**

**Digiplex AS**

**Data Centre Colocation Hosting Services**

**Combined SOC1 and ISAE 3402 Type II Report on Controls at a Service Organization**

***for the period 01 January 2019 to 31 December 2019***

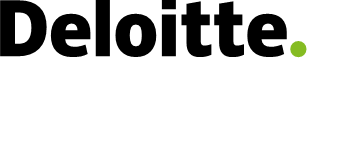


Table of Contents

[Executive Summary 3](#_Toc32498683)

[Section One – Independent Service Auditors’ Report 5](#_Toc32498684)

[Section Two – Management’s Assertion Provided by Service Organization and Subservice Organization 9](#_Toc32498685)

[Section Three – Description of DigiPlex’s system related to data centre colocation hosting services throughout the period 01 January 2019 to of 31 December 2019 12](#_Toc32498686)

[I. Overview 13](#_Toc32498687)

[II. The types of services provided 14](#_Toc32498688)

[III. The principal service commitments and system requirements 14](#_Toc32498689)

[IV. The components of the system used to provide the services 18](#_Toc32498690)

[V. Incidents occurring in the 12 months prior to reporting as of date that resulted in a significant impairment of DigiPlex’s ability to achieve its service commitments and system requirements 28](#_Toc32498691)

[VI. Complementary user entity controls 29](#_Toc32498692)

[VII. Complementary subservice organization controls 30](#_Toc32498693)

[Section Four – Information provided by the service auditor 31](#_Toc32498694)

[I. Introduction 32](#_Toc32498695)

[II. Control environment elements 32](#_Toc32498696)

[III. Test of Operating Effectiveness 32](#_Toc32498697)

[IV. Findings and Observations 56](#_Toc32498698)

# Executive Summary

|  |  |
| --- | --- |
| DigiPlex | |
| Scope | Data Centre Colocation Hosting Services |
| For the period | 01 January 2019 to 31 December 2019 |
| Location(s) | Oslo, Norway and Stockholm, Sweden |
| Opinion Result | Qualified |
| Testing Exceptions | Please refer Section Four; subsection IV |
| Complementary User Entity Controls | Yes – see Section Three subsection VII |

# Section One – Independent Service Auditors’ Report

**Deloitte AS**

Dronning Eufemias Gate 14

0191 Oslo

Norway

Tel: +47 23 27 90 00

www.deloitte.no

**INDEPENDENT SERVICE AUDITORS’ REPORT**

**DigiPlex**

***Scope***

We have examined the description of the system of DigiPlex AS (the “Service Organization” or “DigiPlex”) related to data centre colocation hosting services provided to its clients (“User entities” or “User Organizations”) from data centres located at:

* DigiPlex Norway AS (“DNAS”)
* DigiPlex Rosenholm AS (“DRAS”)
* DigiPlex Fetsund AS (“DFAS”)
* DigiPlex Stockholm 1 AB (“DS1”)

throughout the period 01 January 2019 to 31 December 2019 and the suitability of the design and operating effectiveness of controls included in the Description to achieve the related control objectives also included in the Description, based on the criteria identified in Section 2 (the “Assertion”). The controls and control objectives included in the Description are those that management of DigiPlex believes are likely to be relevant to user entities’ internal control over financial reporting and the Description does not include those aspects of the system of DigiPlex that are not likely to be relevant to user entities’ internal control over financial reporting.

The service organization does not use a subservice organization and accordingly, the Description in Section 3 includes only the controls and related control objectives of the Service Organization. Our examination performed on the description of the services relate only to the service organization and did not extend to controls of any subservice organization[s].

The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls contemplated in the design of the Service Organization’s controls are suitably designed and operating effectively, along with related controls at the Service Organization. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

***Service organization’s responsibilities***

In **Section Two**, the Service Organization has provided an assertion about the fairness of the presentation of the Description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the Description. The Service Organization is responsible for preparing the Description and its assertion, including the completeness, accuracy, and method of presentation of the Description and the assertion, providing the services covered by the Description, specifying the control objectives and stating them in the Description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the Description.

***Service auditor’s responsibilities***

Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the Description, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) and International Standard on Assurance Engagements 3402, Assurance Reports on Controls at a Service Organization, issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management’s assertion, the Description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the Description throughout the period 01 January 2019 to 31 December 2019. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization’s system and the suitability of the design and operating effectiveness of controls involves:

* Performing procedures to obtain evidence about the fairness of the presentation of the Description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management’s assertion.
* Assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the Description.
* Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the Description were achieved.
* Evaluating the overall presentation of the Description, suitability of the control objectives stated therein, and suitability of the criteria specified by the service organization in its assertion.

***Service Auditors’ Independence and Quality Control***

We have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the AICPA. We applied the statements on quality control standards established by the AICPA and accordingly maintain a comprehensive system of quality control.

***Inherent Limitations***

The Description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities’ financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. 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 achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

***Description of Tests of Controls***

The specific controls tested and the nature, timing, and results of those tests are listed in Section 4 of the report.

***Basis for Qualified Opinion***

The Service Organization states in its Description that it has controls in place to timely revoke employee access to data centre facilities, perform periodic access review and perform disaster recovery drills as per the company’s continuity plans. However, as noted in Section 4 of the report, controls related to the employee access revocation, periodic access review and disaster recovery drills were not performed during the period 01 January 2019 to 31 December 2019. As a result, controls were not operating effectively to achieve the following control objectives:

* Control Objective #7: Controls provide reasonable assurance that access to the data centre premises and its assets is restricted physically and granted as per need-to-know basis
* Control Objective #11: Controls provide reasonable assurance that organization has documented and implemented Business Continuity plan and Disaster recovery measures in place to ensure minimal impact to operations in case of a disaster

***Opinion***

In our opinion, except for the matter referred to in the preceding paragraph, based on the criteria described in the Service Organization’s assertion in Section 2 of the report:

a. The Description fairly presents the system related to data centre colocation hosting services that was designed and implemented throughout the period 01 January 2019 to 31 December 2019

b. The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period 01 January 2019 to 31 December 2019

c. The controls operated effectively to provide reasonable assurance that the control objectives stated in the Description were achieved, throughout the period 01 January 2019 to 31 December 2019 if complementary user entity controls assumed in the design of the DigiPlex’s service organization controls operated effectively throughout the period 01 January 2019 to 31 December 2019

***Restricted Use***

This report, including the description of tests of controls and results in Section 4,is intended solely for the information and use of management of the Service Organization, user entities of the Service Organization’s system related to data centre colocation hosting services during some or all of the period 01 January 2019 to 31 December 2019, and their auditors who audit and report on such user entities’ financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities’ financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

For Deloitte AS,

­­­­­­­­­­­­­­­­­­­

Oslo, 13. February 2020

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Kevin F. McCloskey, Director, SME TPA Date / Place

Oslo, 13. February 2020

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Bjørn Prestegard, Partner, State Authorized Auditor Date / Place

# Section Two – Management’s Assertion Provided by Service Organization and Subservice Organization

**Management Assertion provided by DigiPlex AS (“Service Organization” or “DigiPlex”) for SOC1 and ISAE 3402 Type II Report for the period 01 January 2019 to 31 December 2019**

We have prepared the description of the system of DigiPlex AS (the “Service Organization” or “DigiPlex”) related to data centre colocation hosting services for user entities during some or all of the period 01 January 2019 to 31 December 2019, and their user auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of the user entities’ financial statements. The description of the system includes data centre colocation hosting services provided to the user entities from the following data centres locations:

* DigiPlex Norway AS (“DNAS”)
* DigiPlex Rosenholm AS (“DRAS”)
* DigiPlex Fetsund AS (“DFAS”)
* DigiPlex Stockholm 1 AB (“DS1”)

.

DigiPlex does not use a subservice organization and accordingly, the Description in Section 3 includes only the controls and related control objectives of the Service Organization. The description of the services relate only to DigiPlex and did not extend to controls of any subservice organization[s].

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of DigiPlex’s controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of the user entities.

**Description Criteria**

We confirm, to the best of our knowledge and belief, that:

We confirm, to the best of our knowledge and belief, that:

1. The description fairly presents DigiPlex’s system made available to user entities of the system during some or all of the period 01 January 2019 to 31 December 2019 for data centre colocation hosting services. The criteria we used in making this assertion were that the description:
2. Presents how the system made available to user entities was designed and implemented to process relevant transactions, including, if applicable:
3. The types of services provided including, as appropriate, the classes of transactions processed.
4. The procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.
5. The information used in the performance of procedures, including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.
6. How the system captures and addresses significant events and conditions.
7. The process used to prepare reports or other information provided to user entities of the system.
8. Services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them.
9. The specified control objectives and controls designed to achieve those objectives, including, as applicable, complementary user entity controls assumed in the design of the service organization’s controls.
10. Other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.
11. The description includes relevant details of changes to DigiPlex’s system during the period covered by the description when the description covers a period of time.
12. 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 user entities of the system and their user auditors and may not, therefore, include every aspect of the system that each individual user entity of the system and its auditor may consider important in its own particular environment.
13. The controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period 01 January 2019 to 31 December 2019 to achieve those control objectives provided that subservice organizations and user entities applied the controls contemplated in the design of the service organization’s controls. The criteria we used in making this assertion were that:
14. The risks that threaten the achievement of the control objectives stated in the description have been identified by DigiPlex
15. Controls identified in our description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in our description from being achieved.
16. The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

For DigiPlex AS (“DigiPlex”)

# Section Three – Description of DigiPlex’s system related to data centre colocation hosting services throughout the period 01 January 2019 to of 31 December 2019

## Overview

**Applicability & Purpose of Report**

The purpose of this report is to cover the description of the system of DigiPlex AS (the “Service Organization” or “DigiPlex”) related to General IT Controls for data centre colocation hosting services provided to its clients (“User entities” or “User Organizations”) from DigiPlex data centres located at:

* DigiPlex Norway AS
* DigiPlex Rosenholm AS
* DigiPlex Fetsund AS
* DigiPlex Stockholm 1 AB

**Business description**

DigiPlex is the market leader in Norway and leading in the Nordics. We are also one of Europe’s longest-standing data-centre operators, with operations since 2001. We are a private company and have had the same owners since the start: William Conway (co-founder and co-CEO of global Asset Management Company The Carlyle Group) and Byrne Murphy (DigiPlex Group Chairman with over 25 years’ experience of international property investment and development).

This ownership structure ensures we have rapid access to capital as and when needed. The access to investment capital benefits you as our customer. Today’s businesses need to be flexible and tying up capital in a data centre can seriously cramp your investment potential and your cash flow. Partnering with DigiPlex gives you a state-of-the-art solution with minimal investment and predictable Opex costs over time.

