IT definitions and abbreviations

Introduction and scope

The purpose of this document is to identify terms currently used in IT procedures, instructions, guidelines and templates and provide standard definitions for these terms.

An overview of the referenced sources is available in sections 2 and 3. Definitions that are based on an internal or external source are quotes. Thus, the definition text has not been changed or adjusted.

It applies to all IT systems, IT infrastructure and IT services in Novo Nordisk in scope of *[Manage IT systems including digital solutions – Q187219]*, *[Manage IT infrastructure – Q216301]* or *[Manage data analysis scripts - Q0822749].* The term 'IT solution' will be used in the remainder of this document.

Applies to

This guideline is targeted at all employees who are responsible for managing an IT solution during its lifecycle.

Table of contents

1. IT terms and definitions

Term	Definition	Source
Acceptance criteria	The criteria that a system must satisfy in order to be accepted and fit for the intended use. The acceptance criteria must cover the scope of the system and be linked to requirements from the URS and relevant parts in the design documents. Acceptance criteria are numerical limits, ranges, or other suitable measures for acceptance of test results. *Note: Other suitable measures can, for example, be Pass or Fail.*	Q218515
Access rights	The permissions or privileges granted to an individual or entity to access and use certain resources or information.	-
Add-on control	Mandatory IT security controls in the IT Risk Assessment for IT solutions connected to CORP, PSnet and Tier 1 network zones.	Q187655
Agreement	Mutual acknowledgement of terms and condition under which a working relationship is conducted. ***Within the IT process**:* *The term is used generally for a written and mutually approved arrangement between two or more parties.*	ISO 24765
ALCOA	Acronym referring to Attributable, Legible, Contemporaneous, Original and Accurate. Sometimes, the acronym ALCOA+ is used by the authorities. The 'plus' refers to Complete, Consistent, Enduring, and Available.	Q054929
Application	Software or a program that is specific to the solution of an application problem. ***Within the IT process:*** *Software installed on defined IT infrastructure that provides specific functionality to support or enable a process.*	GAMP 5
Audit	A systematic and independent examination to determine whether quality or environmental activities and related results comply with planned arrangements, and whether these arrangements are implemented effectively and are suitable to achieve objectives. *Note: Internal ISO/GMP audit and supplier audit are examples of audits.*	Q019473

Audit trail	A secure, computer-generated, time-stamped electronic record that allows for reconstruction of the course of events relating to the creation, modification, or deletion of GxP data. In addition to the above, the audit trail must document *who*, *when*, *what*, *why*.	Q054929 Add-on: Q204010
Availability	Property of being accessible and usable on demand by an authorized entity. ***Within the IT process:*** *This is one of the 3 categories related to information security protection (CIA - Confidentiality, Integrity, Availability) which is covered by the IT risk assessment.*	ISO 27000
Backup	A copy of software or data for recovery purposes: • Software backup: A copy of software created to ensure that in the case of a failure, or after modifications during development or during operation, the latest and correct software version is available and the full IT solution can be restored. • Data backup: A copy of current data ensuring that in case of a failure where the data are corrupted or lost, the data can be restored. *Note from [Protecting and handling information - Q190751]: Backups are not covered by the retention periods stated in the KEEPit system or subject to legal hold.*	-
Baseline	A snapshot at a specific time of approved specification, configuration or IT solution that serves as the basis for further activities and that can only be changed through change control.	-
Biometrics	A method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.	21 CFR Part 11
Business continuity planning	Is a series of related activities and processes concerned with ensuring that an organization is fully prepared to respond effectively in the event of failures and disruptions.	GAMP 5
Code review	Code review has two objectives: • To ensure that programming standards (see 'coding guideline') are consistently and correctly applied • To ensure that the code is written in accordance with the design documentation	GAMP 5

