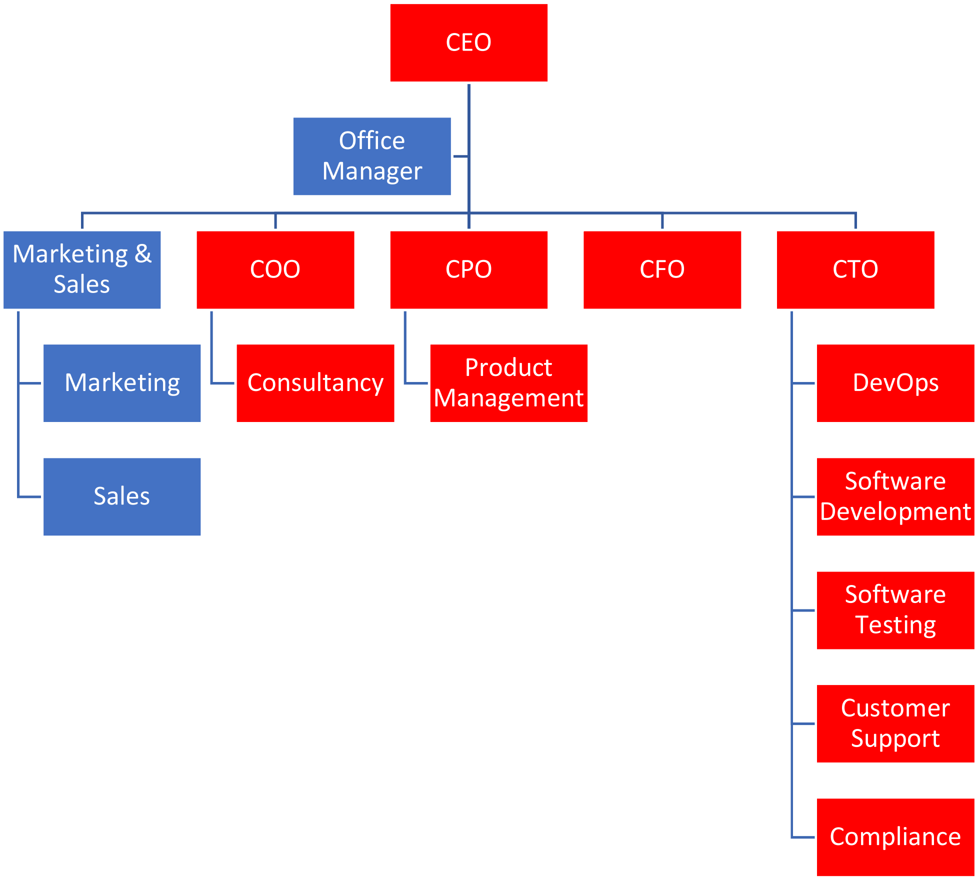

Figure 2: Organisational structure of CERRIX.

CEO

The day-to-day activities of CERRIX are executed under the responsibility of the CEO.

Sales and Marketing

The sales and marketing department consists of 3 people. Their main focus is generating new business. Furthermore they execute marketing activities such as conventions, social media marketing, etc. The sales and marketing processes are not in scope of this report.

Professional Services
The Professional Services department consists of 4 consultants and is responsible for consultancy services in the field of Governance, Risk, Compliance and IT-audit. The department is managed by the Manager Operations.

Customer Support
Since April 2024, CERRIX has a dedicated Customer Support Officer. Customer support is responsible for responding to client questions, problems, and incidents. Also, this employee monitors the progress of change requests. Customer support was managed by the Manager Operations/Professional Services in 2024 but has moved to the responsibility of the CTO in the last quarter of 2024. The following processes in scope of this report are partly executed by this department:

- Incident/problem management
- Change/release management

Compliance
The Compliance department is responsible for facilitating Information Security & Privacy within CERRIX. The department has 1 Information Security Officer and is managed by the CTO who is also the CISO.

Responsibilities for Information Security, Privacy and Compliance are transferred in 2024 from the Manager Operations to the CTO/CISO in august 2024.

The following processes in scope of this report are partly executed by the Compliance department:

- Security management
- Risk Management
- Privacy Management
- Cybersecurity

Software Development
The Development department consists of nine internal employees and 2 external employees and is managed by the Chief Technology Officer (CTO). This department is responsible for the development, delivery, and maintenance of the CERRIX software. The following processes in scope of this report are (partly) executed by this department:

- Change/release management
- Incident/problem management

IT-operations (DevOps)
The IT-operations department consists of 3 people and is managed the Chief Technology Officer (CTO). This department is responsible for IT-operations (IT-availability, IT-maintenance, technical set-up of client environments, etc). The following processes in scope of this report are (partly) executed by this department:

- Availability management
- Change/release management

- Incident/problem management
- Cybersecurity

Software Testing

The Software Testing department consists of 1 Manual Test Engineer and 1 Test Automation Engineer and is responsible for testing activities (Regression testing, functional testing). The department is managed by the Chief Techology Officer (CTO). The following processes in scope of this report are partly executed by this department:

- Incident/problem management
- Change/release management

Management Team

The CERRIX Management Team consists of:

Role	Name
CEO	Niels van Weereld
CFO	Caro van Rompaey
COO	Maurits Toet
CTO/CISO	René van der Horst
VP Marketing & Sales	Emilie Hellemans
Sales Director	Marcel Pentier

Risk Committee

CERRIX's Risk Committee is a subset of the Management team, supported by the Information Security Officer (ISO):

Role	Name
CEO	Niels van Weereld
CFO	Caro van Rompaey
COO	Maurits Toet
CTO/CISO	René van der Horst
ISO	Ilse Vinke

3.3.2 Objective setting

Information security objectives are crucial to protect sensitive customer data, ensure service reliability, and maintain compliance. CERRIX has defined the following information security objectives:

1. **Ensure Data Confidentiality, Integrity and Privacy**
   - Ensure that we protect information (client, internal, employee) from unauthorized access, loss, tampering or leakage.
   - Ensure that information remains accurate and consistent.
   - Ensure that information is recoverable in case of unforeseen events.