DigiPlex currently owns and operates three data centres in Norway, one in Sweden, one in Demark and is looking at further expansion in the Nordics.

**Vision**

We at DigiPlex are all committed to one common purpose:

**“To provide customers with the most reliable and resource efficient IT-housing, enabling individuals, businesses and societies to carry out their critical digital activities”**

**Integrity and Ethical Values**

Corporate governance at DigiPlex starts with a Senior Leadership Team (Board of Directors) that establishes, maintains, and monitors standards and policies for ethics, business practices, and compliance that span the company. Corporate governance at DigiPlex serves several purposes:

1. To establish and preserve management accountability to DigiPlex’s owners by appropriately distributing rights and responsibilities among the Senior Leadership Team, directors, managers, and shareholders.
2. To provide a structure through which management and the Senior Leadership Team set and attain objectives and monitor performance.
3. To strengthen and safeguard a culture of business integrity and responsible business practices.

**Values**

Trust, respect, honesty, transparency and professionalism are the foundation blocks of our relationship with everyone who interacts with our Company.  To achieve this, DigiPlex recognises that the behaviours of all our employees must experience and deliver to the same high expectation, as this acts as the benchmark for our professional conduct.  Our reputation is built upon integrity, honesty and acting responsibly whilst respecting the Laws and Regulations, Traditions and Cultures of the work environments within which we all operate.

In support of our Company mission we are all committed to the following values:

|  |  |
| --- | --- |
| * **Customer Partner** | *to partner with our customers and ensure success by creating exceptional value through innovative solutions and services.* |
| * **Teamwork** | to work together effectively to achieve our goals, while encouraging individual engagement, contribution and responsibility. |
| * **Innovation focused** | *to create and sustain a culture where entrepreneurship is encouraged and rewarded.* |
| * **Personal accountability** | *to be empowered to embrace personal ownership for delivering on our commitments.* |
| * **Respect** | *to act with integrity and considerations towards all.* |
| * **Passionate** | *to be passionate about winning and about DigiPlex, our services, our people, and having fun, while delivering superior value to all stakeholders.* |

These define the way we run and aim to grow DigiPlex.  They set out the services we wish to provide, our behaviours and the way we manage our business.  Our values form the foundations from which our systems and processes are developed and ensure we are all committed to be working from a commonly understood base, that can be consistently applied across our Company.

## The types of services provided

DigiPlex is a company providing highly secure high-powered, energy-efficient, carrier-neutral, co-location data centre space in Scandinavia for our customers' information and communication technology (ICT) equipment.

Our approach ensures a cost-effective environment offering speed to market and inherent flexibility and scalability for the future.

* **Secure**: Our centres deliver several layers of security to organisations who require specialist environments for applications ranging from network operations through disaster recovery to data centre space and secure printing.
* **Resilient**: DigiPlex also provides guaranteed continuity of power into and throughout our conditioned, chilled modules, suites and rooms supporting our customers as they ensure business continuity.
* **Connected**: Our secure centres offer multiple telecoms facilities underpinned by our commitment to independence and neutrality.

DigiPlex supports our customer's competitive quest for best value and best practice. The centre is used by customers for applications ranging from disaster recovery through to frontline server space, and secure network control centres.

## The principal service commitments and system requirements

DigiPlex has adopted a process approach in the development and implementation of its management system for the provision of services. The aim of the management system is to enhance customer satisfaction by meeting customer requirements. In addition, each of the processes undertaken is controlled to reduce the impact of the company’s activities and services on the environment and to eliminate or minimise Health & Safety and Information Security risks to its employees and other interested parties. Continual improvement of the effectiveness and performance of the management system and processes is attained through performance measurement and the achievement of objectives.

**The quality policy of DigiPlex**

Therefore, our reputation and capability to grow our business depends on our ability to provide products and services that are of a consistent, reliable and high quality, meeting or exceeding our customers’ needs and achieving customer satisfaction.

**We will:**

* Work closely with our customers to fully understand their needs and meet their expectations throughout the life of their contract with us.
* Set stretching objectives and targets which are focused on meeting the needs of our customers, our business and other stakeholders.
* Use all necessary resources – in a way that clearly allocates responsibilities relating to quality to appropriate staff – to make sure we meet the commitments we have made to our customers.
* Make sure our employees have adequate training and have the skills, knowledge and experience they need for their roles.
* Encourage effective teamwork and make sure staff feel empowered, accountable and understand how meeting their objectives will contribute to the success of their particular department and DigiPlex.
* Measure and report on our performance in managing our business and meeting our customers’ needs and use performance information to help us improve.
* Independently audit our management systems to confirm whether or not they are adequate for meeting any regulatory requirements as well as the needs of the business, our employees, our customers and others with an interest in our work.
* Use the outcomes of independent audits to help us to continuously improve and meet the needs of our customers.
* all employees and interested parties with relevant information and ensure a structured dialogue on how to improve the quality of our services.
* Regularly review the suitability and effectiveness of our systems to identify improvements that we need to make, to be more able to meet our needs and those of our customers and people who have an interest in our work.
* Develop effective relationships with our subcontractors and suppliers.

We put this policy into practice by applying policies, standards, operating procedures and processes so that we control the delivery of high-quality products and services that reliably and consistently meet our commitments to our customers.

**Objectives and strategy**

The objectives of the quality control efforts in DigiPlex are to ensure the customer feels assured and confident to undertake their day to day business without concern to the services they have purchased from us.

These objectives are achieved by raising the consciousness of quality within the corporate culture, and by establishing relevant measurements/metrics, systematic supervision and enforcement, and deviation management.

**Health and Safety**

DigiPlex is committed to making the work environment safe for its employees and others wherever we operate.  *As a minimum* DigiPlex comply with all applicable Laws and Regulations relating to health and safety in the workplace.  We inform our employees about procedures in place to protect them from generally recognised workplace hazards, using our Risk Assessment process, which ensures the wellbeing of all colleagues is not compromised and the equipment in use, is safe.  Regardless of the specific responsibility that may apply, it is the duty of every employee to co-operate in achieving compliance.  We immediately report dangerous conditions to prevent or otherwise minimise workplace accidents.  In day-to-day conditions, we integrate safety in whatever we do. To demonstrate our commitment all our data centres are certified to ISO 45001:2018

**Environmental vision**

To DigiPlex, environmental sustainability is about making responsible decisions that will reduce our business' negative impact on the environment. It is not simply about reducing the amount of waste we produce or using less energy but is concerned with developing processes that will lead to DigiPlex becoming completely sustainable in the future.  We believe Environmental Sustainability forces us to look beyond making short term gains and look at the long-term impact they are having on the natural world.

You need to consider not only the immediate impact your actions have on the environment, but the long

term implications as well. For example, when undertaking a project, you need to look at the environmental impact of the project’s entire lifecycle, from development to disposal before finalizing your designs.

As a responsible business, we are expected to lead in the area of environmental sustainability as we are considered

to be the biggest contributor and are very much in a position where we can make a significant difference.

We will work in partnership with others to promote environmental care, increasing understanding of environmental issues and disseminate good practice.  DigiPlex is certified to ISO 14001:2015 at all our Data centres.

**The Quality system**

DigiPlex supports our customer's competitive quest for best value and best practice. The centre is used by customers for applications ranging from disaster recovery through to frontline server space, and secure network control centres.

**Process orientation**

DigiPlex has adopted a process approach in the development and implementation of its management system for the provision of services. The aim of the management system is to enhance customer satisfaction by meeting customer requirements. In addition, each of the processes undertaken is controlled to reduce the impact of the company’s activities and services on the environment and to eliminate or minimise Health & Safety and Information Security risks to its employees and other interested parties. Continual improvement of the effectiveness and performance of the management system and processes is attained through performance measurement and the achievement of objectives.

**Management's responsibility**

It is the responsibility of the Chief Executive Officer (CEO) and his Senior Leadership Team (SLT) to identify the vision, direction and goals of the Company and to communicate these to staff. The SLT will lead, inspire and support their staff and promote excellence as the best way to achieve our objectives and report on progress.

The CEO oversees the development of the business plan for the Company. The plan is based on a shared understanding within the DigiPlex SLT of the critical areas of business strategy, the balance between commercial return and prudent risk-taking and the limits and boundaries beyond which risk is deemed unacceptable.

Once the business plan has been finalised, a commitment by each department is made to the achievement of the overall strategy. The business plan is regularly subjected to constructive challenge and examination to ensure it remains resilient and achievable.

To support management decisions and inform discussions with customers and other principal stakeholders, performance against strategic and operational targets is measured. The application of these performance measures provides a focus on what is important and provides the fundamentals for informed decision making.

**Resource management**

The management of people in DigiPlex is focused on the creation, development and leadership of highly engaged and competent teams linked with an integrated approach to change management. The human resource management process aims to ensure that teams have relevant and up to date skills for the work they are doing; work well together; effectively manage change and demonstrate DigiPlex’s culture and values in their dealings with customers, interested parties and with each other.

1. ***Commitment to Competence***

DigiPlex hiring managers define job requirements prior to recruiting, interviewing, and hiring. Job requirements include the primary responsibilities and tasks involved in the job, background skills needed to perform the job, and personal qualifications desired. Once the requirements are determined, managers create a job description, which is a profile of the job, and is used to identify potential candidates. When viable candidates are identified, the interview process begins to evaluate candidates and make an appropriate hiring decision.

DigiPlex employees create individual Core Priorities that align with those of their manager, organisation, and DigiPlex, and are supported with customer-centric actions and measures so that everyone is working toward the same overarching vision. These Core Priorities are established when an employee is hired, and then updated throughout the year during one-on-one career talks with their manager. The primary focus of the career talks is to assess employee performance against their priorities and to agree on an updated list of priorities going forward.

1. ***Personnel***

DigiPlex performs employee background screening on all new recruits. DigiPlex also employs a formal performance review process to ensure employees adequately meet the responsibilities of their position, including adherence to company policies, information security policies, and workplace rules. Hiring managers may, at their discretion, initiate corrective actions, up to and including immediate termination, if any aspect of an employee's performance and conduct is not satisfactory.

**Project Management**

Project Management processes and controls define the acceptable level of quality, which is typically agreed by the customer, and describes how the project will ensure this level of quality in its deliverables and work processes. This ensures that:

* Products are built to meet agreed- upon standards and requirements
* Work processes are performed efficiently and as documented
* Non-conformances found are identified and appropriate corrective action is taken

Project Managers liaise with relevant managers to determine customer, statutory and regulatory requirements and review these against the requirements related to the contract. The review is conducted before acceptance of an order or order amendment.