	The review aims to ensure that the code is fit to enter testing (module, integration or system tests), and that the code can be effectively and efficiently maintained during the period of use of the application.	
Complex custom code	Refers to custom software that is specifically designed and written for a particular application or IT solution and is not based on pre-existing code or pre-built software components. This type of code is typically created from scratch and requires a high level of expertise and knowledge in programming languages and software development. Extensive custom code is often used when off-the-shelf software solutions are not available or do not meet the specific needs of a particular project or organisation.	-
Confidentiality	Property that information is not made available or disclosed to unauthorised individuals, entities or processes. *Note: In NN, confidentiality is defined in the SOP Q190751.* ***Within the IT process:*** *This is one of the 3 categories related to information security protection (CIA - Confidentiality, Integrity, Availability) which is covered by the IT risk assessment.*	ISO 27000
Configuration	Configuration constitutes: • The components of an IT solution, i.e. hardware, software and parameter settings. • Parameterisation, i.e. what is changeable in relation to configuration items and their attributes in an IT solution without having to change the source code of the IT solution or its components.	-
Configuration item (CI)	A component of an IT solution that is identified and managed as a unit to keep the configuration in control. The CI should not change as a result of the normal operation of the IT solution; and it can only be changed through change control.	-
Configuration specification (CS)	Configuration specification should be provided for configured products and cover the appropriate configuration of the software product that comprise the IT solution to meet specified requirements. This includes, but is not limited to: • Required configuration settings or parameters • Dependencies and impacts on other modules or systems • Infrastructure items such as operating systems and layered software.	GAMP 5
COTS	Commercial Off-the-Shelf.	GAMP 5

	Software defined by a market-driven need, commercially available, and whose fitness for use has been demonstrated by a broad spectrum of commercial users.	
Critical aspect (CA)	Critical aspects are functions, features, abilities, performance or characteristics to ensure consistent product quality and patient safety. *Note:* • *Product quality means that we ensure the safety and efficacy of our products.* • *The physical product and the data, including analytical results, that document the product and process goes hand-in-hand and should always be considered together. For that reason, integrity of the data documenting the product and process is considered to be part of product quality.*	Q218515
Critical thinking	Critical thinking is the process of analysing, evaluating and synthesising information to make reasoned judgment or decisions. It involves questioning assumptions, considering multiple perspectives and using logic and evidence to arrive at well-informed conclusions. ***Within the IT process:*** *Critical thinking promotes informed decision-making and good judgment on where and how to scope and scale quality and compliance activities for IT solutions. It relies on knowledge of the supported business process and on the detailed comprehension and analysis of where the business process can potentially impact patient safety, product quality and data integrity.*	-
CSM	Continuous Solution Monitoring. *Note: CSM functionality is part of ServiceNow ITOM.*	-
Data	Data is information recorded by manual or automated processes. ***Within the IT process:*** *Data is information that is input, processed, stored and/or output in an IT solution.*	Q190751
Data integrity	The degree to which a collection of data is complete, consistent, and accurate.	Q190751
Data lifecycle	The four phases (create, use, archive, destroy) that physical and recorded information moves through in its lifetime.	Q190751

	• Create: Life cycle phase in which information is recorded by manual or automated processes. • Use: Life cycle phase in which data are processed, reviewed, analysed, reported, transferred etc. and in which data supports decision making. • Archive: Life cycle phase in which data are protected from the possibility of being further modified or deleted, and in which readability of data is retained throughout the required retention period. • Destroy: The destruction phase refers to the period after the end of retention where the data is eliminated or deleted, beyond any possible reconstruction.	
Defect	Imperfection or deficiency in a work product where that work product does not meet its requirements or specification and needs to be either repaired or replaced. ***Within the IT process**:* *A defect, including software bug, is connected to design, development and verification activities. During operation a defect is regarded to be an IT incident.*	ISO 24765
Deployment	Any case where software and/or settings are pushed or otherwise made available in the relevant environment (for instance, development, test/validation or production environment). ***Within the IT process**:* *Deployment is not the same as release.*	-
Design review	Design reviews evaluate deliverables against standards and requirements, identify issues, and propose required corrective actions. They are planned and systematic reviews of specifications, design, and development. *Note: In the qualification terminology traditionally known as 'design qualification (DQ).*	GAMP 5
Design space	The multidimensional combination and interaction of input variables (e.g. material attributes) and process parameters that have been demonstrated to provide assurance of quality. Working within the design space is not considered as a change. Movement out of the design space is considered to be a change and would normally initiate a regulatory post-approval change process. Design space is proposed by the applicant and is subject to regulatory assessment and approval.	GAMP 5

