Ubeeo | Maaskade 120, 3071NK Rotterdam | +31 10 820 29 10 | info@ubeeo.nl |ubeeo.nl

ISAE-3000

IT SERVICE ORGANIZATION CONTROL REPORT BASED ON THE SOC 2® REPORT MODEL AND THE TRUST SERVICES PRINCIPLES AND CRITERIA

RELEVANT TO: SECURITY, AVAILABILITY, PROCESSING INTEGRITY, CONFIDENTIALITY AND PRIVACY TYPE II

Scope:	Applicant Tracking System Platform and Supporting Services delivery
Period:	November 1, 2023 to April 30, 2024
Reference:	RE202405-01

MATHISON

ubeeo

Contents

I. Introduction

Ubeeo is a software company that focuses on making the recruitment process of organizations more efficient and effective. To achieve this, Ubeeo develops and supplies recruitment software solutions that are user-friendly and reliable and can be intelligently integrated with the customer's website.

Ubeeo's software solutions facilitate, among other things:

- creating and publishing vacancies;
- receiving and processing applications;
- anonymizing applications after the retention period;
- removing anonymized data as soon as it is no longer relevant for reporting;
- generating reports to analyze and improve the customer's recruitment process using Business Intelligence software;
- providing links where data is transferred from and to the customer's internal systems such as HR systems and Business Intelligence software;
- providing links where data is transferred from and to external systems used by the customer, such as online assessment tests or online video interview software.

Ubeeo strives for the smoothest possible recruitment process for both the recruiter and the candidate. The customer as an employer must present himself as best as possible.

Ubeeo is located in Rotterdam.

1 Management's Assertion

We have prepared the description in the section titled, "Ubeeo" description of its Ubeeo Applicant Tracking System Platform and Supporting Services delivery, based on the criteria below (the description criteria). The description is intended to provide users with information about the Ubeeo Applicant Tracking System Platform and Supporting Services delivery, particularly system controls intended to meet the criteria for the security and availability principles (applicable trust services criteria) set forth in TSP section 100A, Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy issued by the American Institute of Certified Public Accountants (applicable trust services criteria).

We confirm, to the best of our knowledge and belief, that the description fairly presents Ubeeo's Applicant Tracking System Platform and Supporting Services delivery throughout the period November 1, 2023 to April 30, 2024 based on the following description criteria:

1) The description fairly presents Ubeeo's Ubeeo Applicant Tracking System Platform and Supporting Services delivery throughout the period November 1, 2023 to April 30, 2024 based on the following description criteria:

    a) The description contains the following information:

        i) The types of services provided.

            (1) The components of the system used to provide the services, which are the following:

            (2) Infrastructure. The physical and hardware components of a system (facilities, equipment, and networks).

            (3) Software. The programs and operating software of a system (systems, applications, and utilities).

            (4) People. The personnel involved in the operation and use of a system (developers, operators, users, and managers).

            (5) Procedures. The automated and manual procedures involved in the operation of a system.

            (6) Data. The information used and supported by a system (transaction streams, files, databases, and tables).

        ii) The boundaries or aspects of the system covered by the description.

        iii) The role of the subservice organization and other parties the procedures performed to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

        iv) The applicable trust services criteria and related controls designed to meet those criteria.

v) How the system captures and addresses significant events and conditions.

vi) The process used to prepare and deliver reports and other information to user entities or other parties.

vii) Any applicable trust services criteria that are not addressed by a control at the service organization and the reasons, therefore.

viii) Other aspects of the service organization's control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria.

2) Ubeeo uses GTT EMEA Ltd for main cloud and infrastructure solutions, Microsoft365 as an identity provider and office workspace services, Atlassian Confluence for technical documentation and Bitbucket code repository services. Management of Ubeeo has chosen the carve-out method to address the services provided by these subservice organizations as mentioned in paragraph Complimentary Subservice Organization Controls. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Ubeeo to achieve the Ubeeo's service commitments and system requirements based on the applicable trust service criteria. The description does not include the actual controls at the subservice organizations.

3) The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

a) The controls stated in the description were suitably designed and implemented throughout the period November 1, 2023 to April 30, 2024 to meet the applicable trust services criteria.

b) The controls stated in the description operated effectively throughout the period November 1, 2023 to April 30, 2024 to meet the applicable trust services criteria.

Rotterdam, 5/7/2024

Ubeeo

DocuSigned by:

6204481E241D40E...

S.L. Buijsman

CEO

2 Independent service auditor's report

To: the Management of Ubeeo

2.1 Opinion

Our opinion has been formed on the basis of the matters outlined in this report. In our opinion, in all material respects, based on the criteria identified in Ubeeo's assertion and the applicable trust services criteria:

1) The description in chapters 3 and 4 fairly presents the Management System of Ubeeo Applicant Tracking System Platform and Supporting Services delivery that was designed and implemented throughout the period November 1, 2023 to April 30, 2024;
2) The controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period November 1, 2023 to April 30, 2024, and user entities applied the complementary user-entity controls contemplated in Ubeeo's Description of its Ubeeo Applicant Tracking System Platform and Supporting Services delivery, throughout the period November 1, 2023 to April 30 2024;
3) The controls tested, which together with the complementary user-entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the applicable trust services criteria were met; operated effectively throughout the period November 1, 2023 to April 30 2024.

The specific controls we have tested, and the nature, timing, and results of our tests are presented in chapter 4 of this report.

2.2 Scope

We have been engaged to obtain reasonable assurance and report on the attached description titled "Ubeeo's description of its Ubeeo ATS System" throughout the period November 1, 2023 to April 30 2024 (the description) and the suitability of the design and implementation of controls to meet the criteria for the security, availability, processing integrity, confidentiality and privacy principles set forth in TSP Section 100 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022) issued by the American Institute of Certified Public Accountants (applicable trust services criteria).

The description indicates that certain applicable trust services criteria specified in the description can be achieved only if complementary user-entity controls contemplated in the description are suitably designed and implemented. We have not evaluated the suitability of the design or operating effectiveness of such complementary user-entity controls.

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. Also, because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

Ubeeo uses GTT EMEA Ltd for main cloud and infrastructure solutions, Microsoft365 as an identity provider and office workspace services, Atlassian Confluence for technical documentation and Bitbucket code repository services. Management of Ubeeo has chosen the carve-out method to address the services provided by these subservice organizations as mentioned in paragraph Complimentary Subservice Organization Controls. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Ubeeo to achieve the Ubeeo's service commitments and system requirements based on the applicable trust service criteria. The description does not include the actual controls at the subservice organizations.

2.3 Service Organization's Responsibilities

Ubeeo has provided the attached assertion titled "Management Assertion" which is based on the criteria identified in management's assertion. Ubeeo is responsible for:

- Preparing the description and assertion;
- The completeness, accuracy, and method of presentation of both the description and assertion;
- Providing the services covered by the description;
- Specifying the controls that meet the applicable trust services criteria and stating them in the description; and
- Designing, implementing, and documenting the controls to meet the applicable trust services criteria.

2.4 Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria set forth in Ubeeo's assertion and on the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria, based on our procedures to obtain reasonable assurance. We conducted our assurance engagement in accordance with Dutch Law and the International Standard on Assurance Engagements Standard 3000, 'Assurance Engagements other than Audits or Reviews of Historical Financial Information' established by The International Auditing and Assurance Standards Board (IAASB). Those standards require that we plan and perform our engagement to obtain reasonable assurance to express our opinion.

We have complied with the independence and other ethical requirements of the Code of Ethics ('Reglement Gedragscode') issued by NOREA, the Dutch IT-Auditors institute, which is founded on fundamental principles of integrity, objectivity, professional competence, and due care, confidentiality, and professional behavior.

Mathison applies the NOREA Standard on Quality Control (Reglement Kwaliteitsbeheersing NOREA –RKBN), 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. Our assurance engagement involved performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria and the suitability of the design and operating effectiveness of those controls to meet the applicable trust services criteria.

Our procedures depend on the service auditor's judgment and included assessing the risks that the description is not fairly presented and that the controls were not suitably designed to meet the applicable trust services criteria. Our procedures also included evaluating the overall presentation of the description.

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

2.5 Inherent limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls my become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

2.6 Description of Test of Controls

The specific controls we have tested, and the nature, timing, and results of those tests are presented in chapter 4 of this report.

2.7 Restricted use

This report and the description of tests of controls and results thereof are intended solely for the information and use of user entities of "Ubeeo's Applicant Tracking System Platform and Supporting Services delivery" throughout the period November 1, 2023 to April 30 2024; and independent auditors and practitioners providing services to such user entities who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization;
- How the service organization's system interacts with user entities, subservice organizations, and other parties;
- Internal control and its limitations;
- Complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria;
- The applicable trust services criteria;
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

This report is not intended to be and should not be used by anyone other than these specified parties.

