www.pwc.dk

Aarhus University

Aarhus Genome Data Center

Independent service auditor's ISAE 3000 assurance report on IT general controls during the period from 1 September 2024 to 31 August 2025 in relation to Aarhus Genome Data Center's GenomeDK HPC services

September 2025

Contents

1 Management's statement

The accompanying description has been prepared for customers who have used Aarhus Genome Data Center's GenomeDK HPC services (GenomeDK) and who have a sufficient understanding to consider the description, along with other information, including information about controls operated by the customers' themselves, when assessing the risks of material misstatements.

GenomeDK uses Incuba as subservice supplier of housing for backup, and AU IT and AU BYG (NAT) as subservice suppliers of hosting services. This report uses the carve-out method and does not comprise control objectives and related controls that Incuba performs for GenomeDK.

Some of the control objectives stated in our description in section 3 can only be achieved if the complementary controls at the customers are suitably designed and operating effectively with our controls. This report does not comprise the suitability of the design and operating effectiveness of these complementary controls.

GenomeDK confirms that:

a) The accompanying description in section 3 fairly presents GenomeDK's operation of HPC services that have processed the customers' transactions throughout the period from 1 September 2024 to 31 August 2025. The criteria used in making this statement were that the accompanying description:

   (i) Presents how IT general controls in relation to GenomeDK's operation of HPC services were designed and implemented, including:

   - The types of services provided
   - The procedures, within both information technology and manual systems, by which the IT general controls were managed
   - Relevant control objectives and controls designed to achieve those objectives
   - Controls that we assumed, in the design of GenomeDK's operation of HPC services, would be implemented by user entities and which, if necessary to achieve the control objectives stated in the accompanying description, are identified in the description
   - How the system dealt with significant events and conditions other than transactions
   - Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that were relevant to the IT general controls

   (ii) Includes relevant details of changes to IT general controls in relation to GenomeDK's operation of HPC services during the period from 1 September 2024 to 31 August 2025

   (iii) Does not omit or distort information relevant to the scope of the IT general controls in relation to GenomeDK's operation of HPC services being described, while acknowledging that the description is prepared to meet the common needs of a broad range of customers and may not, therefore, include every aspect of the IT general controls in relation to GenomeDK's operation of HPC services that each individual customer may consider important in its own particular environment.

b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from 1 September 2024 to 31 August 2025. The criteria used in making this statement were that:

(i) The risks that threatened achievement of the control objectives stated in the description were identified;

(ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved; and

(iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, throughout the period from 1 September 2024 to 31 August 2025.

Aarhus, 17. september 2025
Aarhus Genome Data Center

Anders Børglum
Professor

2 Independent service auditor's assurance report on the description, design and operating effectiveness of controls

Independent service auditor's ISAE 3000 assurance report on IT general controls during the period from 1 September 2024 to 31 August 2025 in relation to Aarhus Genome Data Center's GenomeDK HPC services to customers

To: GenomeDK and customers who have used GenomeDK's HPC services

Scope

We have been engaged to provide assurance about GenomeDK's description in section 3 of its IT general controls in relation to GenomeDK's operation of HPC services which have processed customers' transactions throughout the period from 1 September 2024 to 31 August 2025 and about the design and operating effectiveness of controls related to the control objectives stated in the description.

GenomeDK uses Incuba as subservice supplier of housing for backup, and AU IT and AU BYG (NAT) as subservice suppliers of hosting services. This report uses the carve-out method and does not comprise control objectives and related controls that Incuba performs for GenomeDK.

Some of the control objectives stated in GenomeDK's description in section 3 can only be achieved if the complementary controls at the customers are suitably designed and operating effectively with GenomeDK's controls. This report does not comprise the suitability of the design and operating effectiveness of these complementary controls.

We express reasonable assurance in our conclusion.

GenomeDK's responsibilities

GenomeDK is responsible for: preparing the description and accompanying statement in section 1, including the completeness, accuracy and method of presentation of the description and statement; providing the services covered by the description; stating the control objectives and designing, implementing and effectively operating controls to achieve the stated control objectives.

Service auditor's independence and quality control

We have complied with the independence and other ethical requirements in the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional conduct, as well as ethical requirements applicable in Denmark.

Our firm applies International Standard on Quality Management 1, ISQM 1, which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Service auditor's responsibilities

Our responsibility is to express an opinion on GenomeDK's description and on the design and operating effectiveness of controls related to the control objectives stated in that description, based on our procedures.

We conducted our engagement in accordance with ISAE 3000, "Assurance engagements other than audits or reviews of historical financial information", and additional requirements applicable in Denmark to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed and operating effectively.

An assurance engagement to report on the description, design and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of its service and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgement, including the assessment of risks that the description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein and the suitability of the criteria specified and described by GenomeDK in the Management's statement section.

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

Limitations of controls at a service organisation

GenomeDK's description is prepared to meet the common needs of a broad range of customers and may not, therefore, include every aspect of the GenomeDK HPC services that the individual customer may consider important in its particular circumstances. Also, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions in processing or reporting transactions. Furthermore, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a service organisation may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this auditor's report. The criteria we used in forming our opinion are those described in the Management's statement section. In our opinion, in all material respects:

a) The description fairly presents how IT general controls in relation to GenomeDK's operation of HPC services were designed and implemented throughout the period from 1 September 2024 to 31 August 2025;

b) The controls related to the control objectives stated in the description were suitably designed throughout the period from 1 September 2024 to 31 August 2025; and

c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from 1 September 2024 to 31 August 2025.