	Within the IT process: *Design space is the software configuration possibilities provided to the customer via standard interfaces and functions (see 'Configuration'). Note: This does not include coding.*	
Design specification (DS)	Design specification: • should contain sufficient detail to enable the system to be built and maintained • provides a detailed and technical expansion of the functional specification • is usually required for custom applications (GAMP category 5).	GAMP 5
Development environment	An environment used to create or modify IT solutions. Development environments are typically not subject to the same degree of control as test/validation or production environments.	-
Development model	Framework or methodology used to guide the process of software development. It provides a structured approach to building software by outlining the steps involved in the development process and the order in which they should be completed. Development models can vary in their complexity and the specific steps. There are many different development models, including Waterfall, Agile, Scrum and DevOps. The choice of development model will depend on the specific needs and goals of the project, as well as the resources available.	-
Development platform	Development platforms are designed to provide citizen/professional developers with the tools and resources they need to create software applications. These platforms typically include programming languages, integrated development environments, software development kits, application programming interfaces (APIs) and other tools and resources that are necessary to develop software applications. Examples of development platforms in NN are Power Platform, Alteryx, Tableau and RPA-UiPath. Development platforms should be managed according to *[Manage IT infrastructure – Q216301]*.	-
Deviation	When we do not follow a procedure, specification or other standard approved in the Quality Management System in processes that are subject to regulatory requirements within healthcare, including GXP requirements.	Q205479

	For medical devices, the above definition includes deviations relating to nonconforming products. For IT Systems or IT Infrastructure a deviation is defined as an IT incident affecting data or functionality that directly impacts product quality, patient safety or compliance with regulatory documentation submitted to authorities. IT incidents outside of this definition are handled according to [*Manage IT Systems including digital solutions - Q187219*] or *[Manage IT infrastructure – Q216301]*.	
Digital solution	A digital solution refers to a technology-based product or service that provides a solution to a particular problem or need. It involves the use of digital tools, such as software and applications, to address a specific challenge or to improve an existing process. Digital solutions should be managed according to *[Manage IT Systems including digital solutions - Q187219]*.	-
Disaster	A major IT incident affecting multiple IT solutions and which is escalated to initiate one or more IT recovery plans (e.g. fire at the data centre).	-
Dynamic data format	"Dynamic" means that the data format and media allows interaction between the user and the content of the data. For example, an analytical chromatographic record is dynamic in the sense that it may allow the user to change the baseline and reprocess chromatographic data so that the resulting peaks may appear smaller or larger. A data set printed to pdf or paper listing data points is not dynamic in the sense that the user can only read the data points one by one.	Q054929
Electronic record	A record in electronic form. Electronic means any combination of text, graphics, data, audio, pictures or other information in digital form that is created, modified, maintained, archived, retrieved or distributed by an IT system. An electronic record may also include an applied electronic signature. In NN, electronic records subject to GxP regulatory requirements are called 'GxP data'.	Q153763 Q204010
Electronic signature	Electronic signature is a legally binding equivalent to a handwritten signature. The term is generally used as an umbrella term that covers anything from simple signatures, like drawing your name with a finger on a screen, to advanced digital signatures based on specific encryption technology. In Novo Nordisk, we use healthcare-regulated (cGxP) electronic signatures, see [*Manage IT Systems including digital solutions – Q187219*] and [*Manage data integrity in IT solutions*	Q054929