2. **Guarantee Service Availability**
   - Ensure continuous access to our SaaS GRC platform.
   - Ensure platform performance and scalability to avoid outages and bottlenecks.

3. **Comply with Regulatory and Legal Requirements**
   - Ensure that we comply with relevant regulations, depending on the clients and regions served.

4. **Maintain Secure Software Development Practices**
   - Ensure that we comply with CERRIX internal security standards.
   - Ensure that we limit security vulnerabilities.
   - Ensure that we limit security incidents.

5. **Enhance Incident Detection and Response**
   - Ensure that incidents are detected in a timely manner.
   - Ensure that the incident response is adequate and incidents are resolved within the agreed Service Levels.

6. **Control Internal, External and Third-Party Risks**
   - Ensure that Risks are identified, prioritized and mitigated.
   - Ensure business continuity by protecting against identified as well as unidentified risks (preparedness).

7. **Foster a Security-Aware culture**
   - Ensure employee awareness of security risks.
   - Promote Secure Behavior and Best Practices.

3.3.3 Risk Assessment

Risk Assessment is executed annually by CERRIX's Risk Committee and facilitated by the Information Security Officer for the processes and systems in scope of this report. During the Risk Assessment, the Risk Committee will identify the relevant risks and re-evaluate the existing risks, after which a gross risk score is given to all identified and re-evaluated risks on a five-point scale for both impact and likelihood. Then the related (key) controls are identified that manage these risks. Taking the implemented controls into account, the net risk is scored using a five-point scale for both impact and likelihood. All risks, scores and controls will be recorded in CERRIX's GRC tooling, CERRIX.

Additionally, risks, risk scores, controls, incidents, and measures of improvements are continuously updated. All changes are documented in CERRIX.

3.3.4 Risk response

After the risk assessment the Management Team will review the identified and scored risks and related (key) controls and will determine if each risk is at an acceptable level (within the risk appetite). During this review, the following risk response options are available:

- **Accept:** the risk at its current level of impact and likelihood is accepted
- **Mitigate risk:** Additional controls are implemented to manage the risk further
- **Transfer risk:** Risk is transferred to an external party (i.e., IT-supplier, insurer)
- **Avoid:** The activity the risk relates to is stopped

Any necessary actions are coordinated by the CISO. For each risk, the risk response is documented in CERRIX.

3.3.5 Control activities

After the controls are identified in the event identification and risk assessment they are implemented in the organisation. Control activities are then executed on a day-to-day basis. Evidence of control activities is stored on CERRIX's network and in CERRIX. For a description of control objectives and controls, we refer to Section 4 of this report.

3.3.6 Information and communication

This paragraph describes the mechanism for information and communication within CERRIX. Here CERRIX's meeting structures, reporting structures and communication of the information security policy are described.

Meeting structures

CERRIX has implemented the following meeting structures:

Meeting	Participants	Frequency
Consultants meeting	Manager Operations, Consultants	On event
Development meeting	Product Owner, Development team	Bi-Weekly
Management meeting	Managing Director, Manager Operations & CTO.	Monthly

Reporting structures

CERRIX has implemented the following reporting structures:

Report name	Report description
CRSA report	Once every year, after the risk assessment is executed, a CRSA report is generated for the CEO. This report contains the identified and scored risks and the related (key) controls.
Monitoring Report, Microsoft	Once every year, The SOC of Microsoft Azure and Azure Devops are reviewed by the Manager Operations or the CISO

Report name	Report description
Azure and Azure Devops	and a monitoring report is created with the conclusions of the monitored ISAE3402 or SOC reports.
Follow up on measures of improvement	During MT meetings and planning meetings a follow up on measures of improvement is performed. Progress and issues are discussed and if necessary, measures of improvement are adjusted.

Communication of Information Security Policy & Code of Conduct

Employees of CERRIX must uphold CERRIX's Information Security Policies and the Code of Conduct. The Strategic Information Security Policy and the Code of Conduct are communicated annually to all employees after changes have been approved. Employees must confirm that they have taken notice of the Information Security Policy & Code of Conduct and will act accordingly. Employees who do not uphold CERRIX's norms for Information Security & the Code of Conduct will be sanctioned (with the possibility of contract termination) accordingly.

3.3.7 Monitoring

Monitoring of CERRIX's risk and control framework

The CEO periodically monitors the risk and control framework by:

- Monitoring the timely execution of the risk assessments
- Monitoring the status of risks and control measurers
- Monitoring the design and implementation of executed controls within the department
- Monitoring audits and audit findings
  - PwC is the independent external auditor for ISAE 3402 type II
  - BSI is the independent external auditor for ISO 27001
  - Audit & Risk Solutions is the Internal auditor for ISO 27001
- Monitoring the status of implementation of measures of improvement

Monitoring risk related to external suppliers

Once a year, a risk analysis is performed for all external suppliers. For external suppliers with a high-risk profile a yearly review is performed. For these key suppliers, the assurance reports (in relation to CERRIX's outsourced processes, systems) are reviewed. If an assurance report (or accepted equivalent) is not available or inadequate, an audit review (questionnaire or meeting) will be conducted by CERRIX in order to establish if it's risk and control framework (related to CERRIX's outsourced processes, systems) is adequately set up, implemented and effective.

3.4 CERRIX processes

For the objective and scope of this report we have selected processes that are important for our clients. In the following paragraphs a description is given of all processes in scope (see also 3.2.2) of this report.

Description for back-up and restore

Client data is stored on the Microsoft Azure platform. To ensure availability, point in time, (weekly and monthly) back-ups are performed by Microsoft Azure. These back-ups are stored as follows:

- Point in time: 2 week point in time back-up is available.
- Weekly back-ups: Stored for 4 weeks on a secure location at Microsoft Azure within Western Europe.
- Monthly back-ups: Stored for 6 months on a secure location at Microsoft Azure within Western Europe.

All internal CERRIX files are placed on Microsoft Teams which has its own back-up program.