Description of test of controls

The specific controls tested and the nature, timing and results of these tests are listed in section 4.

Intended users and purpose

This report and the description of tests of controls in section 4 are intended only for customers who have used GenomeDK HPC services and who have a sufficient understanding to consider it along with other information, including information about controls operated by the customers themselves, in assessing the risks of material misstatement.

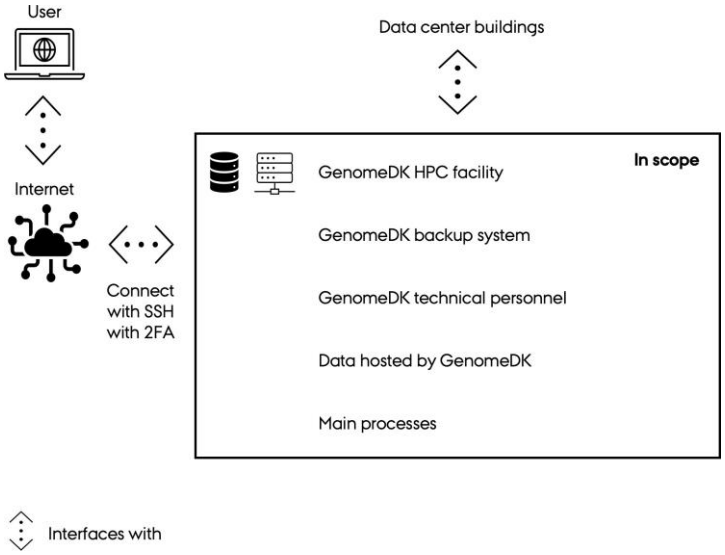
Aarhus, 17. september 2025
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR no. 33 77 12 31

Jesper Parsberg Madsen
State-Authorised Public Accountant
mne26801

3 System description

3.1 Introduction

GenomeDK is a high-performance computing facility designed to store and compute on large, sensitive data sets. The facility is ISO 27001-certified, and is compliant with the General Data Protection Regulation (GDPR) and the Danish Data Protection Act. The facility is owned by Aarhus University (AU) and managed under Aarhus Genome Data Center (AGC). GenomeDK hosts large amounts (petabytes) of sensitive data for researchers, SMEs and Aarhus University Hospital (AUH).



3.1.1 Scope

The scope of this ISMS is limited to GenomeDK as a hosting service providing computational power and storage capacity. As such, the scope only contains the hardware, software and the processes that are involved in providing this capacity and securing user data.

GenomeDK is completely isolated from Aarhus University. The reason we can consider this isolated is we only have two controlled interfaces to the surroundings:

- Data centre room provided by Aarhus University with cooling, emergency power, fire protection, etc.
- Internet access provided by Aarhus University, use of this connection for GenomeDK access is encrypted by SSH.

The separation between Aarhus University and GenomeDK allows GenomeDK to provide tightened security for the data hosted on GenomeDK and makes it convenient to support access to GenomeDK for non-Aarhus University collaborators and SMEs.

3.1.1.1 Processes included in the scope

The scope includes the following processes:

- User request process description:
  - Input: a user request
  - Output: approved user can access GenomeDK

  - Main activities:
    - Zone owner approves or rejects the user request.
    - If approved, technical personnel use an automated procedure to create the user on GenomeDK.
    - User is informed by the automated procedure.

- Project folder creation:
  - Input: a user requests a project folder
  - Output: user can access the approved project folder
  - Main activities:
    - User requests a project folder on GenomeDK.
    - Project folder request is approved or rejected by technical personnel. If accepted, the technical personnel use an automated procedure to create the project folder.
    - User is informed by the automated procedure.

- User deactivation:
  - Input: zone owner requests deactivation, user inactivity, user violates terms of service.
  - Output: the user is deactivated and can no longer access GenomeDK.
  - Main activities:
    - Technical personnel use an automated procedure to deactivate the user.

- Technical maintenance:
  - Input: ad-hoc maintenance, planned maintenance, maintenance triggered by incidents, alarms, or other events.
  - Output: stable and secure compute and storage capacity.
  - Main activities:
    - Keeping system software up-to-date planned and carried out by the technical personnel.
    - Planning purchase and installation of new assets, and retirement of old assets.
    - Ensuring that the necessary software services and tools are present and working.
    - Information security activities according to ISO 27001 and this ISMS.

The processes are supported as necessary by software developed by the technical personnel for GenomeDK.

3.1.2 The provided services

GenomeDK offers access to a Linux-based high-performance computing facility on which users can submit jobs to a range of "compute" machines to perform computations on those machines in a highly parallel fashion. The compute machines have access to a high-capacity, parallel file system. Users can obtain "project folders" on this file system to securely store and manage access to their data. A project folder is the only way to share data between users on GenomeDK, and the project owner is responsible for the resources by the project.

For users with additional requirements, GenomeDK provides an additional layer of control through "closed zones". Closed zones are designed to prevent accidental or unintended disclosure of sensitive data located in the closed zone by restricting the user to a virtual desktop without copy-paste, restricting Internet access, and only allowing data to leave the zone/GenomeDK with approval from the zone owner.