**Management review**

The CEO chairs a Management Review Meeting made up of members of the Senior Leadership Team as well as invited managers when required. The purpose of the meeting is to maximise the self-management of the business enabling the SLT to manage as a team, rather than just as individuals. The Company has an established auditor; their role being to ensure that the business has appropriate procedures to manage the risks to which the Company may be exposed.

**Information Security Management**

Information security requirements, policies, disaster recovery and continuity plans, and risk assessments are systematically reviewed. DigiPlex’s Information Security Management System (ISMS) is an internal management system where requirements, policies, disaster recovery and continuity plans, and risk assessments are systematically documented and updated.

**Certifications and compliance**

DigiPlex’s Management System is an integrated management system where requirements, policies, disaster recovery and continuity plans, and risk assessments are systematically documented and updated.

Policies, procedures and controls for the information security management have been designed using recognised frameworks and best practices such as ISO 27001, ISO 9001, ISO 14001, ISO 45001, ISO 23001, COBIT, ITIL and is ISO 27001, ISO 9001 ISO 14001 and ISO 45001 accredited.



.

**Regulatory compliance**

DigiPlex adhere to several regulatory and legal requirements with specific prerequisites for information security management and privacy of information and data.

**Independent security assessments**

DigiPlex collaborates with an independent security company to continuously assess and improve the operational environment from a technical security perspective and thus address staff awareness and the organisation’s ability to respond to security incidents.

Independent penetration testing and vulnerability assessments of the technical infrastructure are conducted periodically (annually or more frequently).

**Whistleblowing**

There is a confidential and anonymous Whistle Blowing Hotline available for both employees and suppliers to report issues. The hotline is accessible 24x7 through email, phone, and mail. The individual may also send a letter reporting the concern to DigiPlex’s Compliance and Assurance Director. Employees and Suppliers are instructed that it is their duty to promptly report any concerns of suspected or known violations of the Business Code of Conduct or the Supplier Code of Practice or other DigiPlex policies or guidelines. The procedures to be followed for such a report are outlined in the Code of Business Principles and Supplier code of Practice. Employees are also encouraged to communicate the issue to their manager, their manager’s manager, of the HR Director, or the Compliance Department.

## The components of the system used to provide the services

1. **Infrastructure**

DigiPlex’s data centre services are based on a set of requirements in terms of room/hardware rack space, UPS protection, power and physical and environmental security features. The infrastructure of the data centres are designed to ensure a secure and continuous operation in terms of redundant power systems, cooling and communication lines. Advanced systems for monitoring alarms, climate controls, power and networks are also vital elements of the systems and procedures that safeguard the physical and environmental protection of the data centre.

DigiPlex’s data centre have facilities that include the following physical and environmental security measures:

* Two-factor authentication for physical access
* 24/7/365 environmental monitoring (air temperature and humidity)
* Redundant cooling
* Redundant power supplies, diesel generator and UPS systems
* Redundant fibre optic internet links
* Fire detection extinguishing systems
* Leak detection systems

1. **People**

Our organisation employs 80+ people, and designs, builds and operates data centres in the Nordics. We specialise in delivering best-in-class services to our customers by delivering tailored, secure and resilient environments with the highest possible availability. As a result, DigiPlex is trusted by public and private customers alike – including security sensitive organisations such as government and financial institutions.

DigiPlex’s head office is located in Oslo.

1. **Processes and procedures**

The following processes are in place and formally documented to provide data centre colocation hosting Services to DigiPlex’s customers:

* Entity Level Controls
* Human Resource management
* Incident and Problem Management
* Information Security Management
* Operations management & Environmental Controls
* Physical Security and Access management
* Risk management
* Access management for customer's third-party suppliers
* Infrastructure Change Management
* Continuity Management

Descriptions of each of these are provided in the pages that follow:

**Entity Level controls**

All DigiPlex employees are accountable for understanding and adhering to the guidance contained in the DigiPlex’s Information Security Manual and any applicable supporting procedures. Individuals not employed by DigiPlex are also accountable for understanding and adhering to the guidance contained in the Information Security Policy, Manual and procedures.

Control Objective #1: Controls provide reasonable assurance that the management has established governance oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives

| Domain | Control Activity # | Control Activity Description |
| --- | --- | --- |
| Entity Level Controls | CA01 | DigiPlex has established ethical values applicable to the company and its employees, supported by governing documents and commitment are communicated by management. |
| Entity Level Controls | CA02 | The DigiPlex Code of Business Principles reflect a commitment to integrity and ethical business practices and regulatory compliance. They summarize the principles and policies that guide DigiPlex’s business activities and communicated to all employees via or Internet. |
| Entity Level Controls | CA03 | DigiPlex has established management reporting lines with defined organization structure for governance. |
| Entity Level Controls | CA04 | DigiPlex has established a formal process to communicate internal control responsibilities to all employees. |
| Entity Level Controls | CA05 | DigiPlex has established a whistle blower hotline enabling anonymous and confidential communication. |
| Entity Level Controls | CA06 | DigiPlex management has established a Balanced Scorecard to reflect business objectives, structure and processes. |

**Human Resources (HR)**

The management of people in DigiPlex is focused on the creation, development and leadership of highly engaged and competent teams linked with an integrated approach to change management. The human resource management process aims to ensure that teams have relevant and up to date skills for the work they are doing; work well together; effectively manage change and demonstrate DigiPlex’s culture and values in their dealings with customers, interested parties and with each other.

***Commitment to Competence***

DigiPlex hiring managers define job requirements prior to recruiting, interviewing, and hiring. Job requirements include the primary responsibilities and tasks involved in the job, background skills needed to perform the job, and personal qualifications desired. Once the requirements are determined, managers create a job description, which is a profile of the job, and is used to identify potential candidates. When viable candidates are identified, the interview process begins to evaluate candidates and make an appropriate hiring decision.

DigiPlex employees create individual Core Priorities that align with those of their manager, organisation, and DigiPlex, and are supported with customer-centric actions and measures so that everyone is working toward the same overarching vision. These Core Priorities are established when an employee is hired, and then updated throughout the year during one-on-one career talks with their manager. The primary focus of the career talks is to assess employee performance against their priorities and to agree on an updated list of priorities going forward.

***Personnel***

DigiPlex performs employee background screening on all new recruits. DigiPlex also employs a formal performance review process to ensure employees adequately meet the responsibilities of their position, including adherence to company policies, information security policies, and workplace rules. Hiring managers may, at their discretion, initiate corrective actions, up to and including immediate termination, if any aspect of an employee's performance and conduct is not satisfactory.

Control Objective #2: Controls provide reasonable assurance that the risk of human errors, theft, fraud or misuse of information is minimized.

| Domain | Control Activity # | Control Activity Description |
| --- | --- | --- |
| Human Resource Management | CA07 | DigiPlex has defined and documented roles and responsibilities for each level within the organization structure and the same is communicated to the employees |
| Human Resource Management | CA08 | Employees are required to sign Confidentiality Agreements consisting of Non-Disclosure Agreements (NDA), and duties of insider information. |
| Human Resource Management | CA09 | Disciplinary action is taken against Associates for violating Security Policy based on disciplinary procedures documented as part of the Information security policy . |
| Human Resource Management | CA10 | Background checks are carried out for employees at the time joining as per defined company procedures. |

**Incident and problem management**

**Incident Identification**

All incidents are either submitted to DigiPlex’s ticketing management system or detected by monitoring systems. Operations focuses on identifying and resolving incidents prior to any impact on the Customer’s business. Monitoring key infrastructure components is critical for the detection of incidents.

**Incident Logging**

Incidents are logged in a ticketing management system and are managed in accordance with contractually agreed response times. All relevant information is documented.

**Incident Categorization**

All incidents are categorized. Incidents may be re categorized later in the process if deemed necessary. The Operations department utilize categorization data to facilitate for trend analysis to support its problem management process.

**Incident Prioritization**

Incidents are prioritized based on impact and severity. Level 1 & 2 incidents are escalated immediately to the Major Incident Team.

**Initial Diagnosis**

When the incident has been logged, categorized and prioritize, an attempt to diagnose the issue to fully identify the symptoms is performed. Minor Incidents (Level3) will be typical handled and solved by DigiPlex Operations without escalation or involvement of the Senior Leadership Team. Level 1 and 2 Incidents will be escalated to the Major Incident Team or specialized Subject Matter Experts or manufactures of the equipment.

**Major Incidents**

Major Incidents have a higher degree of business impact and urgency. They therefore require a separate management process. If the initial diagnosis identifies the incident as major, this process is triggered.

Major incidents are managed by the Senior Leadership team (SLT). The SLT coordinates incident response activities, monitors development, and keeps affected parties informed on progress.

**Problem Management**

The Objective of DigiPlex’s problem management process is to ensure management of the lifecycle of all problems that happen or could happen in DigiPlex’s service deliveries. The primary objectives are to prevent problems and resulting incidents from happening, to eliminate recurring incidents , and to minimize the impact of incidents that cannot be prevented.

Control Objective #3: Controls provide reasonable assurance that problems and / or incidents are recorded and investigated for resolution in accordance with documented procedures.

| Domain | Control Activity # | Control Activity Description |
| --- | --- | --- |
| Incident and Problem Management | CA11 | DigiPlex has established procedures for responding to security incidents and periodic evaluation of these procedures. |
| Incident and Problem Management | CA12 | DigiPlex has established roles and responsibilities for the design, implementation, maintenance, and execution of the incident response procedures, including the use of external resources when necessary |
| Incident and Problem Management | CA13 | Procedure to classify incidents as problems have been defined and documented and a root cause analysis for problems is documented. |

**Information security management**

DigiPlex has a responsibility for safeguarding internal information and IT assets. As a result, the goal for DigiPlex’s information security efforts is to minimise the risk of security breaches, downtime and loss of data through systematic and risk-based control measures. DigiPlex’s information security management is the sum of all the measures, efforts and controls that exists in order to safeguard confidentiality, integrity and availability of information assets. This includes:

* Clearly defined roles and responsibilities for information security management
* Policies, procedures, and controls based on best-practices and renowned frameworks
* Periodic risk assessments
* Automation, standardization and security technologies
* Regulatory compliance
* Independent audits and security assessments

**Roles and responsibilities**

Roles and responsibilities for the information security efforts are clearly defined:

* The Chief Executive Officer is ultimately responsible for the information security management, and all of DigiPlex’s information security measures and efforts.
* The information security department is responsible for implementing and ensuring compliance with DigiPlex’s information security policy, and all supplementary policies, procedures, guidelines and regulatory requirements for the management of information security
* The heads of departments and line managers are responsible for collaboration with the information security department in order to ensure compliance with the information security principles described in DigiPlex’s information security policy
* All employees are responsible for following the guidelines and principles for information security as described in DigiPlex’s information security policy, and to use the information security department as a proactive partner in information security-related matters

Control Objective #4: Controls provide reasonable assurance that Information Security Policies and Procedures are documented, approved, communicated, and their compliance is monitored.

| Domain | Control Activity # | Control Activity Description |
| --- | --- | --- |
| Information Security Management | CA14 | DigiPlex' governing documents are documented, maintained and communicated in DigiPlex’s Information Security Management System (ISMS).  The following governing documents are revised at least annually and approved by management, and authorized by CEO or COO:  • Information Security policy statement  • Information Security Manual  • Legal register  • Business continuity policy statement  • Business continuity manual  • Crisis communication Plan  • Site business continuity plan  • Risk management, Asset risk register |

**Operations management and environmental controls**

The data centre is fully monitored 24/7 by a state-of-the-art Building Management System (BMS).