	- *Q204010*]. A healthcare-regulated electronic signature is an entry made into an IT system or computerised equipment by an individual which unambiguously identifies that individual. We use it to document that specific events/actions (for example approval, review, or verification) have occurred in accordance with the regulation. An electronic signature applied via a specific encryption technology is called a digital signature. Digital signatures are generally used on pdf documents to lock the document for editing and to embed the signature directly into the document.	
End-user	An individual who directly uses the IT solution for its intended purpose. *Note: This includes super users and other users within the business process.*	ISO 24765
Expected result	Expected results are the detailed specification of what is expected for the individual test steps.	Q218515
Fit for the intended use	The intended use is what we want the IT solution to do and the business need it should fulfil. Being fit for use requires suitable design, implementation, control and maintenance.	ITIL
Functional specification (FS)	Functional specification is normally written by the supplier and describe the details functions of the system, i.e. what the system will do to meet the requirements.	GAMP 5
GDPR	The EU General Data Protection Regulation (GDPR), effective 25 May 2018, imposes strict requirements on how entities based in the EU and offering services to EU residents can collect, use, and store personal data.	GDPR
GIA	Group Internal Audit.	-
GISP	Global Infrastructure Standardisation Programme. GISP is implemented to ensure that the IT infrastructure provides a stable environment that meets the required quality, security and business requirements of NN.	Q127938
Good IT practice	Good IT practices refer to a set of guidelines, principles and procedures that are followed by IT professionals to ensure the efficient and effective use of technology in an organisation. These practices are designed to ensure that IT solutions are secure, reliable and available to meet the needs of the organisation and its users. Examples of Good IT practices are: • ISO (International Organization for Standardization)	-

	• ITIL (Information Technology Infrastructure Library) • COBIT (Control Objectives for Information and Related Technology) • NIST (National Institute of Standards and Technology) • ISPE (International Society for Pharmaceutical Engineering) • GAMP (Good Automated Manufacturing Practice) • IEEE (Institute of Electrical and Electronics Engineers). ***Within the IT process:*** *The operationalisation of the IT process activities described in the IT SOPs follows Good IT practices and is supported by IT solutions, templates and guidelines that are available on the IT&Q Portal.*	
Gross risk	Gross risk is the risk assessed *without* mitigating security controls applied, however considering controls in place that the IT solution manager cannot affect.	Q187655
GxP	Regulatory requirements in the form of 'Good ... Practice". It is the common name for grouping GMP, GLP, GCP, GDP, and current good industry practices. Examples of GxP areas are: • Good Manufacturing Practices (GMP) • Good Laboratory Practices (GLP) • Good Clinical Practices (GCP) • Good Pharmacovigilance Practices (GVP) • Good Distribution Practices (GDP).	Q166087
GxP data	GxP data is electronic data in scope of regulatory requirements within GxP.	Q204010
GxP requirements	Requirements based on health authority regulations to the different activities performed throughout the product life cycle, from developing the drug, medical devices, or the treatment, to delivering them to patients.	Based on Q166087
GxP signature	See 'Electronic signature'.	-
Harm	Injury or damage to health, including the damage that can occur from loss of product quality or availability.	Q176354
Hazard	Potential source of harm.	Q176354
Human readable form	A display or printout of data, which is readable by a person, for instance an inspector, with the purpose of understanding and interpreting the data, as opposed to information only readable by an IT system.	Q054929
Information security	Preservation of confidentiality, integrity and availability of information.	ISO 27000