Description of change/release management

Customer Change Requests are registered in HaloPSA by CERRIX's Customers or the Customer Support Officer. The Support Officer checks if the change requests are clear and accurately described. If not, the customer is contacted for further information. After this the change requests are discussed internally and then classified for importance. Emergency requests (blockers) are picked up ASAP.

CERRIX uses the DTAP-model to develop, test and implement changes. DTAP stands for:

- Development: development of changes/releases in the development environment
- Testing: testing of changes/releases in the testing environment
- Acceptance: acceptance of changes/releases by clients in the acceptance environment
- Production: implementing the changes/releases into production environment

Purpose of the DTAP model is to maintain a sturdy process of software development and a strict segregation between production and non-production environments. Important aspects considered by CERRIX are the availability and integrity of the production environment. Below we further explain the DTAP model we use.

Development environment

For the development of the software a separate environment is used by the Development department. This environment is only available for developers and cannot be accessed by other CERRIX employees. When new developments are ready for testing an employee of this department will transfer them to the testing environment.

Test environment

The test environment is used for testing of changes and for regression testing. The environment is available for testers. This environment is separated from the production environment. First CERRIX employees test the changes. The test results (approval by CERRIX responsible) are documented in Azure DevOps. If test results are negative, adjustments will be made in the development environment. After the adjustment, changes will be retested until test results are satisfactory.

When all the changes for the release are ready, a regression test is performed in the test environment. If test results are negative, adjustments will be made in the development environment and pushed to the test environment for retesting.
If the regression test is completed with positive results the release is pushed to acceptation environment.

Acceptation environment
The release and/or changes will be made available for clients to test. If the client does not accept the changes, the responsible CERRIX employee reviews all test results and discusses a solution with the client and/or reopens the tickets for development. If the client deems the results to be satisfactory, the changes are scheduled for the next release.

Production environment
The production environment is used for day-to-day operations. The production environment is only accessible for clients and CERRIX administrators.

Release management
CERRIX delivers 4 to 6 production releases a year. Releases are based on client input, priorities and CERRIX input. For all items in the release a ticket is available in Azure DevOps. An Agile dashboard is created for each release in Azure DevOps. The Agile dashboard contains the list of tickets specified for the release. Based on the Agile dashboard, release notes are developed and communicated to affected customers when a release is ready.

Description for incident/problem management
Incidents and problems directly related to the production environments are reported by clients via CERRIX's issue tracking system Azure DevOps.

All incidents/problems directly related to the production environments are investigated and classified by CERRIX. Solution times depends on the classification, complexity of the incident/problem and agreed upon service levels. Solutions are built according to the change management process or are considered in upcoming releases. After the client accepts and approves the solution the incident/problem is closed.

Description for security management
Security management consists of the following sub processes:

- Maintain Information Security Policies
- Physical Access control
- Logical Access control
- Network & Infrastructure security
- Endpoint Security.

Maintain information security policies

information security policies are implemented and maintained by CERRIX to ensure client information is well protected and handled with care by CERRIX employees. The polices are reviewed and communicated to all CERRIX employees on a regular basis.

Physical access

Physical access controls are implemented by CERRIX to ensure that no unauthorised individuals enter the office in the Hague. Within our The Hague office this is done by means of locks on the entrances and individual rooms. Only a limited and registered number of employees have a keyset to open/close the offices. Also, an alarm system is installed with motion sensors. Only a limited and registered number of employees have personal alarm codes.

Within the The Hague office a Main Equipment Room (MER) is present. This room contains the primary network equipment and firewall for the office, however, no hosting services for clients are dependent on this MER or any equipment in the MER. This room has a fireproof door and is secured with an electronic keypad. Only authorised employees have access to the server room.

Logical access

Logical access controls are implemented by CERRIX to ensure that no unauthorised individuals have access to CERRIX's network and systems. User authorisation is maintained by the Security Officer. Periodically the Security Officer will check whether the authorisations of CERRIX employees are still accurate and up to date. This check is reviewed and approved by the CISO. Admin access to client environments is limited to 4 personalized accounts. Administrative actions on clients' environments require a PIM request and are logged and validated by the CTO.

Network & Infrastructure security.

Within CERRIX several solutions are implemented to ensure Network & Infrastructure Security. The following solutions are implemented:

- Multi-factor authentication
  CERRIX mandates Risk Based Multi-Factor authentication on all (internal- and external) employee user accounts.
- Privileged Identity Management
  Administrators (DevOps) have to make a PIM-request to receive administrative privileges before they can gain access to a customer environment.
- Network segmentation
  The network(s) are segmented to limit the risk of the potential damage of cyber threats.
- Antivirus software
  End-points are protected by anti-virus and anti-malware software which is continually updated and monitored for compliance.
- Security Information and Event Management (SIEM)
  The hosting environment is monitored 24x7 by and external Security Operations Center (SOC) by using a SIEM solution.

- IP-Whitelisting
  Customer environments are usually protected by IP whitelisting, which limits the risk of unauthorized access (from unauthorized locations).
- SSL connections
  All CERRIX client environments are SSL protected with a GlobalSign provided SSL certificate.
- Execution and follow up of penetration tests
  At least once a year, the CERRIX application undergoes an extensive pentest by a specialized external party.
- Protection against Distributed Denial of Service (DDoS) attacks
  The hosting environment is protected against DDoS attacks via Azure DDoS protection.

Endpoint Security

Within CERRIX several solutions are implemented to ensure Endpoint Security. The following solutions are implemented:

- Disk-encryption
- Antivirus software
- Anti malware
- Personal Firewall

Description for monitoring of external suppliers

Monitoring of external suppliers

An initial risk analysis is performed on external suppliers to determine the suppliers' risk profile. Secondly, in order to properly manage the suppliers with a high-risk profile, CERRIX monitors these external suppliers by reviewing the suppliers' assurance reports / certifications (ISAE3402, SOC 1/2 and/or Nen/ISO) or by performing reviews via audit questionnaires/interviews. In case of deficiencies, CERRIX will perform additional controls to ensure risks are adequately managed or consider alternative parties.