The BMS gives us full control over the respective data hall environmental parameters such as temperature, humidity and power. The BMS also provides alarms on all systems to the on-duty engineers.

Control Objective #5: Controls provide reasonable assurance that resources are made available and monitored as per the requirements of the operations

| Domain | Control Activity # | Control Activity Description |
| --- | --- | --- |
| Operations Management and Environmental Controls | CA15 | DigiPlex has identified and manages an inventory/ overview of information assets. |
| Operations Management and Environmental Controls | CA16 | DigiPlex has implemented detection measures to identify anomalies that could result from failure of environmental control systems, failure of electrical/power supply, fire, and water damage. |
| Operations Management and Environmental Controls | CA17 | DigiPlex operations team monitors and evaluates current processing capacity and use of system components on a continuous basis. Alerts are triggered when capacity thresholds are reached and mitigating actions are initiated. |
| Operations Management and Environmental Controls | CA18 | Appropriate fire detection & suppression systems are in implemented at data centres.  Fire detection and suppression systems are covered under annual maintenance contract with respective vendors. |
| Operations Management and Environmental Controls | CA19 | Fire detection and suppression systems are maintained as per the established maintenance schedule |

Control Objective #6: Controls provide reasonable assurance that appropriate measures are in place to protect the data centre premises and equipment from environmental hazards such as fire, excessive heating, electricity failure, water leakage, etc.

|  |  |  |
| --- | --- | --- |
| Domain | Control Activity # | Control Activity Description |
| Operations Management and Environmental Controls | CA20 | Appropriate HVAC controls are in place to maintain heat, ventilation and air conditioning in the data centre. Temperature controls & monitoring is in place  HVAC systems are covered under annual maintenance contract with respective vendors. |
| Operations Management and Environmental Controls | CA21 | HVAC systems are maintained as per the established maintenance schedule |
| Operations Management and Environmental Controls | CA22 | Uninterrupted Power System (UPS) and DGs are installed at the primary and secondary data centre facilities to provide uninterrupted power supply and ensure backup whenever there are any power interruptions.  UPS and DGs is covered under annual maintenance contract with respective vendors. |
| Operations Management and Environmental Controls | CA23 | UPS and DGs are maintained as per the established maintenance schedule |
| Operations Management and Environmental Controls | CA24 | Server rooms are constructed to protect server room equipment from environmental threats, e.g. overheating, power outage and excessive moisture: - Raised access floors and adequate leak detection systems - Different fire zones, the server rooms are their own fire zone |

**Physical Security and access management**

**Physical Security.**

The facilities are protected by high security perimeter fence. The risk for tailgating at the gate is avoided through the car trap with access control gates. Reception staff follow pre-defined procedures, and the cameras are used for monitoring and continuously log recording.

A man trap provides intruder protection of the data centre building. Advanced security surveillance camera systems monitor both indoors and outdoors. A proximity and PIN card access system is implemented throughout.

Customer modules may optionally benefit from additional biometric access control.

**Alarm system and Security personnel**

The data centres are protected by advanced external security systems including surveillance cameras and access card readers. DigiPlex use a security firm as an “emergency responder” to any incidents at the data centre sites. Security staff is operated 24/7/365, also monitoring the site grounds and car park areas of the facilities. All doors and windows at the facilities are protected with alarm systems. The data centre operates a multi-layer access security system.

**Access controls**

Access is monitored through manned security presence 24/7. Security operates from a purpose-built Operations Centre. Security personnel, together with reception staff, operate a rigorous identification system to allow access to customers and their nominated representatives without compromising security.

Security access cards to the common areas and dedicated customer areas are only issued on receipt of written instructions from the customer’s Level 1 contact.

The data centre premises have access control procedures that have been implemented in cooperation with our Customers. All new admissions must be approved by the Customer Contact. Only authorised personnel are granted access to the data centre. To obtain a valid access card, a written application form must be completed and approved by the Customer Authorised Signatory.

Access is only granted using written application forms. Access cards and associated codes are personal and non-transferable. The Customer is responsible for performing quarterly entitlement reviews of personnel with access to the data centre.

Visitors must be registered in the data centre’s electronic visitor’s register and escorted by authorised Customer personnel. At the end of the visit, visitors are required to sign out.

**Access management for customer's third-party suppliers**

Third-party suppliers are only granted access privileges necessary for them to be able to perform specific tasks as requested by the customer. Confirmation / approval of access must always be given in writing by the Customer Contact.

Control Objective #7: Controls provide reasonable assurance that access to the data centre premises and its assets is restricted physically and granted as per need-to-know basis

| Domain | Control Activity # | Control Activity Description |
| --- | --- | --- |
| Physical Security and Access Management | CA25 | Closed Circuit Television (CCTV) systems are installed at strategic locations at the entry and exit points of the data centre facilities to record all the events.   The CCTV systems are continuously monitored by the Physical Security team.   The CCTV equipment is maintained on a regular basis. |
| Physical Security and Access Management | CA26 | There are no windows or skylights in server rooms. All other openings (e.g. ventilation) are properly blocked or locked. |
| Physical Security and Access Management | CA27 | The data centres are equipped with access control and alarm systems in order to detect unauthorized access to the data centre premises. |
| Physical Security and Access Management | CA28 | The access control and alarm systems are regularly maintained as per defined scheduled. |
| Physical Security and Access Management | CA29 | DigiPlex has established and documented procedures for access creation and revocation to the data centre facilities as per 'Security Manual' |
| Physical Security and Access Management | CA30 | Access to data centre facilities is revoked on the last working day of resigned/terminated employee.   Customer access is revoked based on intimation from authorized customer personnel through ticket in Service Now. |
| Physical Security and Access Management | CA31 | DigiPlex has processes in place to periodically review physical access to ensure consistency with job responsibilities. |
| Physical Security and Access Management | CA32 | Two factor authentication mechanism is established to access the data centre. E.g. swipe card and biometric or Proximity and biometric based access control systems |
| Physical Security and Access Management | CA33 | The data centre facilities are manned by trained Security Guards round the clock, for restricting access to authorized individuals. |
| Physical Security and Access Management | CA34 | Entry and exit details of the visitors accessing the data centre facilities are logged and documented. Access to visitors is granted only after obtaining appropriate approvals from designated personnel in the management All visitors must be escorted by an authorized person while on the premises. |
| Physical Security and Access Management | CA35 | Movements of materials within the data centre is monitored and tracked, logged and only permitted with proper authorization |
| Physical Security and Access Management | CA36 | Access to data centre facilities is granted to DigiPlex employees based on approvals as per the 'access management procedures'.  Access to customers is granted based on approvals from authorized customer personnel through tickets documented in Service Now. |
| Physical Security and Access Management | CA37 | There are formal processes for managing and controlling access to mechanical keys including: - Mechanical keys are kept in a hidden and physical secured lockbox at each location (separate systems) - Access to mechanical keys are restricted to a limited number of authorized personnel. Access to specific keys is granted based on needs - Code and fingerprint are required to gain access to lockbox |

**Risk management**

DigiPlex continuously assesses and improves its information security measures and efforts in order to reduce the risk of commercial repercussions for its customers in connection with the following security breach scenarios:

* **Confidentiality:** Unauthorised access to data due to weak information security and access management controls, cyber-attacks, theft or deliberate attack on DigiPlex’s infrastructure
* **Availability:** Unavailable systems or data caused by downtime, system failure, fire, theft and internal procedures
* **Integrity:** DigiPlex performs periodic risk assessments in order to identify and address information security risks in an operational environment that is continuously subject to development and change. The risk assessments’ results are summarised in reports with recommended actions for improvement. The reports are communicated to the information security department and upper management and used by them for prioritising future security efforts and measures.

Control Objective #8: Controls provide reasonable assurance that the company has established a risk management framework to identify, assess, mitigate and remediate risks to the services provided to the customers and organization as a whole.

| Domain | Control Activity # | Control Activity Description |
| --- | --- | --- |
| Risk Management | CA38 | DigiPlex' risk identification and assessment process includes (1) identifying information assets (physical), (2) assessing the criticality of those information assets, (3) identifying the threats to the assets (intentional, unintentional and environmental), and (4) identifying the vulnerabilities of the identified assets. |
| Risk Management | CA39 | Risks identified during risk assessment are documented and mitigating procedures are initiated. |

**Third Party Management**

The DigiPlex Code of Practice for Suppliers (“the Code”) defines the non-negotiable minimum standards that we ask our suppliers and their sub-tier suppliers (“the Supplier”), to respect and to adhere to when conducting business with DigiPlex. This document helps the continued implementation of our commitment to international standards such as the 10 Principles of the United Nations Global Compact, beyond our own operation. The Supplier Code of Practice reflects what expectations DigiPlex requires from outsources service providers with regard to integrity and ethical business practices

Security requirements for the subcontractors are agreed in service agreements, which include statements on the rights and obligations of both parties and a confidentiality agreement, if there is a possibility that the subcontractor personnel can see confidential information.

Control Objective #9: Controls provide reasonable assurance that system requirements, boundaries of the system, ,roles and responsibilities, and performance requirements are formally defined and documented with third party service providers. Compliance to service level agreements with third parties is monitored periodically by the management.

| Domain | Control Activity # | Control Activity Description |
| --- | --- | --- |
| Third party management | CA40 | Security requirements for the subcontractors are agreed in service agreements, which include statements on the rights and obligations of both parties and a confidentiality agreement, if there is a possibility that the subcontractor personnel can see confidential information. |
| Third party management | CA41 | The Supplier Code of Practice reflects what expectations DigiPlex requires from outsources service providers with regard to integrity and ethical business practices |

**Infrastructure change management**

Our clients depend upon us to deliver a service that provides a secure, humidity and temperature-controlled environment, with robust diverse power supplies.  Protection of the environment is therefore a key operational function. The Service Change Management process is designed to protect the service environment by ensuring that any activities that have the potential to affect that environment are risk mitigated before Approval is granted and are reviewed once completed to identify any lessons that might be learned.