Capelle aan den IJssel, 5/7/2024

Mathison B.V.

DocuSigned by:

Leo Benschop

CF1DDADBE1F747E...

L.A.T. Benschop

Director of Mathison

3 Ubeeo's description of the ATS System

3.1 Ubeeo Background

Jeremy Ovenden starts building an Internet Candidate Management System in 1997 in the United Kingdom and names it iCams. Two years later the product is offered as a service. In 2004 Leon Buijsman starts distributing the product in the Netherlands and formally founds Hireserve BV in 2007. Leon Buijsman becomes co-owner next to Jeremy Ovenden. In 2007 the product is completely rebuilt. After that the software is completely modular and meets the strictest safety requirements. In the same year Hireserve Ltd onboards its first employee and Hireserve BV follows one year later. In the following years both Hireserve Ltd and Hireserve BV grow in number of customers and employees. Until on June 23, 2016, United Kingdom votes in favor of Brexit. In anticipation of Brexit Hireserve BV opens a datacenter in the Netherlands in 2017.

In 2018 Hireserve BV has 12 employees when it is formally split from Hireserve Ltd. Leon Buijsman becomes fully owner of Hireserve BV. In 2019 Hireserve moves into a bigger office in Rotterdam and the ISO 27001 certificate is obtained. When the marketing agreement ends in 2021, Hireserve BV changes it trading name to Ubeeo and obtains the ISO-9001 certificate. In 2022, Ubeeo is listed in the Main Software 50 Benelux and expands its certifications to ISO-27017 and ISO-27018. In 2023, Ubeeo is listed FD Gazelle 2023 employs 27 people and has become one of the most chosen corporate recruitment systems within the Netherlands. Ubeeo operates within different branches such as education, healthcare, government, and retail.

Ubeeo has the following mission:

Building and selling recruitment software to support the entire recruitment and selection process. For our clients and their candidates.

In our vision we distinguish four important pillars:

1) Providing robust technology
2) Always in flux
3) Offering endless possibilities
4) Being a partner instead of a supplier

To realize our mission within this context, we pursue the following strategy:

- Responding to developments in the field of increased security awareness;
- Providing intuitive technology;
- Be available on any device;
- Provide integration with social media where possible;
- Candidates must be able to apply simply and quickly;
- Offer standard connections with best-of-breed solutions;
- Provide simple integration with content management systems;
- Measuring is knowing.

3.2 Description of Services Provided

The services included in Ubeeo ATS Platform and supporting Services delivery are the following functionalities that enable:

1) Publishing vacancies and events on client intranet and internet webpages.
2) Publishing vacancies to external websites through direct integrations with jobboards (a.o. LinkedIn, Monster, Indeed, Talent.com) and integrations with jobmarketing agencies (a.o. Mimir, AdverOnline, Brockmeyer).
3) Tracking and processing applications and bookings of candidates, including support for:
   a) Planning job interviews: recruiters can send Outlook-like invitations to candidates and interviewers from Ubeeo ATS or the candidate can select from available interview slots.
   b) Candidate selection: supporting managers and selection committees with selection of candidates.
   c) Online assessments: include integration with online assessment (cognitive ability tests, personality tests, skills tests, and situational judgment tests).
   d) Employment conditions proposal: Companies can draw up an employment conditions proposal in Ubeeo ATS.
4) Matching: Ubeeo analyzes which candidate in the candidate database best suits a new vacancy.
5) Referrals: If employees do not want to apply themselves but know a suitable candidate, they can recommend him or her.
6) Integrations: Ubeeo ATS can integrate with different HR systems.

Apart from these core functionalities Ubeeo can also create career websites where candidates can find the companies vacancies and where they can apply. The website is integrated with Ubeeo ATS. Alternatively, Ubeeo ATS can integrate with a website that is created by the company itself.

3.2.1 Service commitments

Ubeeo strives for the smoothest possible recruitment process for both the recruiter and the candidate. The customer as an employer must present himself as best as possible.

Ubeeo customers are data controllers as owners of candidate data. Ubeeo is data processor and processes the data GDPR-proof.

Service commitments include:

- Handling of reported Malfunctions and Security Incidents, which is not attributable to the availability of access to the Internet in general;

- Handling of Defects;
- Handling of Change Requests;
- Handling of Questions.

Notifications are classified into the following priority categories and Notification Groups:

Priority	Notification group	Maximum Response Time	Maximum resolution time
P1	Blocking Incident	Directly	8 hours
	Blocking Incident	Directly through LiveChat / Phone Other channels 4 Working hours	8 hours after processing Notification
	Serious incident	Direct through LiveChat Other channels 4 Working hours	8 Working Hours After Processing Notification
P2	Major Incident	Direct through LiveChat Other channels 4 Working hours	40 Working Hours After Processing Notification
P3	Small Incident	Direct through LiveChat Other channels 4 Working hours	40 Working Hours After Processing Notification
P4	Small change request	4 Working Hours	40 Working Hours After Processing Notification
P5	Change request	4 Working Hours	In consultation
P6	Small Change Request (unpaid)	Not applicable	Not applicable
P7	Product development	Maximum Response Time	Maximum Response Time
P8	Question	Directly through LiveChat Other channels 4 Working hours	Directly through LiveChat Other channels 8 Working hours

Customers can view the availability of the system environment per day, per month and the past 90 days via the Status Page (https://status.ubeeo.nl).

At the customer's request, Ubeeo provides a quarterly JIRA ServiceDesk report. This report contains the number of Reports and resolved Reports within and outside the maximum resolution times per month.

3.2.2 System requirements

Based upon the commitments, the following system requirements are strived for:

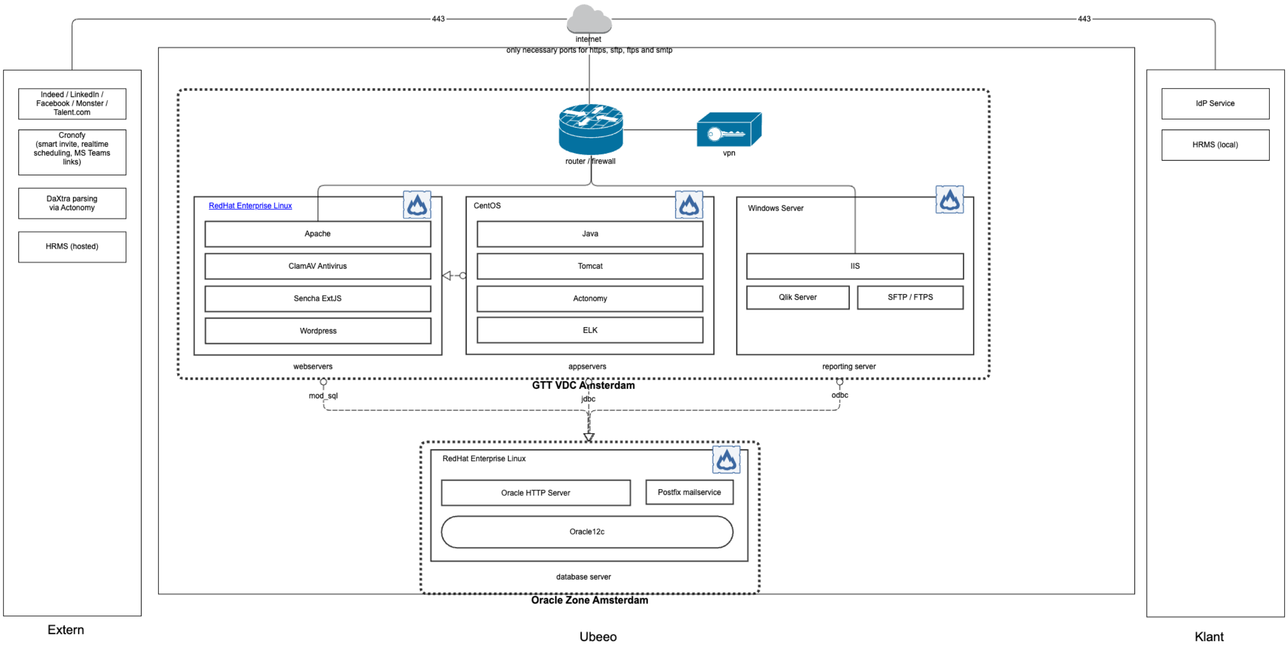
- Risk assessments are performed to determine the necessary controls.
- Customer data is not distributed to persons who have not been granted access rights to the data.
- Customer data entrusted to Ubeeo may not be changed undesirably.
- The backup policy ensures that the maximum data loss (MGV) is not exceeded.
- Providing a secure, managed and monitored cloud environment.
- Suppliers are monitored to maintain quality and security in outsourced processes.
- DPA's are signed with suppliers that process personal client data.
- Compliance with applicable personal data protection laws.
- Compliance with contractual agreements regarding information security.
- The customer is enabled to use the software in a safe manner and in accordance with the GDPR guidelines.