Description for business continuity management

BCM consists of 2 sub processes:

- BCM at CERRIX The Hague Office
- BCM at Microsoft Azure

BCM at CERRIX The Hague Office

CERRIX has a BCM plan for managing calamities & emergencies. Our primary defence lies in preventative hard (alarms, fire extinguishers, first-aid, etc) and soft measures (awareness & training of personnel). In case of a calamity or emergency CERRIX personnel can operate from home since CERRIX is working fully virtually and therefor Operations will be fully operational same day. We retain our back-ups of our internal files on Microsoft Teams and our software licenses are stored outside the office to ensure that quick recovery is possible. Also, we have a flexible shell of consultants who can help in times of personnel shortages.

BCM at Azure

Client production environments are hosted at Azure. Azure has an array of preventative hard and soft measures (secondary locations, fire prevention systems, alternative power sources, etc) to ensure continuity of service after calamities or emergencies. CERRIX checks these measures via the ISAE3402/SOC of Azure.

BCP scenarios are tested at least annually to increase readiness for disaster scenarios.

3.5 User control considerations

This report provides an understanding of the internal control system that underlie our services. CERRIX notes, however, that its engagement with clients involves a two-way effort, with both parties having to honour their commitments. The client's role and performance are a contributing factor to the quality of our services.

Our clients' responsibilities include but are not limited to the following:

1. Clients should give CERRIX accurate, full, and timely instructions and information (in line with contract terms) to adequately complete projects or changes
2. Clients are responsible for testing software and content changes made on their behalf
3. Clients are responsible for delivering malware-free files
4. Clients should check reports and information provided by CERRIX and report any shortcomings accurately, completely and in a timely fashion
5. Clients are responsible for reporting identified incidents or problems in CERRIX software accurately, completely and timely in CERRIX's ticket system (Azure DevOps)
6. Clients are responsible for requesting a revision of the SLA. If not, SLA's are tacitly renewed
7. Clients are responsible for the timely, accurate, complete delivery of the correct users and user-roles for authorisation in CERRIX
8. Clients are responsible for fraud committed in CERRIX software by their employees
9. Clients are responsible for upholding CERRIX's intellectual property rights.

3.6 Changes in CERRIX system and Control framework

In 2024 CERRIX has made the following changes to its system compared to the controls found in the report over 2023:

- Control 29 on the review and communication of the data management policy, has been merged into control C7 (previously control 142).
- Control 116: The business continuity test control has been reinstated and now focus on relevant disaster recovery scenarios like application or datacenter outages, cyber attacks, natural disasters, etc.
- Control 87: The control for logging of administrator access to client databases has been changed. CERRIX has implemented Privileged Identity Management (PIM) in August 2024 which improves this control. Administrators now have to perform a PIM request and motivate why they need access to a customer environment. Every PIM request is logged and validated by the CTO.
- Control 27 (previously control 169) has been changed from a quarterly control to one that is performed on-event to shorten the response time in case of reported vulnerabilities.
- Control 47 (previously control 155) has been changed to reflect the BCP is changed based on the outcomes of the business recovery test and ICT readiness assessments.
- Control 71 (previously control 78) has been changed to reflect that only the DevOps team and CTO may have administrator rights.
- Control 103 (previously control 132) has been changed to expand upon the control activities from request through approval of customer-initiated requests.
- Control 126 (previously control 140) has been changed to specify the classification of tickets (bugs, incidents, and service- and change requests initiated by customers.

- Control 127 (previously 141) has been changed to reflect the change to HaloPSA as customer portal for the reporting of tickets.
- Control 171, the check on correct merging of fixes has been integrated in control 95 (previously control 101)

3.7 Other information provided by the service auditor

PricewaterhouseCoopers Accountants N.V. (PwC) has conducted the engagement in accordance with Dutch Standard 3402, “Assurancerapporten betreffende interne beheersingsmaatregelen bij een serviceorganisatie’ (assurance reports on controls at a service organisation).

It is the user entities’ responsibility to evaluate this information in relation to internal controls in place to obtain an understanding of the internal controls and assess control risk. The user control considerations and controls by CERRIX B.V. must be evaluated together. If effective user organization internal controls are not in place, the controls by CERRIX B.V. may not compensate for such weaknesses.

The control objectives and control activities were specified by CERRIX’s management. The tests performed and the results of these tests were specified by PwC.

PwC’s test procedures were designed to cover a range of controls, processes and sub-processes at CERRIX B.V.. In selecting particular tests PwC considered (a) the nature of the items being tested, (b) the types of available evidence, (c) the nature of the audit objectives to be achieved, (d) the assessed level of control risk and (e) the expected efficiency and effectiveness of the test.

As a part of the examination of CERRIX B.V.’s controls, PwC performed several interviews and tests. The test procedures performed are described in the table below.

Testing procedure	Description
Re-performance	Re-performed the operating effectiveness of the automated, IT dependent or manual control activity
Inspection	Inspected documents and reports indicating performance of the control activity
Observation	Observed the operating effectiveness of the specific control activity
Inquiry	Made inquiries with the appropriate personnel and corroborated responses with management

The size of the samples we have selected in order to test the operating effectiveness of the controls primarily depends on the frequency of controls and assumed population of controls occurrences:

Frequency of control (category)	Sample size
Annual	1

Quarterly	2
Monthly	2 to5
Weekly	5 to 15
Daily	20 to 40
Multiple times per day	25 to 60

SECTION 4: Control framework, testing and test results

In this section control objectives and controls in scope of this report are described. design and operating effectiveness of the controls was tested by the external service auditor. The conclusions of the service auditor related to the design and operating effectiveness of these controls are described in the column "Testing by PwC."

4.1 Control Measures

4.1.1 Availability management

Control objective: Backups of client data are regularly and securely performed.