	Within the IT process: *The protection of information and information technology (IT) solutions from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability.*	Q187655
Information technology (IT)	The use of technology for the storage, communication or processing of information. The technology typically includes computers, telecommunications, applications and other software. The information may include business data, voice, images, video etc. Information technology is often used to support business processes through IT services.	ITIL
Infrastructure as a service (IaaS)	IT infrastructure delivered and operated as a service by an IT supplier. See 'IT infrastructure'.	Q216301
Inspection	Inspections from Health Authorities help us ensure continued focus on high quality and safety, and the outcome of inspections is critically important for keeping our license to operate. We must therefore do our utmost to cooperate and respond to requests related to inspections.	Q169237
Installation verification	Documented verification that a system is installed according to written and pre-approved specifications. *Note: In the qualification terminology traditionally known as 'installation qualification (IQ).* ***Within the IT process:*** *Verification in the test/validation environment documenting that the IT solution is installed and/or deployed correctly (this includes the IT infrastructure it is running on) and that the IT solution complies with the agreed design.*	GAMP 5
Integrity	Property of accuracy and completeness. ***Within the IT process:*** *This is one of the 3 categories related to information security protection (CIA - Confidentiality, Integrity, Availability) which is covered by the IT risk assessment.*	ISO 27000
IT change	The addition, modification or removal of anything that could have an effect on IT services. The scope should include changes to all architectures, processes, tools, metrics and documentation, as well as changes to IT services and other configuration items.	ITIL

	Within the IT process: *There are three types of IT changes:* • *Normal IT change: A change following the normal process for authorisation and implementation of changes.* • *Standard IT change: A repetitive change pre-approved in for instance the operation and maintenance description.* • *Emergency change: When there is a documented need to implement a change without following the normal process for authorisation and implementation of changes. This requires that an IT incident is raised to investigate the incident and assess the impact.*	
IT incident	Unplanned interruption to an IT service or a reduction in the quality of an IT service at a specific time. ***Within the IT process:*** *An IT incident can:* • *Have impact on information security or* • *Involve a potential personal data breach or* • *Affect data or functionality that directly impacts product quality, patient safety or compliance with regulatory documentation submitted to authorities – see 'Deviation'.*	ITIL
IT infrastructure	All the technical components, system software, databases and data files and deployed application software, technical procedures, and technical documentation used to make the information available. ***Within the IT process:*** • *The 'deployed application software' might be managed separately from the IT infrastructure, for instance as an IT system.* • *The term also covers the governance – thus, not only the information technology, but also the people managing the IT infrastructure and its documentation.*	ISO 24765
IT infrastructure system	Refers to a collection of hardware, software, and network components that work together to manage, process, store, and transmit data and information within an organization. IT infrastructure systems are used to enable or support NN 'Manage IT' process. ***Within the IT process:***	Q216301

	The term also covers the governance – thus, not only the information technology, but also the people managing the IT infrastructure system and its documentation.	
IT interface	Hardware or software component that connects two or more other components for the purpose of passing information from one to the other.	ISO 24765
IT platform	An IT platform refers to the underlying hardware and software infrastructure that supports the development, deployment and management of IT services and applications.	-
IT problem	A cause of one or more incidents. The cause is not usually known at the time a problem record is created, and the problem management process is responsible for further investigation. IT problems are also called an IT investigation which includes the investigation of root cause of IT incident(s).	ITIL
IT recovery plan	An IT recovery plan contains detailed instructions for returning specific services and/or systems to a working state, which often includes recovering data to a known consistent state.	ITIL
IT service	A service provided by an IT service provider. An IT service is made up of a combination of information technology, people and processes. IT services should be managed according to *[Manage IT infrastructure – Q216301]*.	ITIL
IT service provider	An internal IT department in Novo Nordisk providing IT services to other departments in Novo Nordisk.	Q187219
IT solution	Term used to cover IT system including digital solutions (Q187219), IT infrastructure (Q216301) and/or computerised equipment (Q0300378).	-
IT solution lifecycle	Evolution of an IT solution or IT service from conception through retirement. The IT lifecycle processes consist of a set of interrelated activities that result in the analyse, implement, operate and retire phases of system, software or hardware products.	-
IT supplier	Organization or individual that enters into an agreement with the acquirer for the supply of a product or service. *Note: The term 'vendor' is also used.* ***Within the IT process:*** *An external/non-Novo Nordisk company that provides IT services to Novo Nordisk.*	ISO 24765