3.3 Components of the system

The following subsections describe the components of Ubeeo's software and services in terms of Infrastructure; Software; People; Procedures; and Data.

The description in the following Infrastructure subsection is limited to those hardware and network components that are relevant to the provision of Ubeeo ATS platform and supporting service delivery.

3.3.1 Infrastructure



The Ubeeo ATS infrastructure is managed by hosting provider GTT:

1) Dedicated encrypted database server in GTT Schiphol datacenter running an Oracle database;

2) Virtualized servers in GTT VDC Amsterdam which serve as:
    a) Linux servers which proxy traffic to Ubeeo applications;
    b) Linux servers to run Java microservices;
    c) Linux servers to run matching engine;
    d) Linux servers to run monitoring tools;
    e) Linux servers to run email service;
    f) Linux servers hosting various customer websites;
    g) Windows servers to run business intelligence tools.
3) Firewalls on each server;
4) Firewall on environment (Checkpoint firewall);
5) VPN to access the environment (Checkpoint VPN).

Database back-up follows Oracle recommended RMAN backup procedure (continuous journaling, daily incremental, weekly full backup). The back-up is also stored in a second back-up location (Frankfurt). Virtualized servers are back-uped in VDC.

GTT Schiphol datacenter and Frankfurt co-location are ISO-27001 certified and annually ISAE-3402 / SOC-1 Type II audited.

Microsoft365 (Office365 and Azure AD / Entra services) is ISO-27001 certified and annually SOC-2 Type II audited.

Atlassian (Confluence and Bitbucket) is ISO-27001 certified and annually SOC-2 Type II audited.

3.3.2 Software

The description in this subsection is limited to those software components that are relevant to the provision of Ubeeo ATS platform and supporting service delivery. The emphasis is on outlining the main functionalities and characteristics of the software components in relation to the service commitments and system requirements.

<u>Ubeeo ATS application:</u>

- All applicant tracking data are stored in an Oracle database. The application is divided in three pillars: back office (accessed by company users), front office (accessed by candidates) and integrations (used by internal applications and for third party integrations). Program logic is built with Oracle PL/SQL and Java. JavaScript libraries are used for user interaction and presentation layer.

<u>Ubeeo career websites:</u>

- Career websites built by Ubeeo make use of Wordpress and several plugins to enhanced security, add search filters, and enforce styling.

Sales:

- Sales CRM to register sales leads, quotations, contracts, and invoicing information.

Services - Implementation:

- Monday
  The software tool Monday is used for project management purposes facilitating the implementation and improvement projects of customers.

Services - Support:

- Jira Service Management
  The software tool Jira is used to register, monitor, analyze, respond to, and handle customer requests, incidents, and bugs.
- Intercom
  The software tool Intercom is used to respond to customer chat requests.

Developments:

- Jira
  The software tool Jira is used to register, monitor, analyze, respond to, and handle customer requests, incidents, and bugs.
- Bitbucket
  The software tool Bitbucket is used to storing software code and versioning.
- Duplicator
  The software tool Duplicator is used to create, monitor, and restore back-ups of career websites.

DevOps:

- Elastic Search / Logstash / Kibana (ELK)
  The software tool Kibana is used to monitor the capacity of the Ubeeo ATS infrastructure.
- Solarwinds

  The tool Solarwinds is used to monitor the performance of the Ubeeo ATS.
- SonarQube

  The tool SonarQube is used for Java code scanning (uniformity and weaknesses).
- ClamAV

  Antivirus engine used for scanning documents.
- Outpost24

  The software tool Outpost24 is used to detect and analyze weaknesses in the Ubeeo ATS software.
- Sentry

  The software tool Sentry is used to analyze Ubeeo ATS software errors.

- Uptime Robot

  A software service to monitor service uptime and inform customers / users when service is experiencing issues.

- Selenium

  A playback tool for authoring functional tests across most modern web browsers, without the need to learn a test scripting language.

Internal

- Confluence

  The software tool Confluence is used to document and manage work instructions, system documentation and release notes.

- Base27

  The software tool Base27 is used to inform employees, make processes secure, perform risk assessments and continuously monitor and improve Ubeeo's information security and quality.

- Lastpass

  The software tool Lastpass is used to store and share passwords and to assess if the passwords comply with Ubeeo's password policy.

- Slack

  The software tool Slack is used for alerting and internal communication.

These software tools are all cloud based. The suppliers are responsible for monitoring the uptime, encryption, back-ups and solving incidents. Ubeeo monitors the performance of these suppliers.

3.3.3 People

Ubeeo's staff is involved in the operation of Ubeeo ATS, but in different roles and with different responsibilities. The most important roles in terms of the service commitments are:

- Support employees;
- Implementation consultants;
- Software developers;
- DevOps engineers;
- Management.

Support employees

The Support employees are the first point of contact for customers using the Ubeeo ATS. They deal with incoming requests/incidents by answering them. If a Support employee is unable to answer a request or resolve an incident, it will be passed on to a Developer or DevOps employee. Required skills for Support employees:

- a structured and systematic way of working;

- solid communication skills;
- general system knowledge.

Implementation Consultants
The Implementation Consultants are responsible for implementing Ubeeo ATS for new customers. Required skills for Implementation Consultants:

- A structured and systematic way of working
- Solid communication skills
- General system knowledge

Software developers
Software developers are responsible for analyzing internal and external requests for new Ubeeo ATS functionalities, defining requirements, and writing new software code. Software developers also perform code reviews and tests to make sure new code is secure, written according to Ubeeo's software development policy and results in workable software which complies to the defined requirements. Required skills for Software developers:

- A structured and systematic way of working
- Excellent programming skills
- Thorough system knowledge

DevOps engineers
A DevOps engineer is responsible for the smooth operation of Ubeeo's infrastructure. They work with developers to deploy and manage code changes, and with operations staff to ensure that systems are up and running smoothly. Required skills for DevOps Engineers:

- a structured and systematic way of working
- excellent programming skills
- thorough system knowledge
- thorough understanding op operations processes

Management
Senior management is responsible for overseeing the overall working of Ubeeo's quality and security policies and procedures.

Senior management is supported by an internal audit function for independent periodic auditing and reporting management on compliance status towards company policies, procedures and applicable laws and legislation.

3.3.4 Procedures

Procedures are in place and regularly updated in order to guide employees with their tasks. The procedures are documented in the software tool Base27. Below a general description of the procedures that are relevant for the scope of this SOC report are mentioned.

Human Resource Management
Human resource management communicates a quality and information security policy with employees addressing Ubeeo's core values for integrity and ethical behavior. Each role has a clear responsibility to comply with and attribute to quality and information security.

At the start of the employment each employee requires a certificate of conduct (VOG) issued by the Government of the Netherlands. Employees have acknowledged in writing they have read the contents of and understand the responsibility of their roles with regards to the quality and information security policy.

Acting responsibly, with integrity, respect and professionalism are the four basic ethical principles on which Ubeeo's Code of Conduct is based. These principles apply to all employees. In relation to each other, towards the customer and towards external partners.

Ubeeo's core values are committed, down-to-earth, honest, unconventional, knowledgeable, progressive, intuitive, reliable, and flexible.

Access Management
A role-based authorization matrix has been established to grant employees access to critical and non-critical systems. Quarterly checks are performed to validate authorizations. New employees or employees in new roles are onboarded in accordance with an onboarding procedure and instructions. Access to critical systems is revoked within 24 hours when employees no longer need the assigned rights or leave the organization.

Development operations / DevOps
DevOps is a methodology that has evolved from the experience and best practices of managing the security, development, testing, and support processes in a software development product lifecycle. These practices help Ubeeo manage the development, tools deployment, integrated testing, and assistance with increased productivity and speed.

Monitoring
Ubeeo's application is continuously monitored. In addition to GTT's monitoring tools all executed queries are analyzed using SolarWinds DPA and all systems logs are collected in Elastic and analyzed using a self-developed Kibana dashboard. Automated alerts have been implemented when thresholds are surpassed. A status page has been implemented to inform Ubeeo customers about system performance and provide information in case of performance issues.

Continuity Management
Ubeeo has a business continuity plan in place including roles and responsibilities for handling incidents during adverse situations.

Ubeeo's IT infrastructure and service delivery platform is set up redundantly. Customer data is back-uped following Oracle's recommended RMAN back-up strategy and back-up restore is tested annually.

Software development
The software development procedure ensures that changes in the Ubeeo ATS are prepared and implemented in a controlled manner. The procedure describes the way in which new changes are defined and prioritized and new code is developed and reviewed. The second part of the procedure described the way in which new software is pre-released to the acceptance environment, tested and released in the production environment.