Controls for Availability management				
CERRIX ID	**#**	**Controls**	**Testing by PwC**	**Test results PwC**
C84	**1.1.2**	**External back-up** Client production environments are backed-up continuously for 14 days (point in time) by Azure. Full back-ups are performed on a weekly basis by Azure with a retention period of one month. Monthly full back-ups are performed with a retention period of 6 months. Yearly the system admin checks if backup settings are correct for all client environments.	We inspected the yearly check on back-up and retention settings on client production environments to determine whether the system admin determined the correctness of backup settings.	No exceptions noted.

Control objective: Archived client data is available for complete and correct restoration in the event of processing errors.

Controls for Availability management				
CERRIX ID	**#**	**Controls**	**Testing by PwC**	**Test results PwC**
C85	**1.2.1**	**External back-up restore testing** Twice a year the System Administrator will test if a Point In Time Retention back-up and a Long Time Retention back-up at Azure can be restored. This test includes a full (client database) restore test. The test is successful if the client site can be started and data is available. When issues occur they will be discussed with Azure, solved and retested until restore test is correctly performed.	We inspected a half yearly back-up restore test for Point in Time Retention and Long Time Retention to determine whether a CERRIX system administrator performed this restore test. In addition, we inspected if issues have been discussed with Azure, resolved, and retested correctly.	No exceptions noted.

4.1.2 Change / Release Management

Control objective: All changes are registered, classified, tested and approved prior to migration to the production environment.

Controls for change/release management				
CERRIX ID	**#**	**Controls**	**Testing by PwC**	**Test results PwC**
C103	**2.1.1**	**Registration and requirements of changes** Changes are requested via the ITSM system of CERRIX. Clients can request a change via the customer portal and involved CERRIX employees can request changes directly in the backend of the ITSM system. The customer support officer will validate the request and make sure the request is clear and updated with relevant information. Change Requests will be assessed and approved before they are executed. The assessment will contain an assessment of the impact on Information Security. The ticket is updated with applicable information security impact and the approval.	We have inspected a selection of change requests within the ITSM system and the backend of the ITSM system. We determined if these change requests have been validated and updated by the customer support officer. In addition, determined if the assessment was performed including the impact of Information Security.	Exception noted: For 6 out of 30 selected change requests within the ITSM system, we were unable to determine that the customer support officer validated and assessed the request before execution.
C126	**2.1.2**	**Classification of tickets** Customer can enter tickets (bug, incident, service request, change request) in the support portal. The Customer Support Officer will assess and classify the ticket and assign it to the proper support group. Customer will be notified by e-mail about the registration of the ticket and can check any updates in the portal.	We have inspected a sample of tickets requested by clients within the ITSM system to determine whether these tickets have been assessed and classified by the Customer Support Officer. Furthermore, determined whether the customer is notified by e-mail about the registration of the ticket and updates are provided within the portal.	No exceptions noted.
C102	**2.1.3**	**Annual check on Separate DTAP environments**	We inspected the implementation of DTAP	No exceptions noted.

		CERRIX has implemented separate environments for development, testing, acceptance and production. The system administrator creates and releases the environments to the clients. The acceptance environment is available for clients if (contractually) agreed upon.	environments to determine whether CERRIX has implemented separate environments for development, testing, acceptance and production for client environments.	
C94	**2.1.4**	**Code reviews on programmed solutions** When a developer finished a change/bug ticket, a reviewer will assess the code based on the CERRIX coding conventions. Outcome is discussed between coder and reviewer. If outcome is positive, the code is committed to source control and the name of the reviewer is added.	We inspected the implementation of the enforced check within the DevOps environment of CERRIX to determine whether CERRIX has implemented an enforced check which ensures that a reviewer needs to assess the code. the DevOps environment records the name of the reviewer and, in case of a negative outcome, sends the ticket back to the initial developer to resolve.	No exceptions noted.
C95	**2.1.5**	**Functional test of developed solutions** The tester compares the developed solution with the Azure DevOps change request. If ok, the Azure DevOps ticket status will be updated to "testing - done" for Azure DevOps. If the developed solution does not meet the requirements as stated in Azure DevOps, the ticket status will be set to 'ready for dev' for Azure DevOps with additional comments for the developers.	We inspected a sample of functional tests on developed solutions to determine whether tests have been performed by a test engineer of CERRIX for change requests. In addition, per inspection we determined whether the test engineer has changed the ticket status to “done” or “ready4dev” dependent on the result of the test.	No exceptions noted.

C93	**2.1.6**	**Regression tests for each production release** Every new release is subject to regression testing before deployment to customers. Software Testers execute a regression test based on the regression test plans. Regression testing is performed in a CERRIX test environment. Results are registered in Azure DevOps. If errors occur in regression test, development will be notified of the errors via Azure DevOps tickets and solutions will be developed. The solutions will be retested.	We inspected a sample of regression tests performed to determine whether regression testing has been performed by CERRIX for each release before deployment and test results were registered within Azure DevOps.	No exceptions noted.
C125	**2.1.8**	**Review and communication of Release Notes** With each new release, release notes are created by the Product Owner based on the items in the sprint. The release notes are published in CERRIX with each release.	We inspected a sample of release notes to determine whether release notes have been created by the Product Owner based on the items in the sprint and published in CERRIX.	No exceptions noted.

4.1.3 Incident & Problem Management

Control objective: All incidents and problems are adequately reported, registered and classified.

Controls for Incident & Problem Management				
CERRIX ID	**#**	**Controls**	**Testing PwC**	**Test results PwC**
C127	**3.1.1**	**Review of client accounts** All clients are given one or more account(s) to report tickets in the customer portal. The customer support officer reviews every half year if all CERRIX clients have an account. If there are clients without an account, the Support Officer will create additional accounts for these clients. If accounts are no longer valid, the accounts will be deleted.	We inspected a half yearly client account review to determine whether the customer support officer reviewed the CERRIX client accounts within the customer portal. Furthermore, determined whether the Support Officer created or deleted accounts based on the review.	No exceptions noted.

4.1.4 Security Management

Control objective:
Information security policy / code of conduct is up to date and communicated to relevant parties.