3.1.3 Information security objectives

GenomeDK aims to maintain confidentiality, integrity and availability (CIA) by:

- defining clear business objectives and documenting these (see "Business objectives")

- deriving information security objectives from our business objectives, to ensure that our information security objectives are aligned with our business objectives
- establishing an information security risk assessment process that defines risk acceptance criteria and criteria for performing risk assessments
- documenting our risk assessment process through our risk analysis and risk treatment plan
- the adherence of the plan-do-check-act process which is documented through monthly meeting minutes and checklists.

Significant incidents that influence our business or information security objectives are discussed at monthly steering committee meetings. These processes ensure that GenomeDK continuously improves with regard to the information security objectives.

3.1.3.1 Documentation organisation

In accordance with the ISO 27001 standards section 7.5 on "Documented organization", the documentation in this ISMS is:

- Reviewed yearly for suitability and adequacy by the technical steering committee
- Made available through the standard PDF format.

All documents are named uniquely and are available to GenomeDK employees and management. The ISMS is stored in automatic version control and is backed up.

There have been no significant changes to procedures and controls in the period from 1 September 2024 to 31 August 2025.

3.2 Stakeholder analysis

Stakeholder	Description	Formal information security requirements
Aarhus University (AU)	AU owns GenomeDK and provides it as a service to its own researchers and students, as well as their (international) collaborators, and to other Danish universities through the DeiC National HPC collaboration (see below). GenomeDK is a significant asset to AU because it provides significant computational resources used for a wide range or research, but also because GenomeDK is the only infrastructure at AU which can store large amounts of sensitive data and allow computations on such data.	AU has no formal requirements for GenomeDK.
Aarhus University Hospital (AUH)/ Region Midtjylland	AUH is a major contributor to GenomeDK's yearly budget. AUH uses GenomeDK for both research and clinical applications, with strict requirements on reliability and security.	Requirements specified in the data protection agreement between GenomeDK and Region Midtjylland and the associated appendices.
Danish e-Infrastructure Consortium (DeiC)	DeiC contributes significantly to GenomeDK's yearly budget and relies on GenomeDK for providing secure HPC services to researchers at other Danish universities.	Requirements specified in the agreement between GenomeDK and DeiC. ISO 27001-compliance is required.
Others	Other users include the researchers, students, and SMEs that use GenomeDK for data storage and processing.	Users can expect GenomeDK to provide the services described above under the terms described in GenomeDK's Terms of Service.

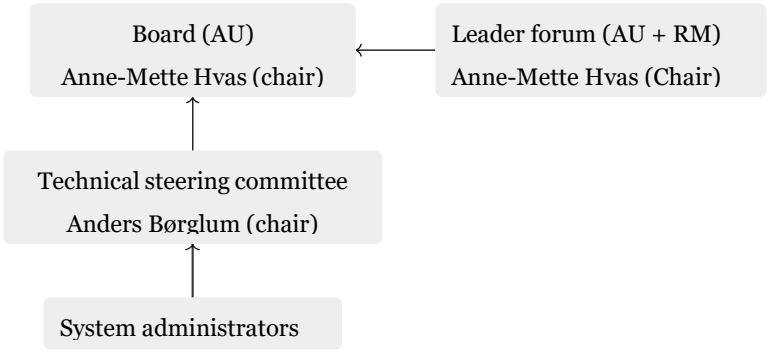
3.3 Organisation

Aarhus Genome Data Center (AGC) is centre at Aarhus University. The centre is formally anchored under Institute of Biomedicine, Faculty of Health.

The centre is a collaboration between Aarhus University (AU) and the Central Denmark Region (RM), however, the GenomeDK is owned and run solely by AU.

The centre is managed by the board, which consists of representatives from AU. The leader forum consists of representatives from both AU and RM and provides input to the board and facilitates synergies between the two parties.

The technical steering committee is responsible for day-to-day management of GenomeDK and consists of representatives from the three parties and the technical personnel (system administrators) at GenomeDK.



Anders Børglum is head of AGC and is responsible for day-to-day management of GenomeDK, as well as responsible for overall information security at GenomeDK.

3.4 Plan-do-check-act

GenomeDK follows the plan-do-check-act process and has incorporated it directly into the monthly steering committee meetings.

In the meeting minute templates used by the GenomeDK steering committee, it can be seen how GenomeDK has planned, implemented and controlled the processes needed to meet the ISMS requirements and how GenomeDK has implemented risk analysis and risk treatment actions in the risk assessment and fulfils the stated security objectives in accordance with the ISO 27001 standard.

Additionally, yearly information security objectives are planned by the technical steering committee and managed through a plan-do-check-act template.

3.5 Risk management and policies

GenomeDK uses a scenario-based risk assessment approach closely aligned to risks and threats defined in ISO 27005. Policies have been defined for all relevant items in Annex A of the ISO 27001 specification to ensure that risks are controlled and minimised. The risk assessment is continuously updated and discussed in the technical steering committee.

The following matrix shows which preventative and remedial controls have been implemented by GenomeDK:

	Preventative controls	**Remedial controls**
Organisational controls	Policies and procedures; Awareness; Change management; Technical best practices; Compliance controls	Incident management; Disaster management
Physical and technical controls	Firewalls; Health checks; Isolated test environments; UPS; Emergency power generator; Dynamic network segregation; Fire detection system	Logging; Backup/restore; Fire suppression system

3.5.1 Information security policy and organisation of information security

A formal policy has been defined to ensure that information security responsibilities and roles are clearly defined.