Control objective #10:

Controls provide reasonable assurance that changes performed to infrastructure follow defined change management procedures to prevent unauthorized changes to the environment.

| Domain | Control Activity # | Control Activity Description |
| --- | --- | --- |
| Infrastructure Change Management | CA42 | DigiPlex has established and documented a change management process which is approved by the 'designation'.  Changes are raised, classified, tracked and approved in Service Now ticketing system. |

**Continuity management**

Dealing with a crisis is the most demanding challenge likely to face DigiPlex. The crisis may result from a fire or flood affecting the company's business continuity, a major accident or some form of business crisis. The ability to manage the crisis effectively, to handle the media issues and to restore normal operation will determine whether DigiPlex survives the experience.

**Business continuity** encompasses planning and preparation to ensure that DigiPlex can continue to operate in case of serious incidents or disasters and is able to recover to an operational state within a reasonably short period. As such, DigiPlex’s business continuity includes three key elements and they are

1. **Resilience**: critical business functions and the supporting infrastructure must be designed in such a way that they are materially unaffected by relevant disruptions, for example through the use of redundancy and spare capacity;
2. **Recovery**: arrangements have to be made to recover or restore critical and less critical business functions that fail for some reason.
3. **Contingency:** DigiPlex has established a generalised capability and readiness to cope effectively with whatever major incidents and disasters occur, including those that were not, and perhaps could not have been, foreseen. Contingency preparations constitute a last-resort response if resilience and recovery arrangements should prove inadequate in practice.

DigiPlex will respond effectively to a crisis in whatever form it might take, establishes initial procedures and defines key responsibilities for the appropriate response to business disruptions that might threaten personnel, buildings, daily operations, DigiPlex’s and customer reputation. Each Datacentre has a Site Business Continuity Plan

The principles behind this plan are:

* Risks are assessed for both probability and business impact
* Emergency Response Plans must be reasonable, practical and achievable
* Our plans can be interwoven with our customers plans

In other words, we are not planning for every possibility. Diminishing returns affect the benefits of planning for extreme cases.

Other functions of the Site Business Continuity Plan are as follows:

* Describe preventive measures that decrease the risk of a crisis event.
* Promote personal accountability and responsibility and the safe evacuation/invacuation of individuals.
* Lessen the possible impact on our operations.
* Establish procedures that can help us quickly and correctly deal with an emergency or crisis situation.
* Establish a process of regularly training and testing of our emergency response plans.
* Learning Lessons from every practice.

**Covid-19**

On the 5th March 2020 Digiplex activated its Coronavirus /Pandemic Influenza – Business Continuity Plan. This plan was shared with our customers are Suppliers.

For our purposes, to manage this crisis we developed an Alert state.

|  |
| --- |
| Alert Level Green |
| Alert Level Yellow |
| Alert Level Amber |
| Alert Level Red |

DigiPlex has operated at Alert state Yellow initially. On the 12th March the Norwegian Government launched its Covid-19 response plan. We are currently operating at Alert State Amber.

Overall, although the COVID-19 pandemic has led to significant changes in the way we go about our daily lives, and has dramatically altered how we work, it has also illustrated the resilience, flexibility and positive attitude of our employees. Not only have we delivered all that we set out to in 2020, but we have, in several cases, improved processes and found better ways of working. We are a very social company, and people undoubtedly missed the in-person interactions in the office and outside of it – and we are committed to returning to this experience as soon as we can. However, morale has been kept high and engagement even increased by clever use of digital and social technologies and deep commitment to the company culture.

In spite of the global pandemic, in the last nine months we have not only grown our headcount by 30%, hiring 25 new members of the DigiPlex Team, but opened two new data centers in Norway. An additional facility at our Fetsund campus and a brand-new campus site in Hobøl, Holtskogen. Both projects were delivered on time for the respective customers. The quick buildout of our data center portfolio underlines our ability to deliver against the high demands for speed, resource, and capability.

Control Objective #11: Controls provide reasonable assurance that organization has documented and implemented Business Continuity plan and Disaster recovery measures in place to ensure minimal impact to operations in case of a disaster

| Domain | Control Activity # | Control Activity Description |
| --- | --- | --- |
| Continuity Management | CA43 | DigiPlex has established and documented Business Continuity and Disaster Recovery plan |
| Continuity Management | CA44 | DigiPlex has implemented testing of the Business Continuity Plan, this is performed on a periodic basis. The testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of system components from across the entity that can impair the availability; (3) scenarios that consider the potential for the lack of availability of key personnel; and (4) revision of continuity plans and systems based on test results. |

## Incidents occurring in the 12 months prior to reporting as of date that resulted in a significant impairment of DigiPlex’s ability to achieve its service commitments and system requirements

There were no incidents occurring in the 12 months prior to reporting as of date that resulted in a significant impairment of DigiPlex’s ability to achieve its service commitments and system requirements.

## Complementary user entity controls

Controls at DigiPlex relating to data centre colocation hosting services provided to user entities, cover only a portion of the overall internal control structure of user entities. The control objectives cannot be achieved without taking into consideration operating effectiveness of controls at DigiPlex as well as controls at the user entity. Therefore, user entities internal control structure must be evaluated in conjunction with DigiPlex’s control policies and procedures, and the results of testing summarized in Section 4 of this report.

This section highlights those internal control structure responsibilities that the DigiPlex believes should be present at the user entity, and which DigiPlex has considered in developing its control structure policies and the procedures described in this report. In order to rely on the control structure policies and procedures reported herein, the user entity and their auditors should evaluate user entities internal control structure to determine if the CUECs mentioned below or similar procedures are in place and operating effectively.

User entity is responsible for defining and implementing CUECs provided in sub-section 3.7, These controls address the interface and communication between user entities and DigiPlex and are not intended to be a complete listing of the controls related to the financial statements of user entities.

User entities are responsible for implementing and maintaining effective internal controls that extend beyond those covered in this report, including, but not limited to the following:

* + 1. User entities are responsible for assessing risk related to the operation of the User entity and the information specific to the User entity stored and processed by DigiPlex (User entity risk assessment)
    2. User entities are responsible for deciding the type and level of services, including security services, delivered by DigiPlex based on their risk assessment, risk appetite, and budget.
    3. User entities are responsible for requesting, controlling, and revoking access and privileges to users acting on behalf of the User entity. User entities are responsible for sending authorized visitor requests to DigiPlex.
    4. User entities are responsible for raising required goods ticket, for receipt of material.
    5. User entities are responsible for approving changes that effect their environment.
    6. User entities are responsible for keeping DigiPlex informed about User entity contact information, including authorized requesters and escalation points.

## Complementary subservice organization controls

Controls at DigiPlex related to data centre colocation hosting services for the period 01 January 2019 to 31 December 2019 (the “Description”) provided to clients (‘User Organizations’ or ‘User Entities’) cover the overall internal control structure of service organization and does not use any subservice organization.

# 

# Section Four – Information provided by the service auditor

## Introduction

This report is intended to provide user entities with information about the controls at DigiPlex that may affect the processing of user entity transactions and also to provide users with information about the operating effectiveness of the controls that were tested. This report, when combined with an understanding and assessment of the controls at user entity, is intended to assist user entities auditors in (1) planning the audit of user entities financial statements and in (2) assessing control risk for assertions in user entities financial statements that may be affected by controls at DigiPlex.

Our testing of DigiPlex’s controls was restricted to the control objectives and related controls listed in Section 4.3 of the report and were not extended to controls described in system description but not included in the aforementioned section, or to controls that may be in effect at the user entity, as referred in section 3.7. It is user entities auditor’s responsibility to evaluate this information in relation to the controls in place at the user entity. If certain complementary controls are not in place at user entity, DigiPlex’s controls may not compensate for such weaknesses.

## Control environment elements

In addition to the tests of operating effectiveness of the controls in the matrices in this section of the report, our procedures included tests of the following relevant elements of DigiPlex’s control environment:

* DigiPlex’s Board of Directors;
* Human Resources Policies and Practices;
* Corporate Internal Audit Function;
* Risk Management;
* Monitoring.

Our procedures included testing those relevant elements of the control environment that we considered necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. We have considered the details of the control environment as provided by DigiPlex in its management assertion, in the tests of operating effectiveness.

Our tests of the control environment included inquiry of appropriate management, supervisory, and staff personnel, and inspection of DigiPlex’s documents and records. The control environment was considered in determining the nature, timing, and extent of the tests of operating effectiveness of controls.

## Test of Operating Effectiveness

Our tests of effectiveness of the controls included such tests as we considered necessary in the circumstances to evaluate whether those controls, and the extent of compliance with them, was sufficient to provide reasonable, but not absolute, assurance that the specified control objectives were achieved during the period from January 1, 2019 to December 31, 2019. Our tests of the operational effectiveness of controls were designed to cover a representative number of transactions throughout the period of January 1, 2019 to December 31, 2019, for each of the controls listed in this section, which are designed to achieve the specific control objectives. In selecting particular tests of the operational effectiveness of controls, we considered (a) the nature of the items being tested, (b) the types of available evidential matter, (c) the nature of the audit objectives to be achieved (d) the assessed level of control risk and, (e) the expected efficiency and effectiveness of the test.

**Description of Testing Procedures Performed**

As a part of the examination of DigiPlex’s controls, Deloitte has performed a variety of tests, each of which provided the basis for understanding the framework for controls, and determined whether the controls supporting processing, which DigiPlex represented were in operation, were actually in place and operating effectively with respect to the processing of transactions in accordance with DigiPlex’s controls during the period from 01 January, 2019 to 31 December 2019.

The types of tests performed of operational effectiveness of controls detailed in this section are described below:

|  |  |
| --- | --- |
| Test | Description |
| Corroborative inquiry | Made inquiries of appropriate personnel and corroborated responses with other personnel to ascertain the compliance of controls. |
| Observation | Observed application of specific controls. |
| Examination of documentation | Inspected documents and reports indicating performance of the controls. |
| Re-performance | Re-performed application of the controls. |

**Results of Testing Procedures Performed**

The results of the testing of the control environment and controls were sufficient to conclude that controls were operating effectively to provide reasonable, but not absolute, assurance that the control objectives were achieved during the period from 01 January 2019 to 31 December 2019.

It is each interested party’s responsibility to evaluate this information in relation to internal controls in place at each user organization in order to assess the total system of internal control. If it is concluded that the user organization does not have effective internal controls in place, DigiPlex’s internal controls may not compensate for such weaknesses.