Controls for security management				
CERRIX ID	**#**	**Controls**	**Testing PwC**	**Test results PwC**
C7	**4.1.1**	**Annual review and distribution of the Strategic Information Security Policy** Annually, or in case of significant changes to the ISMS, the Strategic Information Security Policy is reviewed by the CTO and updated if necessary. At least the following things will be checked: - The information security principles. - The information security objectives. - The key roles and responsibilities for information security. - The high level information security policies. The new version is approved by the CERRIX CEO. The newly approved version is distributed to all personnel. All personnel will digitally confirm he/she has read and will comply to the Information Security Policy..	We inspected the signed information security policy and evidence of its distribution to determine whether the information security policy is updated and confirmed by all personnel.	Exception noted: Based on our inspection and inquiry, we note that there are no criteria defining the timeliness of the distribution of the information security policy. The information security policy was not distributed within the audit period.
C22	**4.1.2**	**Annual review and distribution of the Code of Conduct** Annually, the CTO reviews and updates the Code of Conduct according to the latest developments. The new version is approved by the CEO. The newly approved Code of Conduct is distributed to all CERRIX personnel and all CERRIX personnel need to digitally confirm he/she has read and will comply to the Code of Conduct.	We inspected the signed code of conduct and evidence of its distribution to determine whether the information security policy is updated and confirmed by all personnel.	Exception noted: Based on our inspection and inquiry, we note that there are no criteria defining the timeliness of the distribution of the code of conduct. The code of conduct was not distributed within the audit period.

Control objective:
User access is limited to users based on their function.

Controls for security management				
CERRIX ID	**#**	**Controls**	**Testing PwC**	**Test results PwC**
C35	**4.2.1**	**Authorization request procedure** All requests for adding/changing/revoking users and/or authorizations are submitted in a CERRIX Form and assessed by the Security Officer. Only exceptions on the SOLL-matrix require the approval of the Managing Director. Regular changes that are in line with the SOLL-matrix will be sent to the System Administrator for execution.	We have inspected a selection of CERRIX forms to add, change, or revoke user access to determine whether the authorisations are assessed by the security officer.	No exceptions noted.
C36	**4.2.2**	**Annual review of the SOLL-matrix** Annually, a review of functional descriptions including needed user authorizations (registered in the SOLL-matrix) is performed by the Manager Operations and/or CTO within a CERRIX Form. If deficiencies are found a new version of the SOLL-matrix will be issued and communicated to all stakeholders.	We inspected the annual review of user accounts and user rights in the SOLL-matrix to determine whether the Manager Operations and/or CTO of CERRIX performed this review. Furthermore, determined whether deficiencies have been remediated in a new version of the SOLL-matrix which is communicated to relevant stakeholders.	No exceptions noted.
C144	**4.2.3**	**Annual comparison of the actual situation (IST) to the desired situation (SOLL)** Annually, the actual user authorizations are compared to the authorizations in the SOLL-matrix by the Security Officer. Deficiencies are discussed with the Manager Operations or CTO. If changes are required, in the SOLL-matrix or in the authorizations of the user (IST-matrix), Results are documented within a control execution in CERRIX.	We inspected the annual comparison of the SOLL-matrix to the actual user authorizations to determine whether the security officer of CERRIX performed this review. Furthermore, determined whether deficiencies were discussed with the Manager Operations or CTO and resolved.	No exceptions noted.
C38	**4.2.4**	**Annual review of personal and non-personal accounts** All CERRIX employees have a personal user account and unique	We inspected the annual review of personal user accounts and non-personal user	No exceptions noted.

		password. Non-personal accounts are registered by the Security Officer including rights and reason of usage. Annually, the Security Officer reviews if the non-personal accounts are still necessary and if the necessary non-personal accounts are used for the purpose stated and not for other reasons. If issues occur, they are discussed with the Manager Operations and remediating actions are taken if necessary. Results are documented within a control execution in CERRIX.	accounts to determine whether the Security officer performed this review. Furthermore, determined whether remediating actions have been performed if required.	

C78	**4.2.5**	**Limited access for Administrators** Every quarter a check is performed on administrator accounts. Only DevOps team members and the CTO should have administrator rights.	We have inspected a sample of checks on the administrator access in Microsoft Entra-ID to determine whether only the DevOps team and CTO have administrator rights.	Exception noted: For three of our three selected samples, we note that a check was performed on active assignments, as opposed to eligible assignments, therefore we cannot determine that only the DevOps team and the CTO could request administrator rights.
C87	**4.2.6**	**Logging of Administrator actions on client environments** Whenever administrator actions are necessary on client environments, the DevOps team has to do a PIM request to elevate their user rights before they are allowed to access the client database. All PIM requests are reviewed by the CTO, logged and checked on validity. If necessary, appropriate actions are taken.	We performed inquiry with the CTO to determine how the requests to administrator access are logged. In addition, we inspected a sample of PIM requests to determine whether all PIM requests are reviewed by the CTO, logged and checked on validity. If necessary, appropriate actions are taken.	Exception noted: Based on inquiry we determined that no control was implemented as described to log administrator access before August 2024.

Control objective:
Information security solutions are implemented and operated consistently throughout the enterprise to ensure secure client services and data.

Controls for security management				
CERRIX ID	**#**	**Controls**	**Testing PwC**	**Test results PwC**
C92	**4.3.1**	**Conduct SSL scan** Semi-annually, the Security Officer performs an SSL scan to determine if connection to client environments are adequately secured (Data in-transit encryption). If deficiencies are discovered, the SSL certificates will be updated.	We inspected a half-yearly SSL scan to determine whether the security officer performed SSL scans to determine if client environments are adequately secured. Furthermore, determined whether deficiencies have been resolved.	No exceptions noted.
C79	**4.3.2**	**Client CERRIX environment IP Whitelisting check** Semi-annually, a check is performed by the Security Officer on client authorized IP-ranges as stated in their requirement documents versus the current IP-ranges in the list on the production environments.	We inspected a half-yearly check on the client environment IP whitelisting to determine whether the security officer performed IP whitelisting checks to determine if authorized IP-ranges in requirement documents agree to the current IP-ranges in use within CERRIX.	No exceptions noted.
C93	**4.3.3**	**Secure storage of private keys** The passwords for generating certificates are stored at a secure location (last pass). Private keys and certificates for connections (SSL) are stored in the Azure Key Vault.	We inspected the secure storage of private keys to determine whether procedures have been implemented by CERRIX that store the passwords for generating certificates in last pass. Furthermore, determined whether the same is true for private keys and certificates for	No exceptions noted.