The board has defined and described information security responsibilities in a formal information security policy, as well as information security objectives derived from the organisation's long- term business objectives (see section 3.1.3).

GenomeDK is audited with regards to ISO 27001 and GDPR by an external, independent party on an annual basis.

3.5.2 Human resource security

GenomeDK has defined policies for employment/on-boarding of new personnel as well as change of roles/responsibilities and termination of employment.

All employees are obliged to confidentiality and are informed about the criticality of the data that is hosted on GenomeDK. Employees must also read and understand the GenomeDK information security policy.

Employees must only have privileged access to systems during their employment. All privileged access must be revoked if no longer necessary due to a change of employment or termination.

3.5.3 Asset management

GenomeDK has defined policies for ownership and handling of assets and disposal of media.

An inventory is kept for all significant hardware assets. Media containing potentially sensitive data must be destroyed when decommissioned.

3.5.4 Access control

All potential users must submit a formal request to access GenomeDK. The request must be approved by a zone administrator before an account is created on the system.

GenomeDK follows industry best practices for password management and uses two-factor authentication for all connections to the facility.

All users connect to GenomeDK through a secure, encrypted channel (SSH) with two-factor authentication.

Access to data is controlled through *projects*. A project has a project owner. Only the project owner can grant and revoke access to the project and the data contained within. Without access to a project, a user has access to a very limited amount of compute and storage resources.

GenomeDK performs periodic, automated reviews of users to revoke access for users that are no longer active.

System administrators are the *only* privileged users on GenomeDK.

3.5.5 Cryptography

GenomeDK has defined policies for cryptographic controls. All traffic to/from GenomeDK must use an encrypted connection, and only privileged users must be able to access confidential authentication information (passwords, host keys, certificates, etc.).

3.5.6 Physical and environmental security

GenomeDK has defined policies for physical and environmental security based on the criticality of the infrastructure/equipment and the sensitivity of the data stored in the perimeter.

GenomeDK is physically located in a modern, secure server room with 24/7 surveillance at the Aarhus University campus. Data centres are protected from environmental threats and secured with (at least) double doors and door card locks.

Data centres hosting unencrypted data (which may be sensitive) must apply additional controls such as video surveillance and alarm systems.

Work in secure areas must be work-related, and visitors must be authorised and escorted by authorised personnel.

3.5.7 Operations security

As part of the ISMS implemented by GenomeDK, policies and procedures have been defined to ensure stable and secure operations. This is done through (amongst others) change management and procedures for handling incidents. GenomeDK has also implemented weekend duty for system administrators to ensure any critical problems can be handled over the weekend.

Any changes that may affect information security at GenomeDK are discussed at monthly steering committee meetings and may be escalated to the board. Technical changes are carried out by the system administration team. When necessary, peer review is used to ensure that a change will not affect availability, integrity or confidentiality of the system.

All open/read file operations on GenomeDK are logged and stored for at least 6 months. This provides traceability in case of a loss of confidentiality incident.

In case data is lost, GenomeDK provides access to backup. However, only data marked for backup by users is backed up.

3.5.8 Communications security

Policies have been defined for communications internally on GenomeDK as well as externally. GenomeDK implements both physical and virtual network segregation. The management network is physically separated from production networks. Network segregation on production networks uses firewalls to ensure that only machines in the same zone can communicate.

Transfers to/from external entities are performed by the user over a secure, encrypted connection. In closed zones, the user must request approval from the zone administrator to export files, and the exported file is logged for a year.

3.5.9 Supplier relationships

GenomeDK has defined policies for supplier relationships and is continuously working to formalise relationships with providers to ensure a clear division of responsibilities and that suppliers fulfil the information security requirements required by GenomeDK. GenomeDK management assesses changes to suppliers' information security as part of internal risk assessment reviews.

3.5.10 Information security incident management and business continuity

Policies and procedures are defined to handle information security incidents at GenomeDK efficiently and to minimise service interruptions for the users.

GenomeDK has defined clear responsibilities and actionable items/checklists when dealing with incidents. An incident severity classification has been established, and actions associated with each severity level have been defined.

The incident management policies and procedures also apply to business continuity.

3.5.11 Compliance

Policies and procedures are reviewed and, if necessary, revised on a yearly basis. Risks and threats are continuously reviewed by the technical steering committee and – if necessary – the board, on a yearly basis.

A shared document management system is maintained to host all policies and procedures, as well as a contract/agreement register, to facilitate easy access for the technical steering committee.

The facility is audited with regard to ISO 27001 and GDPR by an external, independent party on an annual basis.

3.6 Competency overview

Competencies:

1. Familiarity with the GenomeDK information security management system
2. Expert in the GenomeDK information security management system.
3. Familiarity with HPC or similar large, distributed IT systems.
4. Familiarity with large-scale storage systems.
5. Familiarity with Linux system administration.
6. Familiarity with ISAE 3000, ISO 27001, and GDPR.

Roles and required competencies

- Center manager: 1
- Systemadministrator: 1, 3, 4, 5
- Information security management system manager: 2, 3, 6

Competency overview.