IT system	Refers to a collection of hardware, software, and network components that work together to manage, process, store, and transmit data and information within an organisation. IT systems are used to enable or support NN business process(es). ***Within the IT process:*** *The term also covers the governance – thus, not only the information technology, but also the people managing the IT system and its documentation.*	-
IT system controls	IT system controls are risk mitigating controls, when specifying, designing, developing, verifying, operating and retiring the IT solution. Depending on the type of mitigating control, these can be implemented as: • Risk controls: Controls that are typically implemented as technical controls in the IT solution (for instance differentiated user access rights) or as physical controls (for instance access control to a room). • Lifecycle controls: Controls that are typically implemented in the processes of developing, implementing or operating the IT solution. The controls can be automated, semi-automated workflows or procedural controls and will often entail some recurrence. Examples can be firewall reviews, access management including review.	Q187219
Key performance indicator (KPI)	A metric that is used to help manage an IT service, process, plan, project or other activity. Key performance indicators are used to measure the achievement of critical success factors. Many metrics may be measured, but only the most important of these are defined as key performance indicators and used to actively manage and report on the process, IT service or activity. They should be selected to ensure that efficiency and cost effectiveness are all managed.	ITIL
Known error	A problem that has a documented root cause and a workaround. Known errors are created and managed throughout their lifecycle by problem management. Known errors may also be identified by development or suppliers.	ITIL
LoB	Line of Business.	-
Log	A log is a record of events that occur within a computer system, network or application. Logs are used to track and record various types of events, such as system errors, security events, user actions and application events.	-

	Audit trails are events relating to the creation, modification or deletion of GxP data. (see 'Audit trail') Logs can have different naming conventions depending on the IT solution, for example system log, history, event log, activity log and audit log.	
Low code development	A software development approach that allows developers to create applications with minimal coding. Low-code development platforms provide a visual interface that allows developers to drag and drop pre-built components to create applications. This approach reduces the amount of time and effort required to develop applications as well as the need for specialised coding skills. *Note: In NN the term LCNC (Low Code/No Code) is also used.*	-
Machine/ service account	Type of account that is used by applications, services and devices to authenticate and communicate with other applications, services and devices. Machine/service accounts are usually created and managed by system administrators, and they are often associated with specific roles or permissions that determine what actions the machine/service account can perform.	-
Major IT incident	The highest category of impact for an incident. A major incident results in significant disruption to the business.	ITIL
Maximum tolerable downtime (MTD)	The total amount of time that the business process can be disrupted without causing any unacceptable consequences. *MTD = Recovery time objective (RTO) + Work recovery time (WRT)*	ServiceNow ITOM
Metadata	Data that describe other data. Metadata are data that describe the attributes of other data and provides context and meaning about a record. Typically, metadata describe the structure, data elements, interrelationships and other characteristics of data e.g. audit trails. Metadata also permit data to be attributable to an individual (or if automatically generated, to the original data source).	Q054929
NN	Novo Nordisk.	-
OCM	Organisational Change Management.	-
Operation and maintenance (O&M) description	Describes the activities, including roles and responsibilities, required to operate and maintain IT solutions to ensure availability, performance and, that the IT solution is kept in control and is fit for the intended use at all times.	-