			connections within the Azure Key Vault.	
C79	**4.3.4**	**Annual check on password requirements** Annually, the Security Officer checks if password requirements for Azure meet the information security policy requirements for critical applications. If necessary, adjustments will be made accordingly.	We inspected the annual check on password requirements to determine whether the security officer performed a review to determine if password requirements for Azure meet the requirements for critical applications within the security policy.	No exceptions noted.
C80	**4.3.5**	**Client CERRIX environment file extension check & Intrusion protection module** Annually, The Security Officer checks if the Intrusion Protection Module allows only the upload by the client approved file extensions by matching the file extensions from the client's requirements document to the IPM settings for the environments of the client.	We inspected the annual file extension & intrusion protection module check to determine whether the security officer determined if the intrusion protection module of client's environments allow only the client approved file extensions.	No exceptions noted.
C108	**4.3.6**	**CERRIX clients have separate databases** Twice a year, DevOps checks if all client databases are separated. Each client has its own database which can only be reached by the client through the Azure App Service. Exceptions are reported to the CTO.	We inspected a half-yearly check to determine whether DevOps checked if databases are separated and each client has its own database which can be reached through the Azure App Service. Furthermore, determined whether exceptions have been reported to the CTO.	No exceptions noted.
C98	**4.3.7**	**Penetration tests at planned intervals or high risk releases** Annually or after a high risk release, an independent party performs a penetration test. If deficiencies are	We inspected the results of the penetration test to determine whether an independent party performed a	No exceptions noted.

		discovered a plan with measures of improvement will be created and implemented by the responsible within the CERRIX organization.	penetration test. Furthermore, determined whether measures of improvement have been created for deficiencies identified.	
C109	**4.3.8**	**Annual check of Data at rest encryption of client databases** Transparent Data Encryption on database level is enabled for all client databases (Data-at-rest encryption). Annually, a check is conducted if the database encryption is still enabled.	We inspected check performed on the Azure settings showing the data at rest encryption for client databases to determine whether the information security officer performed an annual check and verified if database encryption has been enabled.	No exceptions noted.
C27	**4.3.9**	**Monitoring of NCSC security issues** On event, The Information Security Officer monitors the security issues communicated by the NCSC. If an event is relevant and deemed high risk for CERRIX, the issue is sent to the CTO. If needed, the issue can then be followed up in the Management Team.	We inspected a selection of sign-offs in CERRIX to determine whether the information security officer verified quarterly that no relevant high-risk NCSC security issues were communicated. We inspected the security issues communicated by the NCSC during the year. As no relevant security issues occurred, no testing could be performed by PwC over the follow up by the management team.	Non-occurrence.
C172	**4.3.10**	**Annual check on two factor authentication on all CERRIX accounts** Two factor authentication is required on all CERRIX accounts. Once a year compliance with this policy will be checked.	We inspected the annual check on two factor authentication to determine whether the information security officer performed a check to determine if the two factor	No exceptions noted.

			authentication policy has been enabled for all CERRIX accounts.	

4.1.5 Monitoring of external suppliers

Control objective:
Suppliers are monitored on operational and information security aspects.

Controls for service level management and monitoring

CERRIX ID	#	Controls	Testing PwC	Test results PwC
42	**5.1.1**	**Annual review of High Risk suppliers** Annually, all service providers that are labeled as 'Important' or 'Critical' are evaluated and reviewed by the CTO on operational- and information security performance. This may include: - SLA validity and performance - Security certifications e.g. ISO27001 - SOC 2 reports - Incidents	We have inspected evidence of review of all service providers labeled "Important" or "Critical" by Cerrix to determine whether these service providers are evaluated and reviewed on operational- and information security performance by the Manager Operations and/or the CTO.	Exception noted: We have not been able to establish that third party assurance reports of Azure and Office 365, and EightFence have been evaluated and reviewed on operational security performance during 2024.
74	**5.1.3**	**Monitoring of Azure resources** The Managing Director monitors the uptime of client environments quarterly via the uptime monitor If uptime is outside parameters a message will be sent to the Slack channel. Azure will resolve as much issues as possible. Exception issues causing major time-outs will be added as an operational incident in the CERRIX event database and followed up.	We performed inquiry with the CTO to determine whether the uptime of client environments is monitored on a quarterly basis via the uptime monitor.	Exception noted Based on inquiry we determined that this control is no longer performed in 2024.
C44	**5.1.4**	**Quarterly check on general service incidents** Azure reports general Service incidents & Security advisories via their Service Health dashboard. The CTO analyses quarterly if there are important items and performs follow up if necessary.	We inspected evidence of the review of a sample of Service Health Dashboards to determine whether these are analysed and followed up by the CTO.	Exception noted We noted that the analysis and review over the first quarter is not documented.
43	**5.1.5**	**Monitor validity of Azure DevOps service level agreement** The Managing Director monitors the validity of the service level agreement of the critical suppliers annually. If needed, he/she will update service level agreement with new requirements. This currently includes: - Microsoft Azure	We inspected the annual review to determine whether the Managing Director monitored the validity of the service level agreement of Microsoft Azure. Furthermore, determined whether an update to the service level	No exceptions noted.

			agreement was required.	

4.1.6 Business Continuity Management

Control objectives:
Business disruptions are mitigated timely and completely.