- Anders Børglum (center manager): 1
- Anders Egerup Halager (systemadministrator): 1, 3, 4, 5
- Dan Søndergaard (systemadministrator, information security management system manager): 2, 3, 4, 5, 6

- Keld Erik Knudsen (system administrator): 1, 3, 4, 5

3.7 Complementary controls at the customers

The customers have the following obligations:

- Upload and maintenance of data

4 Control objectives, control activity, tests and test results

4.1 Purpose and scope

We conducted our engagement in accordance with ISAE 3000, "Assurance engagements other than audits or reviews of historical financial information", and additional requirements applicable in Denmark.

Our testing of the design, implementation and functionality of the controls has included the control objectives and related control activities selected by Management and listed in section 4.3. Any other control objectives, related controls and controls at customers are not covered by our test actions.

Our operating effectiveness testing included the control activities deemed necessary to obtain reasonable assurance that the stated control objectives were achieved.

4.2 Test actions

The test actions performed when determining the operating effectiveness of controls are described below:

Inspection	Reading of documents and reports containing specifications regarding the execution of the control. This includes reading and consideration of reports and other documentation in order to assess whether specific controls are designed so they may be expected to become effective if implemented. Furthermore, it is assessed whether controls are being monitored and checked sufficiently and at appropriate intervals. We have tested the specific system set-up on the technical platforms, databases and network components in order to verify whether controls are implemented and have functioned during the period from 1 September 2024 to 31 August 2025. Among other things, this includes assessment of patching level, permitted services, segmentation, password complexity, etc. as well as inspection of equipment and locations.
Inquiries	Inquiry of appropriate personnel. Inquiries have included how the controls are performed.
Observation	We have observed the execution of the control.
Reperformance of the control	Repetition of the relevant control. We have repeated the execution of the control to verify whether the control functions as assumed.

4.3 Overview of control objectives, control activity, tests and test results

Control objective 5:

Organisational controls

Procedures and controls ensure that management direction and support for information security were provided in accordance with business requirements and relevant laws and regulations, including a management framework to initiate and control the implementation and operation of information security within the organisation

Nr.	GenomeDK's control activity	Tests performed by PwC	Result of PwC's tests
5.1	**Policies for information security** *Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.*	We inquired Management regarding the procedures/control activities performed. We inspected that a Management-approved and updated security policy is in place. We inspected that the information security policies are communicated to employees and relevant parties and is reviewed annually.	No exceptions noted.
5.2	**Information security roles and responsibilities** *Information security roles and responsibilities shall be defined and allocated according to the organisation's needs.*	We inquired Management regarding the procedures/control activities performed. We inspected that the organisational areas of responsibility have been defined and allocated to relevant personnel.	No exceptions noted.
5.3	**Segregation of duties** *Conflicting duties and conflicting areas of responsibility shall be segregated.*	We made inquiries of Management about the procedures/control activities carried out to ensure that access rights to GenomeDK are granted in accordance with adequate business procedures and that the access rights granted are followed up annually.	No exceptions noted.
5.9	**Inventory of information and other associated assets** *An inventory of information and other associated assets, including owners, shall be developed and maintained.*	We inquired Management regarding the procedures/control activities performed. We inspected that adequate controls are in place to ensure documentation and maintenance of the inventory of assets.	No exceptions noted.

Control objective 5:

Organisational controls

Procedures and controls ensure that management direction and support for information security were provided in accordance with business requirements and relevant laws and regulations, including a management framework to initiate and control the implementation and operation of information security within the organisation

Nr.	GenomeDK's control activity	Tests performed by PwC	Result of PwC's tests
5.11	**Acceptable use of information and other associated assets** *Personnel and other interested parties as appropriate should return all the organisation's assets in their possession upon change or termination of their employment, contract or agreement.*	We have made inquiries of Management about the procedures/control activities performed. We have observed that a procedure is in place to ensure that assets are returned upon termination. From a sample of terminated employees, we observed that there is documentation of confirmation that all assets have been returned upon termination.	No exceptions noted.
5.12	**Classification of information** *Information shall be classified according to the information security needs of the organisation based on confidentiality, integrity, availability, and relevant interested party requirements.*	We made inquiries of Management about the procedures/control activities carried out. We inspected that information is classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.	No exceptions noted.
5.14	**Information transfer** *Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organisation and between the organisation and other parties.*	We inquired Management regarding the procedures/control activities performed. We inspected that an appropriate security architecture has been established in the network and that information transfer rules are in place.	No exceptions noted.
5.15	**Access control** *Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.*	We made inquiries of Management regarding the procedures and control activities in place, reviewed the user administration procedures to ensure they are adequate, and inspected that an appropriate approval process is applied at GenomeDK By inspection, we also inspected that users are subject to authentication on all access points. We observed that the network is segmented into smaller networks to reduce the risk of unauthorised access..	No exceptions noted.