[Space left blank intentionally]

**Entity Level Controls (ELC)**

**Control Objective #1:** Controls provide reasonable assurance that the management has established governance oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives

| **Control Activity** | | **Tests Performed** | **CUEC** | **Test Result** |
| --- | --- | --- | --- | --- |
| CA01 | DigiPlex has established ethical values applicable to the company and its employees, supported by governing documents and commitment are communicated by management. | Confirmed via corroborative inquiry with the HR Manager, Compliance and Assurance Director that DigiPlex had established the ethical values applicable to the company and its employees, supported by governing documents and commitment are communicated by management.  Obtained and inspected the ‘Group Management Plan’ document which described the ethical values applicable to the company and its employees and the same was communicated to the employees through intranet portal by the management. | None | No exceptions noted |
| CA02 | The DigiPlex Code of Business Principles reflect a commitment to integrity and ethical business practices and regulatory compliance. They summarize the principles and policies that guide DigiPlex’s business activities and communicated to all employees via or Internet. | Confirmed via corroborative inquiry with the HR Manager, Compliance and Assurance Director that DigiPlex has established a Code of Business Principles that reflected a commitment to integrity and ethical business practices and regulatory compliance.  Obtained and inspected the ‘Code of Business Principles’ document which reflected the integrity and ethical business practices and regulatory compliance commitments of the company. Further noted that the principles guide DigiPlex’s business activities and were communicated to employees over the intranet portal. | None | No exceptions noted |
| CA03 | DigiPlex has established management reporting lines with defined organization structure for governance. | Confirmed via corroborative inquiry with the HR Manager and Compliance and Assurance Director that DigiPlex has established management reporting lines with defined organization structure for governance.  Obtained and inspected the company organization chart with roles and responsibilities document to note that DigiPlex has established management reporting lines with defined organization structure for governance. | None | No exceptions noted |
| CA04 | DigiPlex has established a formal process to communicate internal control responsibilities to all employees. | Confirmed via corroborative inquiry with the with the HR Manager and Compliance and Assurance Director that DigiPlex had established a formal process to communicate internal control responsibilities to all employees.  Inspected the roles and responsibilities description available on the company’s intranet site which was accessible to all employees. | None | No exceptions noted |
| CA05 | DigiPlex has established a whistle blower hotline enabling anonymous and confidential communication. | Confirmed via corroborative inquiry with the HR Manager and Compliance and Assurance Director that DigiPlex had established a whistle blower hotline enabling anonymous and confidential communication.  Observed the whistle blower policy to note that confidential communication lines were established by the company. | None | No exceptions noted |
| CA06 | DigiPlex management has established a Balanced Scorecard to reflect business objectives, structure and processes. | Confirmed via corroborative inquiry with the Compliance and Assurance Director that DigiPlex management had established a Balanced Scorecard to reflect business objectives, structure and processes.  Obtained and inspected the 'Objective and Target Setting Review’ process along with KPI reports comprising of performance scorecards to note that management had established a Balanced Scorecard to reflect business objectives, structure and processes. | None | No exceptions noted |

**Human Resource Management (HR)**

**Control Objective #2:** Controls provide reasonable assurance that the risk of human errors, theft, fraud or misuse of information is minimized.

| **Control Activity** | | **Tests Performed** | **CUEC** | **Test Result** |
| --- | --- | --- | --- | --- |
| CA07 | DigiPlex has defined and documented roles and responsibilities for each level within the organization structure and the same is communicated to the employees | Confirmed via corroborative inquiry with the Compliance and Assurance Director that DigiPlex had defined and documented roles and responsibilities for each level within the organization structure and the same is communicated to the employees.  Obtained and inspected the company organization chart with roles and responsibilities document to note that DigiPlex had defined and documented roles and responsibilities for each level within the organization structure and the same is communicated to the employees | None | No exceptions noted |
| CA08 | Employees are required to sign Confidentiality Agreements consisting of Non-Disclosure Agreements (NDA), and duties of insider information. | Confirmed via corroborative inquiry with the HR Manager that DigiPlex employees are required to sign Confidentiality Agreements consisting of Non-Disclosure Agreements (NDA), and duties of insider information.  Inspected for sample employees, the signed confidentiality agreements consisting of NDA and awareness about insider information to confirm that employees signed Confidentiality Agreements consisting of Non-Disclosure Agreements (NDA), and duties of insider information. | None | No exceptions noted |
| CA09 | Disciplinary action is taken against Associates for violating Security Policy based on disciplinary procedures documented as part of the Information security policy . | Confirmed via corroborative inquiry with the HR Manager that disciplinary procedures were documented and no instances of disciplinary actions occurred during the review period for violating security. | None | No instances noted during the review period |
| CA10 | Background checks are carried out for employees at the time joining as per defined company procedures. | Confirmed via corroborative inquiry with the HR Manager and Compliance and Assurance Director that DigiPlex background checks were carried out for employees at the time joining as per defined company procedures.  Inspected for sample new joiners, the background check reports to confirm whether the background checks were performed for employees as per defined company procedures. | None | No exceptions noted |

**Incident and Problem Management**

**Control Objective #3:** Controls provide reasonable assurance that problems and / or incidents are recorded and investigated for resolution in accordance with documented procedures.

| **Control Activity** | | **Tests Performed** | **CUEC** | **Test Result** |
| --- | --- | --- | --- | --- |
| CA11 | DigiPlex has established procedures for responding to security incidents and periodic evaluation of these procedures. | Confirmed via corroborative inquiry the Compliance and Assurance Director and the Head of Security that DigiPlex had established procedures for responding to security incidents and periodic evaluation of these procedures.  Obtained and inspected the Incident management policy for the organization which encompassed the procedures on responding to security incidents and the same were reviewed on an annual basis by the management for updates, if any. | None | No exceptions noted |
| CA12 | DigiPlex has established roles and responsibilities for the design, implementation, maintenance, and execution of the incident response procedures, including the use of external resources when necessary | Confirmed via corroborative inquiry the Compliance and Assurance Director that DigiPlex had established roles and responsibilities for the design, implementation, maintenance, and execution of the incident response procedures, including the use of external resources when necessary.  Obtained and inspected the Incident management policy for the organization which included roles and responsibilities for the design, implementation, maintenance and execution of the incidents response procedures and the same was communicated to the employees in form of their job description. Further noted that the document included an owner and Business Improvement Manager with details of the procedure in the following sections:  1. Purpose of incident management  2. Definition  3. Scope  4. Role Descriptions  5. Process overview | 3.7.6 | No exceptions noted |
| CA13 | Procedure to classify incidents as problems have been defined and documented and a root cause analysis for problems is documented. | Confirmed via corroborative inquiry the Compliance and Assurance Director that DigiPlex had established procedures to classify incidents as pro and a root cause analysis for problems was documented.  Obtained and inspected the Incident management policy for the organization and noted incidents classified as Major were considered as Problems. Obtained and inspected the “Major Incident” plan which included procedures to establish and document to establish root cause and track any lessons learnt. | None | No exceptions identified |

**Information Security Management**

**Control Objective #4:** Controls provide reasonable assurance that Information Security Policies and Procedures are documented, approved, communicated, and their compliance is monitored.

| **Control Activity** | | **Tests Performed** | **CUEC** | **Test Result** |
| --- | --- | --- | --- | --- |
| CA14 | DigiPlex' governing documents are documented, maintained and communicated in DigiPlex’s Information Security Management System (ISMS).  The following governing documents are revised at least annually and approved by management, and authorized by CEO or COO:  • Information Security policy statement  • Information Security Manual  • Legal register  • Business continuity policy statement  • Business continuity manual  • Crisis communication Plan  • Site business continuity plan  • Risk management, Asset risk register | Confirmed via corroborative inquiry with Head of Security that DigiPlex has established ethical values applicable to the company and its employees, supported by governing documents and commitment were communicated by the management.  Obtained and inspected the following governing documents  • Information Security policy statement  • Information Security Manual  • Legal register  • Business continuity policy statement  • Business continuity manual  • Crisis communication Plan  • Site business continuity plan  • Risk management, Asset risk register  and noted they were all approved and revised within their respective intervals and authorized by the CEO/ COO as applicable.  Further noted that the governing documents were communicated on the intranet portal of the company. | None | No exceptions noted |

**Operations Management and Environmental Controls**

**Control Objective #5:** Controls provide reasonable assurance that resources are made available and monitored as per the requirements of the operations

| **Control Activity** | | **Tests Performed** | **CUEC** | **Test Result** |
| --- | --- | --- | --- | --- |
| CA15 | DigiPlex has identified and manages an inventory/ overview of information assets. | Confirmed via corroborative inquiry with Head of Security that DigiPlex had identified and managed an inventory/ overview of information assets.  Obtained and inspected the "Guidance on Asset Identification & Risk Management" and noted that document included the following:  - Ch 5: Responsibilities  - Ch 6: Overview  - Ch 7: Procedure  - Ch 8: New asset and risk identification  - Ch 9: Measurement  - Ch 10: Forms and templates  - Ch 11: Records and retention  Further obtained and inspected the "DigiPlex Asset Risk Register". Noted that the document includes a list of information assets, listing the attributes such as Information asset reference number, category, Asset, Asset owner, Description, Asset type/format, Classification, Highest score, Security Classification Level, Date added, Review date, Next review, Information/remarks, etc.  Further noted that the document also includes a tab "RA Tool" which includes a more detailed risk analysis for assets. | None | No exceptions noted |
| CA16 | DigiPlex has implemented detection measures to identify anomalies that could result from failure of environmental control systems, failure of electrical/power supply, fire, and water damage. | Confirmed via corroborative inquiry with Data Centre Managers of all data centres in scope and Head of Security that DigiPlex has implemented detection measures to identify anomalies that could result from failure of environmental control systems, failure of electrical/power supply, fire, and water damage.    Observed during site visit that systems used to detect and monitor anomalies in the data centre are BMS monitoring system to monitor the alarms configured to detect anomalies in the environment of the data centre that could result from failure of environmental control systems, failure of electrical/power supply, fire, and water damage. The BMS console was monitored by on ground support team on site and any deviations were addressed. | None | No exceptions noted |
| CA17 | DigiPlex operations team monitors and evaluates current processing capacity and use of system components on a continuous basis. Alerts are triggered when capacity thresholds are reached and mitigating actions are initiated. | Confirmed via corroborative inquiry with Data Centre Managers during site visits that DigiPlex operations team monitors and evaluated current processing capacity and use of system components on a continuous basis. Alerts are triggered when capacity thresholds were reached and mitigating actions were initiated.  Obtained and inspected a screenshot of the capacity management tool and noted that capacity were being monitored.  Observed during site visit that operations team monitored and evaluated current processing capacity and use of system components on a continuous basis through BMS monitoring system and other capacity monitoring alarms configured on the equipment as per defined thresholds. Alerts were triggered when capacity thresholds are reached and mitigating actions were initiated. | None | No exceptions noted |
| CA18 | Appropriate fire detection & suppression systems are in implemented at data centres.  Fire detection and suppression systems are covered under annual maintenance contract with respective vendors. | Confirmed via corroborative inquiry with data centre managers that DigiPlex had appropriate fire detection & suppression systems are in implemented at the data centres and the fire detection and suppression systems were covered under annual maintenance contract with respective vendors.  Observed on site that appropriate fire detection and suppression systems were installed at the data centre premises. Further obtained and inspected the annual maintenance contracts agreed with the service vendors for the equipment to confirm whether the equipment was covered under annual maintenance contract. | None | No exceptions noted |
| CA19 | Fire detection and suppression systems are maintained as per the established maintenance schedule | Confirmed via corroborative inquiry with data centre managers that fire detection and suppression systems were maintained as per the established maintenance schedule.  Obtained and inspected the periodic maintenance reports for the fire detection and suppressions systems installed at the data centres along with the maintenance contracts to confirm that the equipment was maintained regularly as per the frequency agreed with the service vendors. | None | No exceptions noted |