Implementation
Ubeeo implementations are performed according to the Ubeeo Implementation Methodology and do comply with ISO policies and procedures and local GDPR guidelines. Implementations are managed by following the following phases:

- Plan;
- Design;
- Build;
- Test;
- Commissioning;
- Closing;
- Hand over to Support.

Support
Support includes all activities aimed at reacting to support requests from customers using Ubeeo ATS. A support request can be:

- Questions;
- Problems / bugs / malfunctions;
- Change requests;
- Test findings.

Customers can hand in their support request via telephone, email, or chat.

Support requests are classified and prioritized and handled accordingly and within the timelines of the Service Level Agreements. If the request is resolved and the customer is informed the request is closed.

Information security incident management
In case of an information security incident the Managing Director and the Security Officer are informed as soon as possible but at least within 12 hours. An information security incident is an incident with infringement of availability, integrity, or confidentiality. The incident is classified and prioritized and handled accordingly. All

information security incidents are registered in Base27 and analyzed to determine learning points.

Supplier management
Supplier management ensures that the suppliers on which Ubeeo depends on for the supply of its service meet the requirements of Ubeeo. This process consists of determined the quality and information security requirements, checking if the supplier can meet these requirements and collecting the relevant documentation. After a supplier is selected and the supplier is determined critical, the supplier is registered in Base27. All suppliers are monitored, and critical suppliers are also reviewed every year. Part of the review is a documentation check.

Compliancy Management
Ubeeo's quality and security controls are annually audited by an internal and external auditor. Remediation of the mitigating actions is monitored by the Security Officer and discussed in the management team meeting.

Devices containing confidential information are destroyed prior to disposal or are securely wiped prior to reuse. Customer data are stored, anonymized, and destroyed following local GDPR guidelines.

Sales
Ubeeo customers are data controllers as owners of candidate data. Ubeeo is data processor. Our sales organization ensures that Data Processing Agreements are included in sales contracts.

3.3.5 Data

While operating its service delivery, Ubeeo directly or indirectly processes a variety of data. In the context of the Ubeeo ATS, the following types of data are of importance:

Category of data subjects	Purpose of the processing	Type of personal data
• Candidates	• Processing applications through a workflow • Analyzing recruitment processes	• Name, address and place of residence • Phone numbers • E-mail addresses and other addresses for electronic communications • Access or identification data • Gender • Date of birth • Education history • Work history • Curriculum Vitae • List of grades (optional) • Copy of passport / identity card (optional) • Assessment results (optional)
• Users	• Use of the system	• First name • Surname • Gender

Category of data subjects	Purpose of the processing	Type of personal data
	• Analyzing recruitment processes • Use of support	• Business email address • Business phone number • Access or identification data

3.4 Control Environment

3.4.1 Integrity and Ethical Values

The company policy states that employees must behave in accordance with the code of conduct and also try to prevent, identify, and take appropriate measures if violations are found. Employees confirm that they have read, understood, and adhere to the policies and procedures, and the Code of Conduct.

New employees are screened by checking a reference, checking the identification document, checking relevant diplomas and certificates and by requesting a certificate of conduct (VOG).

The responsibilities of each employee are communicated by sharing the ISO management system documentation in Base27.

All managers perform a yearly evaluation with their employees to determine if there are any improvements necessary.

Every employee, including temporary employees and interns, signs as part of their contract a confidentiality agreement.

3.4.2 Ambitions

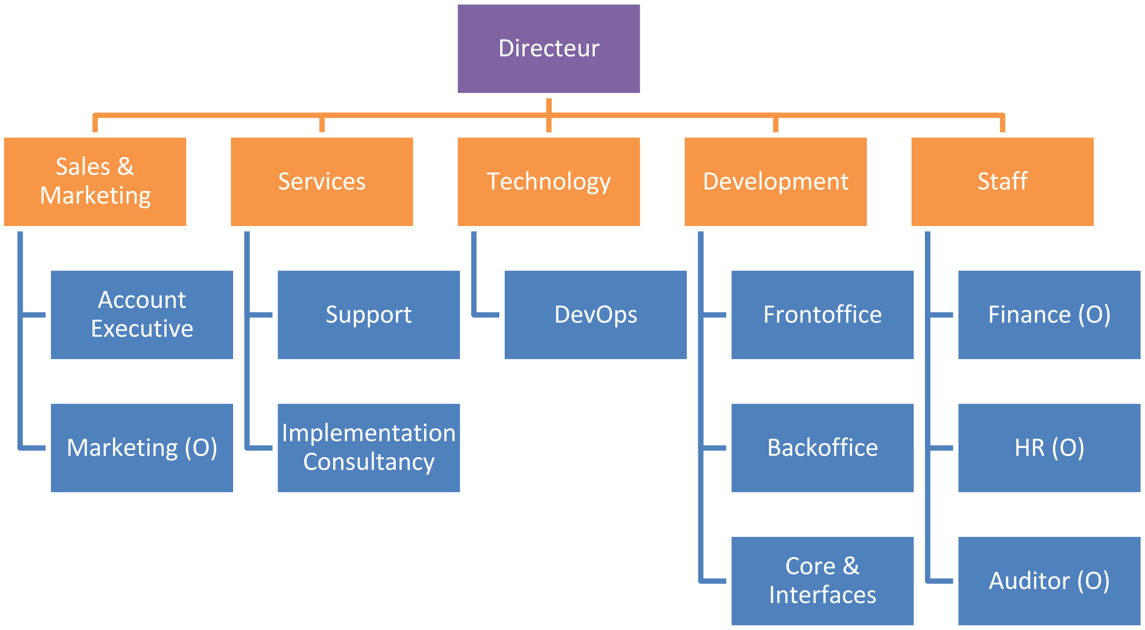
Ubeeo is a service-oriented organization that continuously strives to ensure that every customer can be a reference customer. With a personal approach, Ubeeo implements the best recruitment software solutions together with its customers and thus makes an important contribution to the success of its customers in recruiting and selecting new employees.

Ubeeo's ambition is to make the recruitment process of organizations more efficient and effective. Ubeeo's software should be very user-friendly, secure, and reliable. Given the fact that a lot of personal data of candidates is stored in the application's databases, securing this data is of the utmost importance. In addition to confidentiality, integrity and availability are also important for good customer service.

The management of Ubeeo attaches great importance to an honest, ethical corporate culture. The information security policy states that employees must behave in accordance with the code of conduct and also try to prevent and identify undesirable deviant behavior and take appropriate measures if violations are discovered.

3.4.3 Organizational structure

The structure of the organization is presented in the organization chart below.



(O) = Outsourced

Figure 2. Ubeeo Org chart

The Technology Manager is acting security officer and is responsible for:

- Manage the information security management system;
- Increasing the awareness of employees with regard to information security;
- Make sure the ISO 27001 certification is maintained.

The Privacy Officer is responsible for checking the implementation of GDPR legislation.

The Internal auditor is responsible for checking the quality and information security management system against the ISO standards that Ubeeo has obtained.

The Security Officer, Privacy Officer, and Auditor report to the Managing Director.

3.4.4 Governance structure

The management team is responsible for the management of the organization. The management team consists of the Managing Director, the Services Manager, the Technology Manager, and the Development Manager. The management team determines the organization goals. Each management team member is responsible for reaching the goals that are relevant for their department. The Managing Director is accountable for reaching the organization goals and strategy.

Internal audits are performed every year. The internal auditor reports the findings to the Managing Director and the Service Manager.

External audits are performed every year by the certification body. The external auditor reports the findings to the Managing Director and the Service Manager.

3.5 Risk Management

A risk analysis is performed every year by the Managing Team led by the Technology Manager acting as Security Officer.

During the risk analysis, the possible threats are identified. For each threat, it is examined which existing measures are already in place and which vulnerabilities are possible. The combination of threat, vulnerability and consequences are described as the risk scenario and are recorded as such. For each risk, the probability and impact are estimated. In most cases, risks will be managed by taking measures that reduce the risk.

According to the acceptance criteria it is determined if a risk can be accepted after taking the measures. New measures are determined for the risks that are not accepted. These planned measures are included in the ISO action list by the Services Manager (quality) and Security Officer (security), and an action holder and a deadline are assigned to them.

The Services Manager monitors the progress of the quality measures. The Security Officer monitors the progress of the measures regarding information security.

To evaluate the effectiveness of risk mitigating measures, the total effect is assessed again after their implementation. The residual risk can then be accepted again according to acceptance criteria.

3.6 Communication

The internal organization, legislation and regulations, and the requirements and wishes of external stakeholders are subject to change. There is a risk that the control framework is partially insufficiently aligned with these requirements and is not fully effective. Continuous monitoring of the operation of control measures ensures that vulnerabilities are identified in a timely manner and corrected where necessary. Various internal and external (management) reports are drawn up periodically, which provide insight into and accountability for the functioning of the control system. An overview of the consultations is given below.