Control objective 5:

Organisational controls

Procedures and controls ensure that management direction and support for information security were provided in accordance with business requirements and relevant laws and regulations, including a management framework to initiate and control the implementation and operation of information security within the organisation

Nr.	GenomeDK's control activity	Tests performed by PwC	Result of PwC's tests
5.16	**Identity management** *The full lifecycle of identities should be managed.*	We have made inquiries of Management about the procedures/control activities performed. We have inspected that procedures include the full lifecycle of an identity.	No exceptions noted.
5.18	**Access rights** *Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organisation's topic-specific policy and rules for access control.*	We made inquiries of Management about the procedures/control activities carried out, reviewed the procedures for user administration and inspected that they are adequate. We inspected that the business procedures for users created are complied with. We made inquiries of Management about the procedures/control activities carried out to ensure that access rights are granted in accordance with adequate business procedures and that the access rights granted are followed up annually. We made inquiries of Management about the procedures/control activities carried out to ensure that access rights are revoked in accordance with adequate business processes and that the rights granted are followed up on in accordance with the business processes. We inspected that business procedures for terminated users are complied with.	No exceptions noted.

Control objective 5:

Organisational controls

Procedures and controls ensure that management direction and support for information security were provided in accordance with business requirements and relevant laws and regulations, including a management framework to initiate and control the implementation and operation of information security within the organisation

Nr.	GenomeDK's control activity	Tests performed by PwC	Result of PwC's tests
5.19	**Information security in supplier relationships** *Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of a supplier's products or services.*	We inspected that a formal and documented procedure is in place to ensure that new or re-negotiated application or service supplier contracts are validated against a list of defined information security requirements. From samples of signed contracts, we inspected that risk assessments are performed regularly on critical suppliers. Furthermore, we inspected that GenomeDK audits key suppliers on a periodic basis, based on agreed information security requirements.	No exceptions noted.
5.22	**Monitoring, review, and change management of supplier services** *The organisation shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.*	We inspected that a formal, documented procedure is in place to ensure that new or re-negotiated application or service supplier contracts are validated against a list of defined information security requirements. From a sample of signed contracts, we inspected that information security requirements have been contractually agreed. From a sample of months, we inspected that GenomeDK audits key suppliers on a periodic basis, based on agreed information security requirements. We inspected that third-party declarations have been received and processed by GenomeDK for key suppliers.	No exceptions noted.

Control objective 5:

Organisational controls

Procedures and controls ensure that management direction and support for information security were provided in accordance with business requirements and relevant laws and regulations, including a management framework to initiate and control the implementation and operation of information security within the organisation

Nr.	GenomeDK's control activity	Tests performed by PwC	Result of PwC's tests
5.24	**Information security incident management, planning and preparation** *The organisation shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.*	We inspected that a formal and documented incident management process has been implemented. We inspected that roles and responsibilities related to the incident management process has been communicated to employees.	No exceptions noted.
5.25	**Assessment of security incidents** *The organisation should assess information security events and decide if they are to be categorised as information security incidents.*	We have made inquiries of Management about the procedures/control activities performed. We have observed that a formal and documented incident management process related to information security events and breaches has been implemented. We have observed that all incidents have been registered, that necessary actions have been performed and that the solutions have been documented in an incident management system and reported through the Information Security Board.	No exceptions noted.
5.26	**Response to information security incidents** *Information security incidents shall be responded to in accordance with the documented procedures.*	We inspected that a formal and documented incident management process has been implemented. We inspected that all incidents have been registered, that necessary actions have been performed, and that the solutions have been documented in an incident management system.	No exceptions noted.

Control objective 5:

Organisational controls

Procedures and controls ensure that management direction and support for information security were provided in accordance with business requirements and relevant laws and regulations, including a management framework to initiate and control the implementation and operation of information security within the organisation

Nr.	GenomeDK's control activity	Tests performed by PwC	Result of PwC's tests
5.29	**Information security during disruption** *The organisation shall plan how to maintain information security at an appropriate level during disruption.*	We inspected that a formal and documented business continuity plan is maintained, reviewed and approved annually. We inspected that underlying procedures related to the business continuity plan have been reviewed and approved by appropriate personnel.	No exceptions noted.
5.31	**Legal, statutory, regulatory and contractual requirements** *Legal, statutory, regulatory and contractual requirements relevant to information security and the organisation's approach to meet these requirements shall be identified, documented and kept up to date.*	We inquired management of information security requirements in general terms with GenomeDK. We inspected that Management-approved procedures are in place for handling legislative, statutory, regulatory and contractual requirements in relation to GenomeDK.	No exceptions noted.
5.37	**Documented operating procedures** *Operating procedures for information processing facilities shall be documented and made available to personnel who need them.*	We inquired Management regarding the procedures/control activities performed. We inspected that operating procedures have been established and that these are subject to updating at least once a year. We furthermore inspected that the operating procedures are accessible to all relevant employees.	No exceptions noted.

Control objective 6:

People controls

Procedures and controls ensure that human resource security is implemented and effective prior, during and after employment

Nr.	GenomeDK's control activity	Tests performed by PwC	Result of PwC's tests
6.1	**Screening** *Background verification checks on all candidates to become personnel shall be carried out prior to joining the organisation and on an ongoing basis, take into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.*	We inquired personnel security management in general terms with GenomeDK. By inspection, we inspected that screening of employees is carried out in accordance with relevant laws, regulations and the code of ethics and must be proportional to the business requirements, to the classification of the information to which access is to be granted and to the relevant risks	No exceptions noted.
6.3	**Information security awareness, education and training** *Personnel of the organisation and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organisation's information security policy, topic-specific policies and procedures, as relevant for their job function.*	We inquired personnel security management in general terms with GenomeDK. By inspection, we inspected that a Management approved and updated security policy for GenomeDK is in place.	No exceptions noted.
6.5	**Responsibilities after termination or change of employment** *Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.*	We made inquiries of Management about the procedures/control activities carried out to ensure that access rights are revoked in accordance with adequate business processes and that the rights granted are followed up on in accordance with the business processes. By inspection, we inspected that the business procedures described for terminated users at GenomeDK are complied with.	No exceptions noted.