**Control Objective #6:** Controls provide reasonable assurance that appropriate measures are in place to protect the data centre premises and equipment from environmental hazards such as fire, excessive heating, electricity failure, water leakage, etc.

| **Control Activity** | | **Tests Performed** | **CUEC** | **Test Result** |
| --- | --- | --- | --- | --- |
| CA20 | Appropriate HVAC controls are in place to maintain heat, ventilation and air conditioning in the data centre. Temperature controls & monitoring is in place  HVAC systems are covered under annual maintenance contract with respective vendors. | Confirmed via corroborative inquiry with data centre managers that DigiPlex had appropriate HVAC controls were in place to maintain heat, ventilation and air conditioning in the data centre. Also, temperature controls and monitoring mechanism was in place.  Observed on site that appropriate HVAC equipment were installed at the data centre premises. Further obtained and inspected the annual maintenance contracts agreed with the service vendors for the equipment to confirm whether the equipment was covered under annual maintenance contract. | 3.7.7 | No exceptions noted |
| CA21 | HVAC systems are maintained as per the established maintenance schedule | Confirmed via corroborative inquiry with data centre managers that HVAC equipment were maintained as per the established maintenance schedule.  Obtained and inspected the periodic maintenance reports for the HVAC equipment installed at the data centres along with the maintenance contracts to confirm that the equipment was maintained regularly as per the frequency agreed with the service vendors. | None | No exceptions noted |
| CA22 | Uninterrupted Power System (UPS) and DGs are installed at the primary and secondary data centre facilities to provide uninterrupted power supply and ensure backup whenever there are any power interruptions.  UPS and DGs is covered under annual maintenance contract with respective vendors. | Confirmed via corroborative inquiry with data centre managers that DigiPlex had appropriate uninterrupted power systems (UPS) and diesel generator (DG) were installed at the primary and secondary data centre facilities to provide uninterrupted power supply and ensure backup whenever there are any power interruptions.  Observed on site that appropriate UPS and DG equipment were installed at the data centre premises. Further obtained and inspected the annual maintenance contracts agreed with the service vendors for the equipment to confirm whether the equipment was covered under annual maintenance contract. | None | No exceptions noted |
| CA23 | UPS and DGs are maintained as per the established maintenance schedule | Confirmed via corroborative inquiry with data centre managers that UPS and DG equipment were maintained as per the established maintenance schedule.  Obtained and inspected the periodic maintenance reports for the UPS and DG equipment installed at the data centres along with the maintenance contracts to confirm that the equipment was maintained regularly as per the frequency agreed with the service vendors. | None | No exceptions noted |
| CA24 | Server rooms are constructed to protect server room equipment from environmental threats, e.g. overheating, power outage and excessive moisture: - Raised access floors and adequate leak detection systems - Different fire zones, the server rooms are their own fire zone | Confirmed via corroborative inquiry with the data centre managers that server rooms were constructed to protect server room equipment from environmental threats, e.g. overheating, power outage and excessive moisture, through:  - Raised access floors and adequate leak detection systems - Different fire zones, the server rooms are their own fire zone.  Observed during site visits at the data centres that server rooms were constructed to protect server room equipment from environmental threats, e.g. overheating, power outage and excessive moisture and used the following mechanism:  - Raised access floors and adequate leak detection systems - Different fire zones, where the server rooms were their own fire zone. | None | No exceptions noted |

**Physical Security and access management**

**Control Objective #7:** Controls provide reasonable assurance that access to the data centre premises and its assets is restricted physically and granted as per need-to-know basis

| **Control Activity** | | **Tests Performed** | **CUEC** | **Test Result** |
| --- | --- | --- | --- | --- |
| CA25 | Closed Circuit Television (CCTV) systems are installed at strategic locations at the entry and exit points of the data centre facilities to record all the events.   The CCTV systems are continuously monitored by the Physical Security team.   The CCTV equipment is maintained on a regular basis. | Confirmed via corroborative inquiry with the data centre managers and head of security that closed-circuit television (CCTV) systems were installed at strategic locations at the entry and exit points of the data centre facilities to record all the events.  Observed during site visits at the data centres that the CCTV systems were continuously monitored by the physical security team present at the data centre premises.  Obtained and inspected the annual maintenance contract and periodic maintenance reports for the CCTV equipment to confirm where the CCTV equipment was  regularly maintained. | None | Exceptions noted.  Please refer subsection IV - ‘Findings and Observations’ for more details |
| CA26 | There are no windows or skylights in server rooms. All other openings (e.g. ventilation) are properly blocked or locked. | Confirmed via corroborative inquiry with the data centre managers and head of security that there were no windows or skylights in server rooms. All other openings (e.g. ventilation) were properly blocked or locked.  Observed during site visits at the data centres that there were no windows or skylights in server rooms and all other openings (e.g. ventilation) were properly blocked or locked. | None | No exceptions noted |
| CA27 | The data centres are equipped with access control and alarm systems in order to detect unauthorized access to the data centre premises. | Confirmed via corroborative inquiry with the data centre managers and head of security that the data centres were equipped with access control and alarm systems in order to detect unauthorized access to the data centre premises.  Observed during site visits at the data centres that the data centres were equipped with access control systems which required access card and pass code (2 factor) to get access and to detect any unauthorized access, alarm systems were in place which were monitored by physical security. | None | No exceptions noted |
| CA28 | The access control and alarm systems are regularly maintained as per defined scheduled. | Confirmed via corroborative inquiry with the data centre managers and head of security that the access control systems and alarm systems were regularly maintained as per defined scheduled.  Obtained and inspected the annual maintenance contract and periodic maintenance reports for the access control equipment and alarm systems to confirm where the equipment was  regularly maintained as per defined schedule. | None | No exceptions noted |
| CA29 | DigiPlex has established and documented procedures for access creation and revocation to the data centre facilities as per 'Security Manual' | Confirmed via corroborative inquiry with the data centre managers and head of security that DigiPlex had established and documented procedures for access creation and revocation to the data centre facilities as per 'Security Manual'.  Obtained and inspected the ‘Security Manual’ document for each site in scope and noted that procedures for access creation and revocation were documented by DigiPlex. | None | No exceptions noted |
| CA30 | Access to data centre facilities is revoked on the last working day of resigned/terminated employee.  Customer access is revoked based on intimation from authorized customer personnel through ticket in Service Now. | Confirmed via corroborative inquiry with the data centre managers and head of security that access to data centre facilities for DigiPlex employees was revoked on the last working day of resigned/terminated employee. Further confirmed that customer access to the data centre premises was revoked based on intimation from authorized customer personnel through ticket in Service Now.  Obtained the list of resigned employees at DigiPlex and inspected the access revocation date and time stamp at the data centre to confirm whether the access was revoked on the last working day of the resigned/ terminated employee.  Obtained the list of customer requests raised in Service Now for revocation of access for customer representatives and noted that the request was raised by authorized customer personnel and followed to closure after revoking the access. | 3.7.3 | Exceptions noted.  Please refer subsection IV - ‘Findings and Observations’ for more details |
| CA31 | DigiPlex has processes in place to periodically review physical access to ensure consistency with job responsibilities. | Confirmed via corroborative inquiry with the data centre managers, head of security and compliance & assurance director that DigiPlex had processes in place to periodically review physical access to ensure consistency with job responsibilities.  Obtained and inspected evidence to demonstrate that access to data centre premises was reviewed periodically by the management to ensure consistency with job responsibilities. | None | Exceptions noted.  Please refer subsection IV - ‘Findings and Observations’ for more details |
| CA32 | Two factor authentication mechanism is established to access the data centre. E.g. swipe card and biometric or Proximity and biometric based access control systems | Confirmed via corroborative inquiry with the data centre managers, head of security and compliance & assurance director that two factor authentication mechanism was established to access the data centre. E.g. swipe card and biometric or Proximity and biometric based access control systems.  Observed during site visit at the in-scope data centres that two factor authentication mechanism in the form of access card and pass code was established to access the data centre. | None | No exceptions noted |
| CA33 | The data centre facilities are manned by trained Security Guards round the clock, for restricting access to authorized individuals. | Confirmed via corroborative inquiry with the data centre managers, head of security and compliance & assurance director that the data centre facilities were manned by trained security guards round the clock, for restricting access to authorized individuals.  Observed during site visit at the in-scope data centres that the data centre facilities were manned by trained security guards round the clock, for restricting access to authorized individuals. Noted that for DRAS data centre, security guards of the leased premises were responsible to guard access to the entire facility. | None | No exceptions noted |
| CA34 | Entry and exit details of the visitors accessing the data centre facilities are logged and documented. Access to visitors is granted only after obtaining appropriate approvals from designated personnel in the management All visitors must be escorted by an authorized personnel while on the premises. | Confirmed via corroborative inquiry with data centre managers during site visit on that entry and exit details of the visitors accessing the data centre facilities were logged and documented. Access to visitors was granted only after obtaining appropriate approvals from designated personnel in the management. Further, confirmed that visitors were escorted by an authorized personnel on the premises.  Obtained and inspected the ‘Security Manual’ document for the data centres and noted that procedures for visitor access were documented by the management.  Obtained the logs for the visitors and for sample visitors, noted that appropriate approvals provided by management for DigiPlex visitors and for customers for customer specific visitors were documented in the Service Now tool. | 3.7.3 | No exceptions noted |
| CA35 | Movements of materials within the data centre is monitored and tracked, logged and only permitted with proper authorization | Confirmed via corroborative inquiry with data centre managers during site visit that movements of materials within the data centre was monitored and tracked, logged and only permitted with proper authorization.  Obtained and inspected the goods register for data centre premises in-scope and noted that the movement of materials within the data centre was monitored and tracked, logged and only permitted with proper authorization. | 3.7.4 | No exceptions noted |
| CA36 | Access to data centre facilities is granted to DigiPlex employees based on approvals as per the access management procedures.  Access to customers is granted based on approvals from authorized customer personnel through tickets documented in Service Now. | Confirmed via corroborative inquiry with data centre managers that access to data centre facilities was granted to DigiPlex employees based on approvals as per the 'access management procedures'. Further confirmed that access to customers was granted based on approvals from authorized customer personnel through tickets documented in Service Now.  Obtained and inspected the list granted on behalf of the customer and confirmed that the access requests were from authorized customer personnel through tickets documented in Service Now.  List of DigiPlex employees who were granted access to data centre facilities during the review period was not available for review. | 3.7.3 | Exceptions noted.  Please refer subsection IV - ‘Findings and Observations’ for more details |
| CA37 | There are formal processes for managing and controlling access to mechanical keys including:  - Mechanical keys are kept in a hidden and physical secured lockbox at each location (separate systems)  - Access to mechanical keys are restricted to a limited number of authorized personnel. Access to specific keys is granted based on needs  - Code and fingerprint are required to gain access to lockbox | Confirmed via corroborative inquiry with data centre managers that there were formal processes for managing and controlling access to mechanical keys.  Observed during site visits at the data centre premises that access to keys was restricted to authorized personnel only. Noted that mechanical keys were kept in Key Locker box that required two factor authentication to access. Further the access to the box was restricted to authorized individuals and code or fingerprint was required to gain access to the keys | None | No exceptions noted |