Communication structure	Frequency	Description
Management team meeting	Bi-weekly	• Planning; • monitoring information security and quality; • changes with possible impact on information security and quality.
Management review	Yearly	• changes in the context of the organization; • feedback from stakeholders; • results of risk analysis and status of risk treatment plan; • realization of information security objectives; • information security incidents; • supplier performance; • internal and external audits; • testing outcomes; • status of improvement actions.
Daily stand-up meetings	Daily	Daily stand-up meetings.

3.7 Applicable Trust Service Criteria and related controls

Please see the applicable Trust Service Criteria included in the table in chapter 4.

3.8 Boundaries of the system

We have listed the processes that are outside the boundaries of Ubeeo ATS platform and supporting service delivery and consequently have not been described.

- Websites hosted by customers, or third parties contracted by customers;
- Applications contracted by customers and integrated with Ubeeo ATS using API's.

3.9 Third Party Access

As mentioned under 'Software', Cloud Portal is an important software component of the system. Ubeeo's customers have access to configuration screens and API audit logs to monitor activities under their responsibility.

Some clients, at their request and represented by designated staff, are also able to perform basic user management activities (lock accounts, password resets).

On request of the customer, providers of application software can be granted access to Ubeeo ATS API, a restful webservice for authentication, user provisioning, value lists, vacancy data and candidate data.

3.10 System incidents

As Ubeeo no incidents have been identified that (a) were the result of controls that were not suitably designed or operating effectively or (b) otherwise resulted in a significant failure in the achievement of one or more of Ubeeo's service commitments and system requirements throughout the reporting period of November 1, 2023 to April 30, 2024.

3.11 Complimentary User Entity Controls (CEUCs)

Ubeeo assumes that controls will be implemented by user entities because they are necessary, in combination with controls at Ubeeo, to provide reasonable assurance that Ubeeo's service commitments and system requirements are achieved. These controls are identified as Complimentary User Entity Controls (CEUCs) and are listed below.

- The user entity implements and maintains an adequate level of security on its IT resources;
- The user entity implements and maintains an adequate user- and authorization management on its IT resources;
- The user entity informs Ubeeo of relevant changes that have an impact on the managed assets;
- The user entity detects security incidents and service disruptions and notifies Ubeeo without undue delay;
- The user entity monitors availability of resources.

Controls expected to be implemented at user entity organizations	Complemented TSC
User entities are responsible for ensuring that authorized users are appointed as organizational administrators for granting access to the application.	CC5.2, CC5.4
User entities are responsible for notifying Ubeeo of any known or suspected breach of security that could negatively impact the components of the system or execution of described controls.	CC2.3, CC6.2

3.12 Complimentary Subservice Organization Controls

Management of Ubeeo has chosen the carve-out method to address the services provided by subservice organizations. This implies that the components of the subservice organization's system used to provide the services to Ubeeo are excluded from the description of Ubeeo's system and from the scope of the examination.

In relation to the system described in this section, the following subservice organizations play a role in achieving Ubeeo's service commitments. These subservice organizations are monitored by Ubeeo, via the supplier monitoring process including review of the assurance reports. The nature of their services and the relation to Ubeeo's service commitments and system requirements are described in the next paragraphs.

GTT EMEA Ltd.

GTT EMEA Ltd is a cloud and infrastructure solutions provider. They:

- acquire and provide the physical resources (storage, CPU, memory) that Ubeeo needs for user entities;
- provide data center hosting services (electricity, climate, physical security, cross-connects). These data center hosting services are subcontracted by GTT EMEA Ltd, to GTT Datacenter Schiphol, Exadata and Interoute;
- deploy the physical resources at the data centers;
- technically service the physical resources based on service requests by Ubeeo.

Given these services, GTT EMEA Ltd contributes to the following service commitments and system requirements relevant to the service delivery:

Criteria	Control
CC6.4	• Physical access to data centers is approved by an authorized individual.
CC6.4	• Physical access is timely revoked of the employee or vendor record being deactivated.
CC6.4	• Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
CC6.4	• Access to server locations is managed by electronic access control devices.
CC8.1	• A process is in place to identify, evaluate, test, approve, and implement patches in a timely manner on infrastructure.
A 1.2	• GTT maintains formal policies that provide guidance for information security within the organization and the supporting IT environment.
A 1.2	• GTT owned data centers are protected by fire detection and suppression systems.

Microsoft

The following subservice organization controls have been implemented by Microsoft to provide additional assurance that the trust services criteria are met. Given these services, Microsoft contributes to the following service commitments and system requirements relevant to the service delivery:

Criteria	Control
CC 6.4	• Physical access to data centers is approved by an authorized individual.
CC 6.4	• Physical access is timely revoked of the employee or vendor record being deactivated.
CC 6.4	• Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
CC 6.4	• Access to server locations is managed by electronic access control devices.
A 1.2	• Microsoft maintains formal policies that provide guidance for information security within the organization and the supporting IT environment.
A 1.2	• Microsoft owned data centers are protected by fire detection and suppression systems.

Atlassian

Ubeeo uses Atlassian Confluence for technical documentation and Bitbucket code repository services. Given these services, Atlassian contributes to the following service commitments and system requirements relevant to the service delivery:

Criteria	Control
CC6.1, CC6.4, CC6.5, CC6.6	• Maintaining access management to facilities and protected information assets
CC6.5	• Managing and monitoring of agreements and service delivery of datacenter services ensuring service continuity
CC7.4, CC7.5, A1.2, A1.3	• Backup and restore policy and procedures are in place. Backup schedules are implemented, monitored, and tested ensuring continuity and availability of data.

3.13 Criteria not relevant to the system

As all the applicable trust services are relevant to Ubeeo ATS, all references have been included. The following applicable trust services criteria are excluded to Ubeeo's system. These are listed in the table:

Reference to excluded criteria	Explanation for exclusion
PI1.1 – PI-1.5	The data of the data subjects entrusted by customers and data subjects themselves, are responsible for correct processing of the data. The responsibilities of the data controller (customer) and data processor (Ubeeo) with regards to confidentiality are outlined in the confidentiality clause of the data processor agreement that is part of the contract between Ubeeo and its customer.
P1.1 – P8.1	Within the service delivery of Ubeeo, the organization has the role of data processor for (entrusted) customer information. The customers are data controllers. The responsibilities of the data controller (customer) and data processor (Ubeeo) with regards to use of personal identifiable information (PII) are outlined in the use of personal information clause of the data processor agreement that is part of the contract between Ubeeo and its customer. The explicit consent for the collection and processing of PII data is the responsibility of the data controller (customer).

Changes throughout the period

No relevant internal control changes have occurred throughout the November 1, 2023 to April 30, 2024 that may affect the intended users' understanding of the report.

4 Test of Controls and Results of Tests

The applicable trust services criteria and related controls are presented in this section, are an integral part of Ubeeo's description of its Applicant Tracking System Platform and Supporting Services delivery throughout November 1, 2023 to April 30, 2024.

4.1 Test procedures

The test results were achieved by performing the following test activities:

Test procedure	Description
Interview	Completed interview of appropriate personnel to obtain information, among other things on timing, performance, and review of relevant controls.
Inspection	Review of documents and reports that contain an indication of performance of the control. This includes among other things: Reading and reviewing of management reports if certain actions were performed; Inspection of documentation for evidence of performance; Inspection of operation manuals, flow charts, system documentation.
Observation	Observing the implementation of control measures on site.
Re-performance	Re-perform the operation of a control to ascertain that it was performed correctly

In selecting the test procedures, we considered various factors, including, but not limited to the following: (I) the nature of the control; (II) the control risk mitigated by the control; (III) the effectiveness of entity-level controls, especially controls that monitor other controls; (IV) the degree to which the control relies on the effectiveness of other controls; and (V) whether the control is manually performed or automated.

The results of each test conducted are listed within the paragraph 4.2 Test Results.

4.2 Test results

This chapter describes and assesses the control objectives and measures implemented by Ubeeo and the tested control measures by Mathison. The tested control measures are according to the Trusted Service Criteria published by AICPA and meet the criteria of a SOC 2 report. The reference numbers of the control objectives and measures correspond reference numbers of the Trusted Service Criteria 2017 (With Revised Points of Focus – 2022).