Operational verification	Documented verification that a system operates according to written and pre-approved specifications throughout specified operating ranges. *Note: In the qualification terminology traditionally known as 'operational qualification (OQ).* ***Within the IT process:*** *Verification in the test/validation environment documenting that the IT solution operates as intended throughout the anticipated operating ranges, as defined by the design.*	GAMP 5
Pass list (platforms)	The pass list contains platforms with preset guardrails that reduce the number of 'IT system controls' needed by you as a user. The pass list is used as one of the criteria for determining the level of risk exposure for an IT system according to [*Manage IT Systems including digital solutions - Q187219*].	-
Performance verification (PfV)	Documented verification that a system is capable of performing the activities of the processes it is required to perform, according to written and pre-approved specifications, within the scope of the business process and operating environment. *Note: In the qualification terminology traditionally known as 'performance qualification (PQ).* ***Within the IT process:*** *Verification in the test/validation environment documenting that the IT solution performs effectively according to the user requirements.*	GAMP 5
Pipeline	Software or hardware design technique in which the output of one process serves as input to a second, the output of the second process serves as input to a third, and so on, often with simultaneity within a single cycle time. *Note: Azure DevOps pipeline is an example of a pipeline in NN.*	ISO 24765
Privileged access rights	Access with elevated privileges assigned to a user who has a technical role outside the business process, referred to as a privileged user, for instance system administrator or database administrator. Privileged access rights should only be used for undertaking administrative tasks and not for day-to-day general tasks.	-
Product quality	Degree to which the product (e.g. artifact, software application, IT service) satisfies stated and implied needs when used under specified conditions.	ISO 24765

	*Note: **In relation to NN products**[1], product quality means that we ensure the safety and efficacy of our products. The physical product and the data, including analytical results, that document the product and process goes hand in hand and should always be considered together. For that reason, integrity of the data documenting the product and process is considered part of product quality.*	Q205479
Programming standards	A programming convention specifying rules governing the use of individual constructs provided by the programming language, naming, formatting and software design principles which prevent programming errors, control complexity and promote understandability of the source code. Synonymous with 'coding standard', 'coding/programming guideline' and 'coding/programming best practice'.	-
Qualified	In context of the IT process, the term covers the performance of a systematic, risk-based verification of IT infrastructure, that ensures and demonstrates that the IT infrastructure has been installed, operates and performs as intended and according to specifications.	Q216301
Quality	In Novo Nordisk we define quality as meeting the expectations and needs of stakeholders.	Q166087
Quality assurance (QA)	The Quality Assurance (QA) organisation is independent and has the final decision in quality related matters. Quality Assurance management has the authority to order a production stop and to order the stop of delivery from the area under their responsibility.	Q166087
Quality management system (QMS)	On a day-to-day basis, the Quality Management System (QMS) enables us to live up to our Quality Policy. In Novo Nordisk we have a holistic definition of the QMS, and it covers all our business aspects. It is built on ISO 9001 and includes requirements set by laws and regulations, both GxP requirements and general business requirements. The QMS consists of three core elements: • Processes - transforming input to output • Procedures - describing standards and requirements for the processes • People - operating the processes.	Q166087

[1] According to *[Novo Nordisk Quality Manual - Q166087]*, it covers NN produced biological candidates, drug candidates, compounds, APIs, drug substances, drug products, medical devices, software as medical device, invitro diagnostic and combination products that are researched, tested, developed, manufactured, or distributed by NN.

Quality risk management (QRM)	A systematic process for the assessment, control, communication and review of risks to the quality of Novo Nordisk products and patient safety across the product lifecycle. In Novo Nordisk the term covers both quality risk management for pharmaceutical products, and safety risk management for medical devices.	Q176354
Record	Information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business. *Note: Record can be physical or electronic records.*	Q190751
Recovery point objective (RPO)	The maximum amount of data that may be lost when service is restored after an interruption. The recovery point objective is expressed as a length of time before the failure.	ITIL
Recovery time objective (RTO)	The maximum time allowed for the recovery of an IT service following an interruption.	ITIL
Regression test	Regression testing challenges the system's ability to still do what it should after being modified according to specified requirements, and that portions of the software not involved in the change were not adversely affected.	GAMP 5
Release	In context of the IT process, release refers to the formal decision and process of making a new version of the IT solution available for subsequent validation activities or released for use.	-
Residual risk	Risk remaining after risk control measures have been taken. *Note: In NN the term 'net risk' is also used.*	Q176354
Risk	The combination of the probability of occurrence of harm and the severity of that harm.	Q176354
Risk assessment	A systematic process of organizing information to support a risk decision to be made within a risk management process. It consists of the identification of hazards and the analysis and evaluation of risks associated with exposure to those hazards.	GAMP 5
Risk control measures	In context of the IT process, see 'IT system controls'.	-
Sarbox	Sarbanes-Oxley Act.	Q147644
Scripts	A script is a written set of instructions or a program that is executed by a computer or other device to perform a specific task. It can be written in various programming languages such as Python, JavaScript and others. Scripts are used to automate tasks, manipulate data, and perform various operations on an IT solution. They can be run manually or	-