Control objective 6:

People controls

Procedures and controls ensure that human resource security is implemented and effective prior, during and after employment

Nr.	GenomeDK's control activity	Tests performed by PwC	Result of PwC's tests
6.7	**Remote working** *Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organisation's premises.*	We made inquiries of Management about the procedures/control activities carried out, and we inspected that an appropriate approval process is applied at GenomeDK. By inspection, we also inspected that users are subject to authentication on all access points.	No exceptions noted.
6.8	**Information security event reporting** *The organisation shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.*	We inquired information security management, including information security events, in general terms with GenomeDK. We inspected that adequate procedures are in place for recording and reporting on information security events related to GenomeDK.	No exceptions noted.

Control objective 7:

Physical controls

Procedures and controls ensure that physical security is implemented and effective

Nr.	GenomeDK's control activity	Tests performed by PwC	Result of PwC's tests
7.1	**Physical security perimeters** *Security perimeters shall be defined and used to protect areas that contain information and other associated assets.*	We have made inquiries of Management about the procedures/control activities performed. We have observed that GenomeDK has appropriated physical security perimeters. We have inspected that GenomeDK has obtained assurance reports from hosting providers and that they are reviewed by GenomeDK to ensure that requirements are met.	No exceptions noted.
7.2	**Physical entry** *Secure areas shall be protected by appropriate entry controls and access points.*	We inspected that a formal physical access and security policy is maintained, reviewed and approved. We inspected that GenomeDK has implemented appropriate entry controls to protect physical facilities.	No exceptions noted.
7.3	**Securing offices, rooms and facilities** *Physical security for offices, rooms and facilities shall be designed and implemented.*	We inspected that a formal physical access and security policy is maintained, reviewed and approved. We inspected that GenomeDK has implemented appropriated entry controls to protect offices, rooms and facilities.	No exceptions noted.
7.5	**Protecting against physical and environmental threats** *Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure, shall be designed and implemented.*	We have made inquiries of Management about the procedures/control activities performed. We have inspected that GenomeDK has obtained assurance reports from hosting providers and that they are reviewed by GenomeDK to ensure that requirements are met.	No exceptions noted.

Control objective 7:

Physical controls

Procedures and controls ensure that physical security is implemented and effective

Nr.	GenomeDK's control activity	Tests performed by PwC	Result of PwC's tests
7.10	**Storage media** *Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organisation's classification scheme and handling requirements.*	We inquired Management regarding the procedures/control activities performed. By inspection, we inspected that GenomeDK has implemented formalised procedures for handling storage media throughout their life cycle.	No exceptions noted.
7.11	**Supporting utilities** *Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.*	We inquired Management regarding the procedures/control activities performed. We inspected that GenomeDK has established a fully redundant infrastructure with individual backup.	No exceptions noted.
7.12	**Cabling security** *Cables carrying power, data or supporting information services should be protected from interception, interference or damage.*	We have made inquiries of Management about the procedures/control activities performed. We have inspected that GenomeDK has obtained assurance reports from hosting providers and that they are reviewed by GenomeDK to ensure that requirements are met.	No exceptions noted.
7.13	**Equipment maintenance** *Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.*	We inquired Management regarding the procedures/control activities performed. We inspected that relevant security measures are implemented to ensure maintenance of equipment.	No exceptions noted.

Control objective 8:

Technological controls

Procedures and controls ensure that system and network security is implemented and effective

Nr.	GenomeDK's control activity	Tests performed by PwC	Result of PwC's tests
8.1	**User end point devices** *Information stored on, processed by or accessible via user end point devices shall be protected.*	We made inquiries of Management about the procedures/control activities carried out, and we inspected that an appropriate approval process is applied at GenomeDK. By inspection, we also inspected that users are subject to authentication on all access points.	No exceptions noted.
8.2	**Privileged access rights** *The allocation and use of privileged access rights shall be restricted and managed.*	We made inquiries of Management about the procedures/control activities carried out to ensure that privileged access rights are allocated in accordance with adequate business procedures. By random inspection, we inspected that the business procedures for users created are complied with.	No exceptions noted.
8.3	**Information access restriction**. *Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.*	We inquired Management regarding the procedures/control activities performed. We inspected that a policy of limiting access to systems and applications to employees who have a work-related need has been implemented.	No exceptions noted.
8.5	**Secure authentication** *Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.*	We inspected that a formal access control policy defining allowed technical solutions for authentication is maintained. We inspected that the access control policy has been reviewed and approved. We inspected that applications and systems in scope enforce secure log-on procedures.	No exceptions noted.