Control REF	TSC REF	Control	Mathison's test procedures	Test Result
GOV-1	CC1.2	The information security policy is evaluated by management on a yearly basis and communicated to relevant employees.	Inquired responsible process owner and inspection of the documented information security policy validating it has been timely evaluated.	No exceptions noted
			Inspected system settings on the company management system tooling containing policies and validated the information is accessible and communicated to employees.	
			Observed the in-company communication channels and validated these are utilized for ad-hoc communication on relevant topics, and identified anomalies that might impact adhering to the company policies.	
GOV-2	CC1.2	Supporting policies are documented and reviewed on a yearly basis and are available to relevant employees.	Inquired responsible process owner and inspection of the documented information security policy and supporting documents validating these are timely evaluated.	No exceptions noted
GOV-3	CC1.3	Company objectives are yearly evaluated and established.	Inquired responsible process owner and inspection of the documented management review to validate these include a formal evaluation of the company objectives.	No exceptions noted
GOV-4	CC1.3	Management structures and reporting lines in the pursuit of objectives are in place.	Inquired responsible process owners and inspected the organizational chart and job descriptions to validate responsibilities are outlined for reporting.	No exceptions noted
			Inspected the documented roles and responsibilities to validate the internal control for company objectives	

Control REF	TSC REF	Control	Mathison's test procedures	Test Result
			including information security are assigned to roles which are assigned to employees.	
GOV-5	CC1.3	Management is informed in accordance with the defined reporting lines.	Inquired responsible process owners on the meeting procedures between the management team members to validate such meetings are held. Inspected the organizational chart to validate management positions. Inspected a sample of meeting records to validate management is informed via the appointed methods.	No exceptions noted
GOV-6	CC1.5, CC2.1, CC2.2, CC3.1, CC4.1, CC5.1, CC5.2, CC6.1, CC6.5	The organization has implemented a KPI dashboard, which is used for monitoring of organizational controls.	Inquired responsible process owners on the monitoring of the defined KPI's used for evaluating the status of organizational controls and validated these have been maintained in accordance with the predefined intervals. Inspected a sample of meeting minutes to validate the meetings are held including management participation discussing the KPI dashboard.	No exceptions noted
GOV-7	CC1.5	Within the KPI dashboard, it has been defined what is monitored by whom and with what frequency.	Inquired responsible process owners on the monitoring of the defined KPI's used for evaluating the status of organizational controls and validated monitoring responsibilities and information on the nature of the KPI's are established.	No exceptions noted
GOV-8	CC1.5, CC2.1, CC3.4, CC4.2	A yearly management review takes place with an independent consultant. The development	Inquired responsible process owners on the procedure of the management review. Inspected the	No exceptions noted

Control REF	TSC REF	Control	Mathison's test procedures	Test Result
		and performance of internal controls and changes are discussed during the management review.	management review validating internal controls are evaluated.	
			Inspected a sample of meeting records to validate management is informed, internal control controls are evaluated, and changes are discussed on potential impact.	
GOV-9	CC2.2, CC2.3	A communication matrix is defined and reviewed on a yearly basis, addressing communication responsibilities within the company and to third parties.	Inquired responsible process owners and inspected the communication matrix, validating the reporting lines have been timely reviewed.	No exceptions noted
RIS-1	CC2.1, CC3.1, CC3.2, CC3.3, CC3.4	A risk assessment is conducted on a yearly basis or when significant changes are implemented. The risk assessment includes fraud risks, internal and external context of the organization and legislative and contractual requirements.	Inquired responsible process owner and inspection of the documented risk management process to validate criteria have been defined to rate the significance of risks and identify risk management strategies. Validated the risk assessment has been updated on a timely basis, taking into account the aforementioned risk sources.	No exceptions noted
			Inspected the risk assessment registry to validate the aforementioned risk sources are taken into account and associated potential impacts are identified.	
RIS-2	CC3.1, CC3.2, CC3.3, CC3.4, CC5.1	The organization has a defined risk methodology including risk criteria and risk appetite.	Inquired responsible process owner and inspection of the documented risk management process to validate criteria have been defined to rate the significance of risks and identify risk management strategies. Validated the risk management program has been updated on a timely basis.	No exceptions noted

Control REF	TSC REF	Control	Mathison's test procedures	Test Result
RIS-3	CC3.2	Risks are identified and classified based on impact and likelihood. Risk treatment options are taken and implemented in accordance with risk classification.	Inquired responsible process owner and inspection of the documented risk management process to validate criteria have been defined to rate the significance of risks based upon impact and likelihood.	No exceptions noted
			Inquired responsible process owners on the risk treatment options to validate these are set, in accordance with the risk appetite, by identifying the impact and likelihood. Inspected the risk treatment plans are updated and monitored in accordance with the risk classification.	
HR-1	CC1.1	Management communicates an information security policy with employees and contractors addressing the company's values for integrity and ethical behavior.	Inquired responsible process owners on the company management system tooling with policies and Confluence containing technical procedures and validated the information is accessible and communicated to employees.	No exceptions noted
			Inspected system settings, to validate employees have access to the policies.	
HR-2	CC1.1	Employees receive the information security policy within 1 month upon hire and are informed on updates.	Inquired responsible process owners on the hiring process and inspected checklist tasks for a sample of employees, validating the information security policy is timely communicated.	No exceptions noted
			Inspected for a sample of employees, validating employees formally sign for having received the information security policy.	

Control REF	TSC REF	Control	Mathison's test procedures	Test Result
HR-3	CC1.1	A disciplinary process is defined and implemented for employees not adhering to the company integrity and ethical values as defined in the information security policy.	Inquired responsible process owners on the hiring process and inspected checklist tasks for a sample of employees, validating the disciplinary policy is timely communicated.	No exceptions noted
			Inspected for a sample of employees, validating employees formally sign for having received the disciplinary policy.	
			Inspected system settings, validating employees have access to the disciplinary policy.	
HR-4	CC1.3, CC1.4, CC1.5, CC5.1, CC5.3	The organization has an organizational chart, job descriptions and specific (security) roles are in place.	Inspected the organizational chart and job descriptions validating (security) positions are identified and populated.	No exceptions noted
			Inquired responsible process owners on their job descriptions and roles. Inspected meeting procedures and notes between the security team and management team to validate meetings are held discussing the (security) responsibilities.	
HR-5	CC1.3	Roles include responsibilities that are aligned with the company objectives.	Inquired responsible process owners and inspected the documented roles and responsibilities to validate the roles are addressing the design and implementation of information security controls supporting the company objectives.	No exceptions noted
			Inspected the documented objectives and KPI's validating these are documented and monitored by employees.	

Control REF	TSC REF	Control	Mathison's test procedures	Test Result
HR-6	CC1.4	Competence requirements are defined and at least yearly reviewed by the management team members for their respective teams.	Inquired responsible process owners and inspected the competence matrix to validate competence requirements are formalized for the job roles. Inspected the overview of reviewed competence levels to validate these have been timely and fully performed.	No exceptions noted
HR-7	CC1.1	Employees are required to sign a confidentiality agreement during onboarding.	Inquired responsible process owners on the hiring process and inspected checklist tasks for a sample of employees, validating the agreed upon contract agreements are signed. Inspected for a sample of employees, validating the agreed upon contract includes a confidentiality clause. Inspected for a sample of employees, validating employees formally agree upon the company ethical values of the company.	No exceptions noted
COM-1	CC4.1	Internal controls are annually reviewed by internal audit in accordance with the defined audit plans. Internal audit reports and findings are maintained.	Inquired responsible process owners and inspected registries on recurring tasks and registries with audit findings, validating internal audits are planned and findings are reported, and status is updated with progress and actions. Inspected documentation by the internal auditor validating internal audits are performed by an independent auditing party, and self-assessments via monitoring of processes are performed by the control owners.	No exceptions noted

Control REF	TSC REF	Control	Mathison's test procedures	Test Result
COM-2	CC4.1	Internal audit plans are defined covering the components of internal control, taking into account the risk of failure of internal controls and previous audit findings.	Inquired responsible process owners and inspected registries on recurring tasks and registries with audit findings, validating internal audits are planned for the controls defined for the company's integral compliance framework.	No exceptions noted
			Inspected documentation by the internal auditor validating internal audits are performed by an independent auditing party, incorporating previous audit findings.	
COM-3	CC4.2, CC7.4	Remediation of the mitigating actions is monitored by the Security Officer and when deemed necessary, are discussed in the management team meeting.	Inquired responsible process owners and inspected registries on audit findings within the management system tool, validating internal audit findings are reported, and status is updated with progress and actions.	No exceptions noted
			Inspected a sample of documentation on the meeting notes of the monthly management team meetings and yearly management review, to validate deviations and audit findings are discussed among the management team.	
COM-4	CC1.1	The organization classifies information in accordance with the information security classification.	Inquired responsible process owners and inspected the data classification policy to validate requirements are defined for securing information.	No exceptions noted
COM-5	CC6.5, C1.2,	Devices containing confidential information are destroyed prior to disposal or are securely wiped prior to reuse.	Inquired responsible process owners and inspected the asset management policy to validate requirements are defined for securing information.	No exceptions noted