**Risk Management**

**Control Objective #9:** Controls provide reasonable assurance that redundancy of information is maintained either in logical or physical form and restoration of the same is available.

| **Control Activity** | | **Tests Performed** | **CUEC** | **Test Result** |
| --- | --- | --- | --- | --- |
| CA38 | DigiPlex's risk identification and assessment process includes (1) identifying information assets (physical), (2) assessing the criticality of those information assets, (3) identifying the threats to the assets (intentional, unintentional and environmental), and (4) identifying the vulnerabilities of the identified assets. | Confirmed via corroborative inquiry with the compliance and assurance director that DigiPlex's risk identification and assessment process included (1) identifying information assets (physical), (2) assessing the criticality of those information assets, (3) identifying the threats to the assets (intentional, unintentional and environmental), and (4) identifying the vulnerabilities of the identified assets.  Obtained and inspected the "Procedure on Risk & Opportunity Management" and noted that document included the following:  - Ch 5.0 Objective and commitment  - Ch 6.0 Organization and responsibilities  - Ch 7.0 Risk Management Committee  - Ch 8.0 Procedure  - Ch 9.0 Opportunity assessment  - Ch 10.0 Measurement  - Ch 11.0 Forms and templates  - Ch 12.0 Records and retention  Obtained and inspected the Risk Opportunity Register, Notes from High Risk Review, Management Review Year Wheel and noted that DigiPlex had established risk identification and assessment process. | 3.7.1  3.7.2 | No exceptions noted |
| CA39 | Risks identified during risk assessment are documented and mitigating procedures are initiated. | Confirmed via corroborative inquiry with the compliance and assurance director that the risk assessment was performed for the information assets at DigiPlex and the assigned risks were documented and mitigating procedures were initiated.   Obtained and inspected the ‘DigiPlex Asset Risk Register’ and noted that the document includes a list of information assets, listing the details of the assets and the associated risk, risk score and mitigating review actions.  Further noted that the document also included information from risk assessment "RA Tool" which includes a more detailed risk analysis for assets. | None | No exceptions noted |

**Third Party Management**

**Control Objective #9:** Controls provide reasonable assurance that system requirements, boundaries of the system, ,roles and responsibilities, and performance requirements are formally defined and documented with third party service providers. Compliance to service level agreements with third parties is monitored periodically by the management.

| **Control Activity** | | **Tests Performed** | **CUEC** | **Test Result** |
| --- | --- | --- | --- | --- |
| CA40 | Security requirements for the subcontractors are agreed in service agreements, which include statements on the rights and obligations of both parties and a confidentiality agreement, if there is a possibility that the subcontractor personnel can see confidential information. | Confirmed via corroborative inquiry with the compliance and assurance director that security requirements for the subcontractors were agreed in service agreements, which included statements on the rights and obligations of both parties and a confidentiality agreement, if there was a possibility that the subcontractor personnel can see confidential information.  Obtained and inspected the service agreements, contracts and purchase orders for sample subcontractors and noted that security requirements which included statements on the rights and obligations of both parties and a confidentiality agreement were agreed, if there was a possibility that the subcontractor personnel can see confidential information. | None | No exceptions noted |
| CA41 | The Supplier Code of Practice reflects what expectations DigiPlex requires from outsources service providers with regard to integrity and ethical business practices | Confirmed via corroborative inquiry with the compliance and assurance director that the Supplier Code of Practice reflected what expectations DigiPlex required from outsources service providers with regard to integrity and ethical business practices.  Obtained and inspected the ‘Supplier Code of Practice’ document to be agreed with suppliers and noted for sample suppliers that expectations related to integrity and ethical business practices of DigiPlex were agreed upon. | None | No exceptions noted |

**Infrastructure change management**

**Control Objective #10:** Controls provide reasonable assurance that changes performed to infrastructure follow defined change management procedures to prevent unauthorized changes to the environment.

| **Control Activity** | | **Tests Performed** | **CUEC** | **Test Result** |
| --- | --- | --- | --- | --- |
| CA42 | DigiPlex has established and documented a change management process which is approved by the ‘Transformation Director’.  Changes are raised, classified, tracked and approved in Service Now ticketing system. | Confirmed via corroborative inquiry with the compliance and assurance director that DigiPlex has established and documented a change management process which is approved by the ‘Transformation Director’. Further confirmed that changes were raised, classified, tracked and approved in Service Now ticketing system.  Obtained and inspected the ‘Change Management’ policy for DigiPlex and noted that the same was approved and owned by the ‘Transformation Director’. Further, for sample changes noted that the changes were raised, classified, tracked and approved in Service Now ticketing system. | 3.7.5 | No exceptions noted |

**Continuity Management**

**Control Objective #11:** Controls provide reasonable assurance that organization has documented and implemented Business Continuity plan and Disaster recovery measures in place to ensure minimal impact to operations in case of a disaster

| **Control Activity** | | **Tests Performed** | **CUEC** | **Test Result** |
| --- | --- | --- | --- | --- |
| CA43 | DigiPlex has established and documented Business Continuity and Disaster Recovery plan | Confirmed via corroborative inquiry with the data centre managers and compliance and assurance director that DigiPlex had established and documented Business Continuity and Disaster Recovery plan.  Obtained and inspected the "Business Continuity Statement" and noted that the document was issued in November 2019 and signed by the CEO, Gisle Eckhoff. The document stated that DigiPlex is committed to ensure critical functions and vital services to their customers.  Obtained and inspected the "Crisis and Communication Plan " and noted that document included an issue date, March 2019, and an owner, the Chief Strategy, Marketing & Communication Officer. | 3.7.6 | No exceptions noted |
| CA44 | DigiPlex has implemented testing of the Business Continuity Plan, this is performed on a periodic basis. The testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of system components from across the entity that can impair the availability; (3) scenarios that consider the potential for the lack of availability of key personnel; and (4) revision of continuity plans and systems based on test results. | Confirmed via corroborative inquiry with the data centre managers and compliance and assurance director that DigiPlex has implemented testing of the Business Continuity Plan, this was performed on a periodic basis. The testing included (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of system components from across the entity that can impair the availability; (3) scenarios that consider the potential for the lack of availability of key personnel; and (4) revision of continuity plans and systems based on test results.  Evidence to demonstrate that periodic disaster recovery drills were scheduled and conducted during the review period were not available. | None | Exceptions noted.  Please refer subsection IV - ‘Findings and Observations’ for more details |

## Findings and Observations

The audit observations were reviewed and discussed on January 15, 2020, during a dedicated closing meeting attended by the auditors and by the various stakeholders involved. The details of exceptions noted are as under:

|  |  |  |  |
| --- | --- | --- | --- |
| Sr. # | Description of Testing Exception | Locations | Control Objective/Activity impacted by Exception |
| 1. | Evidence to demonstrate that CCTV systems were maintained regularly was not available for review. | DNAS | **Control Objective #7:**  Controls provide reasonable assurance that access to the data centre premises and its assets is restricted physically and granted as per need-to-know basis  **Control Activity #25:**  Closed Circuit Television (CCTV) systems are installed at strategic locations at the entry and exit points of the data centre facilities to record all the events.  The CCTV systems are continuously monitored by the Physical Security team.  The CCTV equipment is maintained on a regular basis. |
| 2. | 1. Evidence to demonstrate that access for three resigned employees was revoked on the last working day of employment was not available for review. 2. A complete list of revocations performed on request of customers was not made available for sampling and testing. | 1. DFAS 2. All four locations in scope | **Control Objective #7:**  Controls provide reasonable assurance that access to the data centre premises and its assets is restricted physically and granted as per need-to-know basis  **Control Activity #30:**  Access to data centre facilities is revoked on the last working day of resigned/terminated employee.  Customer access is revoked based on intimation from authorized customer personnel through ticket in Service Now. |
| 3. | For three out of four data centres in scope, a physical access privileges review for DigiPlex employees was not performed during the review period | DNAS  DRAS  DFAS | **Control Objective #7:**  Controls provide reasonable assurance that access to the data centre premises and its assets is restricted physically and granted as per need-to-know basis  **Control Activity #31:**  DigiPlex has processes in place to periodically review physical access to ensure consistency with job responsibilities. |
| 4. | A list of DigiPlex employees who were granted access to data centre facilities during the review period was not made available for review. | All four locations in scope | **Control Objective #7:**  Controls provide reasonable assurance that access to the data centre premises and its assets is restricted physically and granted as per need-to-know basis  **Control Activity #36:**  Access to data centre facilities is granted to DigiPlex employees based on approvals as per the 'access management procedures'.  Access to customers is granted based on approvals from authorized customer personnel through tickets documented in Service Now. |
| 5. | Evidence to demonstrate that periodic disaster recovery drills were scheduled and conducted during the review period were not made available | All four locations in scope | **Control Objective #11:**  Controls provide reasonable assurance that organization has documented and implemented Business Continuity plan and Disaster recovery measures in place to ensure minimal impact to operations in case of a disaster  **Control Activity #44:**  DigiPlex has implemented testing of the Business Continuity Plan, this is performed on a periodic basis. The testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of system components from across the entity that can impair the availability; (3) scenarios that consider the potential for the lack of availability of key personnel; and (4) revision of continuity plans and systems based on test results. |

|  |
| --- |
|  |