Control objective 8:

Technological controls

Procedures and controls ensure that system and network security is implemented and effective

Nr.	GenomeDK's control activity	Tests performed by PwC	Result of PwC's tests
8.7	**Protection against malware** *Protection against malware shall be implemented and supported by appropriate user awareness.*	We inquired regarding the procedures/control activities performed. By inspection of random samples, we inspected that antivirus software has been installed on all applicable systems and that antivirus software is monitored. Furthermore, we inspected that user awareness initiatives about antivirus software and malware defence have been established for employees.	No exceptions noted.
8.8	**Management of technical vulnerabilities** *Information about technical vulnerabilities of information systems in use shall be obtained, the organisation's exposure to such vulnerabilities should be evaluated and appropriate measures should be taken.*	We inquired regarding the procedures/control activities performed. By inspection using random samples, we noted that technical vulnerabilities of information systems are obtained in a timely fashion and evaluated, and appropriate measures taken to address the associated risk. Furthermore, we inspected that critical vulnerabilities are communicated to all relevant stakeholders.	No exceptions noted.
8.13	**Information backup** *Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.*	We inquired Management regarding the procedures/control activities performed. We inspected that requirements regarding backup have been established in the contract with sub-contractors that provide services where backup is relevant.	No exceptions noted.

Control objective 8:

Technological controls

Procedures and controls ensure that system and network security is implemented and effective

Nr.	GenomeDK's control activity	Tests performed by PwC	Result of PwC's tests
8.15	**Logging** *Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.*	We made inquiries of Management about the procedures/control activities carried out, reviewed the event logging procedures and inspected that they are adequate. We made inquiries of Management about the procedures/control activities carried out and reviewed the system set-up on servers. Furthermore, we inspected that logging parameters are set up to ensure that actions performed by users with extended access rights are logged. By random inspection, we inspected that logs from critical systems are protected against unauthorised access and tampering. By random inspection, we also inspected that adequate follow-up on logs from critical systems is performed.	No exceptions noted.
8.19	**Installation of software on operational system** *Procedures and measures shall be in place to securely manage software installation on operational systems.*	We inquired Management regarding the procedures/control activities performed. We inspected that software installation on operational systems are managed appropriately and according to current procedures.	No exceptions noted.
8.20	**Networks security** *Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.*	We made inquiries of Management about the procedures/control activities carried out. We observed that the network is segmented into smaller networks to reduce the risk of unauthorised access Access to the network is segregated into relevant user groups based on users' work-related need.	No exceptions noted.

Control objective 8:

Technological controls

Procedures and controls ensure that system and network security is implemented and effective

Nr.	GenomeDK's control activity	Tests performed by PwC	Result of PwC's tests
8.21	**Security of network services** *Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored*	We made inquiries of Management about the procedures/control activities carried out. We observed that the network is segmented into smaller networks to reduce the risk of unauthorised access. Access to the network is segregated into relevant user groups based on users' work-related need.	No exceptions noted.
8.22	**Segregation of networks** *Groups of information services, users and information systems shall be segregated in the organisation's networks.*	We inquired Management regarding the procedures/control activities performed. We inspected the technical security architecture and, by inspection that the network is segmented into smaller networks to reduce the risk of unauthorised access.	No exceptions noted.
8.24	**Use of cryptography** *Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.*	We inquired cryptography management in general terms with GenomeDK. We inspected that appropriate use of cryptography and cryptographic key management have been established.	No exceptions noted.
8.31	**Separation of development, test and production environments** *Development, testing and production environments shall be separated and secured.*	We have made inquiries of Management about the procedures/control activities performed. We have observed whether, in accordance with guidelines, separate environments have been established for development, testing and operation and whether suitable segregation of duties has been established in relation to operation of new functionality.	No exceptions noted.

Control objective 8:

Technological controls

Procedures and controls ensure that system and network security is implemented and effective

Nr.	GenomeDK's control activity	Tests performed by PwC	Result of PwC's tests
8.32	**Change management** *Changes to information processing facilities and information systems shall be subject to change management procedures.*	We made inquiries of Management about the procedures/control activities carried out, reviewed the adequacy of the CM procedures and inspected that an appropriate change management system has been set up.	No exceptions noted.

5 Additional information from GenomeDK

The information included in this section is prepared by GenomeDK to provide the customer with further information. The section should not be regarded as a part of the system description. The information in this section is not covered by audit procedures performed to assess whether the system description gives a true and fair view, whether the controls supporting the control objectives presented in section 4 have been suitably designed and whether they operated effectively throughout the period. Thus, PwC's conclusion in section 2 does not cover the information in section 5.

GenomeDK has the following supplementary comments regarding the observations made by PwC:

- GenomeDK is continuously improving both technical and organizational security. Since the last assurance report, GenomeDK has further improved its information security management system and obtained an ISO 27001 certificate.
- GenomeDK has consistently worked towards its information security goals for 2025, including future-proofing the overall architecture of the system and making space for future expansions.
- GenomeDK is committed to ensuring stability and longevity by expanding the team of technical personnel. Leadership is considering multiple paths for hiring and retaining new talent.

PENNEO

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registreret, og informationerne er listet herunder.

"Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument."

Erik Anders Dupont Børglum
Kunde
Serienummer: 212d7b3e-0903-48e2-9d77-20aa7c97d88b
IP: 130.225.xxx.xxx
2025-09-17 10:10:47 UTC

Mit ID

Jesper Parsberg Madsen
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
Statsautoriseret revisor
Serienummer: 1845f1c8-669f-42ab-ba7e-8a1f6ea3011e
IP: 87.49.xxx.xxx
2025-09-17 10:20:21 UTC

Mit ID

Penneo dokumentnøgle: WQGYJ-CL6R3-VK7F7-CCBZB-GHWOR-LOLK3