Control REF	TSC REF	Control	Mathison's test procedures	Test Result
			Inspected for a sample of assets to validate devices are securely wiped prior to reuse. No assets have been disposed during the reporting period.	
COM-6	C1.2	Documents are handled and destroyed following the information classification policy.	Inquired responsible process owners and inspected the data classification policy to validate requirements are defined for destroying data. Inspected for a sample of companies through system settings, and via querying the platform database to validate candidate data and company data are destroyed effectively.	No exceptions noted
ACC-1	CC5.2, CC6.1, CC6.2	Quarterly checks are performed to validate correct authorizations in key systems and on non-critical systems in accordance with the authorization matrix.	Inquired responsible process owners and inspected access review registries to validate the quarterly access reviews have been performed for the in-scope key system components and changes are registered and tracked.	No exceptions noted
ACC-2	CC6.2	Granting logical access rights to new users is performed in accordance with the onboarding procedure and onboarding instructions for the new user.	Inquired responsible process owners and inspected the access control policy, validating the responsibilities within the processes are defined for modifying user access. Inspected for a sample of new employees the access requests and sampled production systems relevant to the service delivery validating the access control policy is implemented and access is managed in accordance with the procedure.	No exceptions noted

Control REF	TSC REF	Control	Mathison's test procedures	Test Result
ACC-3	CC6.2, CC6.3	Access rights to critical systems are revoked within 24 hours when users no longer need the assigned rights or leave the organization.	Inquired responsible process owners and inspected the access control policy, validating the responsibilities within the processes are defined for modifying user access.	No exceptions noted
			Inspected for a sample of terminated employees to validate the access to sampled production systems relevant to the service delivery is timely revoked in accordance with the procedure.	
ACC-4	CC6.3	The organization controls logical access by granting predefined role-based access rights documented in the authorization matrix.	Inquired responsible process owners and inspected the access control policy, validating the responsibilities within the processes are defined for modifying user access.	No exceptions noted
			Inspection of the authorization matrix to validate access right are setup using the role-based access control methodology.	
			Inspected for a sample of employees and the in-scope systems, the access rights have been issued in accordance with the authorization matrix.	
ACC-5	CC6.3	The authorization matrix is reviewed and established on an annual basis.	Inquired responsible process owners and inspected the access control policy, validating the responsibilities within the processes are defined for modifying user access.	No exceptions noted
ACC-6	CC6.4, C6.5, A.1.1, A1.2	Physical access to the office is restricted to authorized personnel.	Inquired responsible process owners and observed the physical access restrictions of the company office validating access control mechanisms, tag readers and alarms are implemented.	No exceptions noted

Control REF	TSC REF	Control	Mathison's test procedures	Test Result
			Inspected for the sampled tags and tags in stock matched the asset registry and employee mutations were adequately processed in the asset registry.	
ACC-7	CC6.6	Access to Ubeeo servers and database requires VPN access and server user account access.	Inquired responsible process owners and inspected system settings to validate server and database access require a VPN connection.	No exceptions noted
			Observed via reperformance to validate disconnecting the VPN results in access revocation.	
ACC-8	CC6.8	Procedures are defined for implementation of application software.	Inquired responsible process owners and inspected the release process, validating procedures are defined for implementation of application software.	No exceptions noted
SEC-1	CC6.6, CC6.7	Communication to the organization services is secured via HTTPS/SSL connections.	Inquired responsible process owners and inspected security Key Performance Indicators have been defined and are monitored on the HTTPS/SSL connection status on a quarterly basis.	No exceptions noted
			Observed by re performance of the security scans for the Ubeeo platform and for a sample of managed customer websites, validating the HTTPS/SSL connection are securely configured.	
SEC-2	CC6.5, CC6.7	Policies are in place to protect mobile devices (such as laptops, smart phones, and tablets) that serve as information assets.	Inquired responsible process owners and inspected mobile device management policies are implemented, and validated mobile devices that serve as information assets are protected.	No exceptions noted
SEC-3	CC6.8	Anti-malware software is installed on company assets and is being kept up to date.	Inquired responsible process owners and inspected system settings on the mobile device management	No exceptions noted

Control REF	TSC REF	Control	Mathison's test procedures	Test Result
			software, validating anti-malware software is installed on the company assets.	
SEC-4	CC6.8	Laptops have hard disk encryption enabled	Inquired responsible process owners and inspected system settings on the mobile device management software, validating laptops have hard disk encryption is enabled and compliance status is monitored.	No exceptions noted
SEC-5	CC6.8	Compliance status of laptops is being monitored.	Inquired responsible process owners and inspected system settings on the mobile device management software, validating compliance status of laptops is enforced by policies and status is being monitored.	No exceptions noted
SEC-6	CC7.1	Security risks in the IT infrastructure are identified with continuous security scans and the organization takes action when vulnerabilities are found.	Inquired responsible process owners and inspected the security risks in the IT infrastructure, validating procedures are defined for taking action when vulnerabilities are found.	No exceptions noted
			Inspected for a sampled of releases to validate that security scans are performed prior to releases.	
			Inspected system settings on static code scanning, validating the code is scanned on a daily basis and vulnerabilities are addressed.	
			Inspected third party vulnerability scans settings and scanning results to validate these are performed on a daily basis, potential vulnerabilities are identified and evaluated. Remedial actions are taken when deemed necessary.	

Control REF	TSC REF	Control	Mathison's test procedures	Test Result
SEC-7	CC7.2	Detected anomalies in compromising physical barriers, use of compromised identification and authentication credentials, unauthorized access from outside the system boundaries and compromising of authorized external parties are analyzed to validate if they represent security events and remedial actions are addressed.	Inquired responsible process owners on the security barriers within the IT infrastructure, and observed during the office walkthrough physical barriers within the office are set and monitored. Inspected the assurance reports of the subservice organizations to validate the assurance reports include physical access controls and no relevant findings have been identified that may affect the service delivery. Inspected system setting on the firewall settings, validating unauthorized access attempts from outside the system boundaries and compromising of authorized external parties are analyzed to validate if they represent security events and remedial actions are taken.	No exceptions noted
MON-1	CC5.1, CC5.2	The organization monitors system components through automated monitoring systems.	Inquired responsible process owners and inspected system configuration settings of the monitoring tools, validating they are set up to monitor the specified system components. Observed via reperformance of various scenarios of system component failures and anomalies to validate that the automated monitoring systems detect and report these issues accurately and promptly.	No exceptions noted
MON-2	CC7.2	The organization monitors system components against predefined thresholds and suspicious events. Alerts are raised when	Inquired responsible process owners and inspected system settings of monitoring appliances to validate these appliances are set to analyze logging of events	No exceptions noted

Control REF	TSC REF	Control	Mathison's test procedures	Test Result
		thresholds are met. Alerts are handled directly unless software fix is required in which case tickets are raised.	that may have a potential impact on the organizational security posture. Inspection of system settings validating thresholds are set and alerts are generated when thresholds are met, and tickets are raised.	
MON-3	CC7.2	Employees are assigned to monitor alerts that are communicated to personnel for analysis to identify environmental threat events.	Inquired responsible process owners and inspected system settings of monitoring appliances and communication channels are set up to inform employees of events that may have a potential impact on the organizational security posture.	No exceptions noted
MON-4	A1.1	Servers and system components are monitored. Monitoring criteria include response time, uptime, available disk space, memory utilization and service availability.	Inquired responsible process owner and inspected system settings on monitoring systems to validate monitoring abilities have been implemented and alerts are generated when thresholds are met, including the aforementioned monitoring criteria.	No exceptions noted
INC-1	CC7.3	A security incident and incident process are documented, implemented, and reviewed on an annual basis, or after major changes upon the process.	Inquired responsible process owners and inspection of documentation on the incident and security incident reporting procedures, to validate procedures are established and reviewed on a timely basis. Inspected system settings to validate reporting mechanisms have been setup to register such events.	No exceptions noted
INC-2	CC7.3, CC7.4	Security incidents and incidents are registered in appointed registries, depending on the source. These incidents are labeled as security incidents.	Inquired responsible process owners and inspection of documentation on the incident and security incident reporting procedures, to validate procedures are established for handling of such events.	No exceptions noted

Control REF	TSC REF	Control	Mathison's test procedures	Test Result
			Inspected a sample of system registries on incidents and security incidents to validate such incidents are labelled, logged, tracked, and resolved.	
INC-3	CC7.4	A procedure including roles and responsibilities is defined for acting on (security) incidents and data breaches.	Inquired responsible process owners and inspection of documentation on the incident and security incident reporting procedures, to validate procedures include responsibilities for acting upon such events.	No exceptions noted
INC-4	CC7.4	Timely resolution of high and critical incidents is monitored by the Technology Manager (CISO).	Inquired responsible process owners and inspected incidents and reporting mechanisms, validating timely resolutions of high and critical incidents are monitored by the Technology Manager.	No exceptions noted
INC-5	CC7.4	Security incidents and data breaches are reported to the Technology Manager in accordance with the defined procedure. Timely resolution of the security incident or data breach occur, including reporting to the client or the authorities.	Inquired responsible process owners and inspected incidents and reporting mechanisms, validating security incidents and potential data beaches are analyzed and root causes are determined. Observed analyzes demonstrated no data breaches and security incidents occurred during the reporting period, therefore we could not test the reporting procedures to clients or authorities.	No exceptions noted
INC-6	CC7.4, CC7.5	The effectiveness of measures and tasks to remedy security incidents and data breaches are discussed as part of the bi-weekly management team meeting. Remedial actions are identified when deemed necessary.	Inquired responsible process owners and inspected the bi-weekly management team meeting. Validated remedial actions are identified when deemed necessary, including validating of the effectiveness of measures and tasks to remedy security incidents and data breaches are discussed.	No exceptions noted