Controls for Business Continuity Management				
CERRIX ID	**#**	**Controls**	**Testing PwC**	**Test results PwC**
C47	**6.1.1**	**Annual review of the Business Continuity Plan** Annually, the Information Security Officer and/or CTO reviews the Business Continuity Plan for changes based on outcomes of Business Recovery Tests, changes in best practices and changes within CERRIX. When necessary a new version is created and sent to the Managing Director for approval. After approval the new version of the Business Continuity Plan will be communicated to all relevant stakeholders within CERRIX.	We inspected the business continuity plan to determine whether it is reviewed Security Officer and/or CTO reviews the Business Continuity Plan for changes based on outcomes of Business Recovery Tests/ICT readiness assessments, and communicated to relevant stakeholders.	Exception noted: Based on inspection we were not able to establish that the outcomes of Business Recovery Tests/ICT readiness assessments were used to update the plan. In addition, we were not able to establish that the BCP was shared to stakeholders in a timely manner.
C116		**Business Recovery Test** Annually a test of our Business Continuity Plan is executed to verify its effectiveness in maintaining or restoring critical business operations during and after a disruptive incident. The test will simulate a realistic scenario aligned with identified risks.	We inspected the results of the annual business recovery test to determine whether the test of the business continuity plan was performed by CERRIX and documented.	No exceptions noted.

SECTION 5: Management response on auditor findings

The table below contains Management's response to the exceptions identified in SECTION 4: Control framework and auditor findings.

CERRIX ID	Control description	Test results PwC	Management Response
C103	Changes are requested via the ITSM system of CERRIX. Clients can request a change via the customer portal and involved CERRIX employees can request changes directly in the backend of the ITSM system. The customer support officer will validate the request and make sure the request is clear and updated with relevant information. Change Requests will be assessed and approved before they are executed. The assessment will contain an assessment of the impact on Information Security. The ticket is updated with applicable information security impact and the approval.	For 6 out of 30 selected change requests within the ITSM system, we were unable to determine that the customer support officer validated and assessed the request before execution.	All tickets, including Change Requests are validated by the customer support officer. Change Requests are also validated by the Change Advisory board. Due to the use of a new ticket system and a new Customer Support Officer, the evidence of this check was not always stored correctly.
C7	Annually, or in case of significant changes to the ISMS, the Strategic Information Security Policy is reviewed and updated by the CTO and updated if necessary. At least the following things will be checked: - The information security principles. - The information security objectives. - The key roles and responsibilities for information security. - The high level information security policies. The new version is approved by the CERRIX CEO. The newly approved version is distributed to all personnel, All personnel will digitally confirm he/she has read and will comply to the Information Security Policy.	Based on our inspection and inquiry, we note that there are no criteria defining the timeliness of the distribution of the information security policy. The information security policy was not distributed within the audit period.	We acknowledge this finding, however the Strategic Information Security policy received a major update and was distributed to all employees though not within a agreed timeline.
C22	Annually, the CTO reviews and updates the Code of Conduct according to the latest developments. The new version is approved by the CEO. The newly approved Code of Conduct is distributed to all CERRIX personnel	Based on our inspection and inquiry, we note that there are no criteria defining the timeliness of the distribution of the code of conduct. The code of conduct was not	We acknowledge this finding, however the Code of Conduct received a major update and was distributed to all employees

	and all CERRIX personnel need to digitally confirm he/she has read and will comply to the Code of Conduct.	distributed within the audit period.	though not within a agreed timeline.
C78	Every quarter a check is performed on administrator accounts. Only the DevOps team and the CTO should have administrator rights.	For three of our three selected samples, we note that a check was performed on active assignments, as opposed to eligible assignments, therefore we cannot determine that only the DevOps team and the CTO could request administrator rights.	We acknowledge that the evidence for the first quarter was not correct but the control was executed and found correct.
C87	Whenever administrator actions are necessary on client environments, the DevOps team has to do a PIM request to elevate their user rights before they are allowed to access the client database. All PIM requests are reviewed by the CTO, logged and checked on validity. If necessary, appropriate actions are taken.	Based on inquiry we determined that no control was implemented to log administrator access before August 2024.	We acknowledge this, however, after the same finding in 2023 we invested in setting up Privileged Identity Management and from august 2024 this is active and performed correctly.
C42	Annually, all service providers that are labeled as 'Important' or 'Critical' are evaluated and reviewed by the CTO on operational- and information security performance. This may include: - SLA validity and performance - Security certifications e.g. ISO27001 - SOC 2 reports - Incidents	We have not been able to establish that third party assurance reports of Azure and Office 365, and EightFence have been evaluated and reviewed on operational security performance during 2024.	We acknowledge this finding however, Eightfence is not classified as critical and Office 365 will also not be critical in 2025. SOC2 reports for Azure and Azure DevOps have been evaluated but later than expected and too late for this report.
C74	The Managing Director monitors the uptime of client environments quarterly via the uptime monitor If uptime is outside parameters a message will be sent to the Slack channel. Azure will resolve as much issues as possible. Exception issues causing major time-outs will be added as an operational incident in the CERRIX event database and followed up.	Based on inquiry we determined that this control is no longer performed in 2024.	We acknowledge this finding however, this control has been superseded by near real time monitoring of uptime/downtime of environments thus improving response times.
C44	Azure reports general Service incidents & Security advisories via their Service Health dashboard. The CTO analyses quarterly if there are important items and performs follow up if necessary.	We noted that the analysis and review over the first quarter is not documented.	We acknowledge this finding. Evidence was not correctly stored but control was executed.

C47	Annually, the Information Security Officer and/or CTO reviews the Business Continuity Plan for changes based on outcomes of Business Recovery Tests, Changes in best practices and changes within CERRIX. When necessary a new version is created and sent to the Managing Director for approval. After approval the new version of the Business Continuity Plan will be communicated to all relevant stakeholders within CERRIX.	Based on inspection we were not able to establish that the outcomes of Business Recovery Tests/ICT readiness assessments were used to update the plan. In addition, we were not able to establish that the BCP was shared to stakeholders in a timely manner.	The Business Continuity Plan received a major update and we reinstated the control for business continuity testing by doing relevant disaster recovery simulations and table top exercises. This is actually a major improvement over previous years. The only thing that is missing is evidence that test results have been used to update the BCP.