Control REF	TSC REF	Control	Mathison's test procedures	Test Result
			Inspected a sample of management meetings to validate the effectiveness of measures and tasks to remedy security incidents and data breaches are discussed.	
INC-7	CC7.5, CC8.1	The root cause of the security incidents is determined.	Inquired responsible process owners and inspected security incident registries to validate the root cause of the security incidents are determined.	No exceptions noted
DEV-1	CC8.1	Software and system changes are tested in the test environment prior to deployment to production. Test results are documented.	Inquired responsible process owners and inspected the documented test results, validating software and system changes are tested in the test environment prior to deployment to production. Inspected for a sample of releases validating release checklists are also maintained ascertaining all release steps have been followed.	No exceptions noted
DEV-2	CC8.1	Organization code is centrally stored. Changes in code configurations are registered and logs are retained in the central stored code repositories.	Inquired responsible process owners and inspected changes in code configurations to validate these are registered and logs are retained in the central stored code repositories, and validating codes are centrally stored. Inspected releases for a sample of changes to validate changes in code configurations are registered and logs are retained.	No exceptions noted
DEV-3	CC8.1	Changes are reviewed prior to implementation.	Inquired responsible process owners and inspected changes in code configurations, validating codes are reviewed prior to implementation.	No exceptions noted

Control REF	TSC REF	Control	Mathison's test procedures	Test Result
			Inspected releases for a sample of changes to validate reviews of changes are performed prior to implementation.	
			Inspected for a sample of releases validating release checklists are also maintained ascertaining all release steps have been followed.	
DEV-4	CC8.1	Changes to the environment are documented during development and implementation to allow rollback. Changes are logged.	Inquired responsible process owners and inspected changes are logged, validating changes to the environment are documented during development and implementation to allow rollback.	No exceptions noted
			Inspected releases for a sample of changes to validate changes are logged during development and implementation to allow rollback.	
DEV-5	CC8.1	Changes are tested prior to implementation.	Inquired responsible process owners and inspected a sample of changes, validating changes are tested prior to implementation.	No exceptions noted
			Inspected for a sample of releases validating release checklists are also maintained ascertaining all release steps have been followed.	
CTY-1	CC7.4, CC7.5, A1.2, A1.3	The organization has a backup and restore policy in place. Backup schedules are implemented, monitored, and tested.	Inquired responsible process owners and inspected the backup and restore policy documentation validating these have been defined.	No exceptions noted
			Inspected system settings to validate redundancy settings for a sample of customer websites and the platform data are setup and are monitored in accordance with the policy.	

Control REF	TSC REF	Control	Mathison's test procedures	Test Result
CTY-2	CC7.5, CC9.1, A1.2, A1.3	The organization has a Business Continuity plan including roles and responsibilities for handling incidents during adverse situations, in place which is reviewed on an annual basis.	Inquired responsible process owners and inspected Business Continuity documentation to validate that the continuity scenarios are documented addressing continuity and recovery aspects and responsibilities.	No exceptions noted
			Inspected the Business Continuity documentation validating these have been reviewed on a timely basis.	
CTY-3	CC7.5	The Business Continuity plan is tested on an annual basis. Test results are maintained, and remedial actions taken when deemed necessary.	Inquired responsible process owners and inspected documentation on tests that have been performed to validate the tests have occurred on a timely basis and remedial activities are identified when deemed necessary.	No exceptions noted
			Inspected system settings to validate redundancy settings for a sample of customer websites and the platform data are setup in accordance with the policy.	
CTY-4	CC9.1, A1.2	The organization IT infrastructure and service delivery platform is set up redundantly.	Inquired responsible process owners and inspected system settings to validate redundancy settings for a sample of customer websites and the platform data are setup in accordance with the policy.	No exceptions noted
			Inquired responsible process owners and inspected for the critical suppliers relevant to the service delivery the assurance reports have been obtained and include redundancy.	
SUP-1	CC2.3, CC5.2, CC6.4, CC9.2	The organization performs supplier reviews on a yearly basis with critical partners and suppliers regarding the provided services.	Inquired responsible process owners and inspected the supplier management process to validate procedures on performing supplier reviews have been defined in relation to the identified critical vendors.	No exceptions noted

Control REF	TSC REF	Control	Mathison's test procedures	Test Result
			Inspected for a sample of critical suppliers the assessments have been performed.	
SUP-2	CC2.3, CC9.2	Assurance reports of critical Cloud service providers are at least annually requested upon and reviewed. Measures are taken when deemed necessary resulting from findings within the assurance reports.	Inquired responsible process owners and inspected for the critical suppliers relevant to the service delivery the assurance reports have been obtained and have been assessed.	No exceptions noted
SUP-3	CC2.3, CC9.2	New suppliers are assessed against predefined criteria before services are adopted.	Inquired responsible process owners and inspected the supplier management process to validate procedures on performing supplier reviews have been done using the defined criteria.	No exceptions noted
SAL-1	C1.1	The organization has a data processing agreement (DPA)in place with customers including a confidentiality clause addressing protection and destruction responsibilities.	Inquired responsible process owners and inspected for a sample of customers the data processing agreement has been formally agreed upon. Validated the DPA's contained confidentiality clauses and roles and responsibilities for protection of data and destruction of data upon request.	No exceptions noted

4.3 Criteria to controls reference

Ubeeo has established an internal control framework based upon the Trust Service Criteria and ISO27001. For internal efficiency and control ownership allocation, the control naming and numbering of the Ubeeo's processes have been adopted. The included references to applicable AICPA Trusted Services Criteria are mapped to the internal controls.

TSC Criteria	Control REF	Criteria description
CC1.1	HR-1, HR-2, HR-3, HR-7	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.
CC1.2	GOV-1, GOV-2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
CC1.3	GOV-3, GOV-4, GOV-5, HR-4, HR-5	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
CC1.4	HR-4, HR-6	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
CC1.5	GOV-6, GOV-7, GOV-8, HR-5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
CC2.1	GOV-6, GOV-8, RIS-1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.
CC2.2	GOV-6, GOV-9	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
CC2.3	GOV-9, SUP-1, SUP2, SUP-3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.
CC3.1	GOV-6, RIS-1, RIS-2	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
CC3.2	RIS-2, RIS-3	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

TSC Criteria	Control REF	Criteria description
CC3.3	RIS-1, RIS-2	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.
CC3.4	RIS-1, RIS-2	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.
CC4.1	COM-1, COM-2	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
CC4.2	GOV-8, COM-3	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.
CC5.1	RIS-2, MON-1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
CC5.2	MON-1, ACC-1	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.
CC5.3	HR-4	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.
CC6.1	GOV-6, ACC-1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
CC6.2	ACC-1, ACC-2, Acc-3	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
CC6.3	ACC-3, ACC-4, ACC-5	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity’s objectives.
CC6.4	ACC-6, SUP-1	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive

TSC Criteria	Control REF	Criteria description
		locations) to authorized personnel to meet the entity's objectives.
CC6.5	SEC-2, COM-5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.
CC6.6	ACC-7, SEC-1	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
CC6.7	SEC-1, SEC-2	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.
CC6.8	ACC-8, SEC-3, SEC-4, SEC-5	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.
CC7.1	SEC-6	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.
CC7.2	SEC-7, MON-2, MON-3	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.
CC7.3	INC-1, INC-2	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.
CC7.4	INC-2, INC-3, INC-4, INC-5, INC-6, CTY-1	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.
CC7.5	INC-6, INC-7, CTY-1, CTY-2, CTY-3	The entity identifies, develops, and implements activities to recover from identified security incidents.
CC8.1	INC-7, DEV-1, DEV-2, DEV-3, DEV-4, DEV-5	The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

TSC Criteria	Control REF	Criteria description
CC9.1	CTY-2, CTY-4	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
CC9.2	SUP-1, SUP-2, SUP-3	The entity assesses and manages risks associated with vendors and business partners.
A1.1	MON-4	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.
A1.2	ACC-6, CTY-1, CTY-2, CTY-4	The entity authorizes, designs, develops, or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.
A1.3	CTY-1, CTY-2	The entity tests recovery plan procedures supporting system recovery to meet its objectives.
C1.1	COM-4, SAL-1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.
C1.2	COM-5, COM-6	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.