	scheduled to run automatically at a specific time or in response to certain events.	
Separation of duties	Refers to the principle of dividing duties and areas of responsibilities for a process or transaction among different individuals to prevent fraud and errors. The separation of duties ensures that no single person has the ability to both perpetrate and conceal errors or irregularities in the normal course of their duties. For example: administrator rights (permitting activities such as data deletion, database amendment or IT solution configuration changes) are not assigned to individuals with a direct interest in the data (data generation, data review or approval). *Note: 'segregation of duties' is an example of method for implementing the separation of duties principle.*	-
Service request (SR)	A formal request from a user for something to be provided – for example, a request for information or advice; to reset a password; or to install a work station for a new user. Service requests are managed by the request fulfilment process, usually in conjunction with the service desk. Service requests may be linked to a request for change as part of fulfilling the request. ***Within the IT process*** *There are two types of service requests:* • *Standard service request (SSR): A request that is pre-defined in a service catalogue, for instance a request to reset a password or install a workstation for a new user.* • *Non-standard service request (NSSR): A request that is NOT pre-defined in a service catalogue, for instance a request for information or advice.* *Note: Service requests are not considered IT incidents although they are generated via the IT incident workflow in ServiceNow ITSM.*	ITIL
Shift-left testing	Shift-left testing is a software development approach that emphasises testing early and often in the software development lifecycle (SDLC). This approach involves: • having testing considerations when defining requirements, and • moving testing activities to the left of the SDLC - which means that testing is done earlier in the	-

	development process than traditional testing methods. The goal of shift-left testing is to catch defects and issues early in the development process, when they are easier and less expensive to fix.	
SLA	Service Level Agreement	
SOC report	SOC (System and Organisation Controls) report is a type of report that provides information about the controls that an organisation has in place to ensure the security, availability, processing integrity, confidentiality and privacy of its IT solutions and data.	-
Software as a service (SaaS)	IT system delivered and operated as a service by an IT supplier. See 'IT system'.	Q187219
Specification	A documentation that specifies, in a complete, precise, verifiable manner, the requirements, design, behaviour, or other characteristics of a system or component, and often, the procedures for determining whether these provisions have been satisfied. The number of documents and details required to cover the above will depend on the complexity and impact of the IT solution. For example, • for small or low risk systems the functional and configuration specifications maybe combined in one document • complex and GxP critical systems may require a further hierarchy of specifications covering hardware design, functional and configuration specifications	GAMP 5
System administrator rights	Elevated privileges assigned to a user who has a technical role outside the business process, referred to as a privileged user, for instance a system administrator or database administrator.	-
SW	Software.	-
TIMS	Test Information Management System.	-
User	A user is an individual with an account in an IT solution consisting of a unique user ID and a password, assigned to one or more roles.	-
User Requirement Specification (URS)	User requirement specifications define clearly and precisely what the company wants the system to do, state any constraints, and define regulatory and documentation requirements.	GAMP 5

	Within the IT process: *User requirements are high-level descriptions of **what** is expected from the IT solution to enable or support the business process and can include functional and non-functional requirements. Specifications with detailed descriptions on **how** the IT solution must function including features, functionalities, abilities and performance or characteristics, as well as 'IT system controls', are covered by functional, design and/or configuration specifications.*	
Validation	Action of proving, in accordance with the principles of Good Manufacturing Practice, that any procedure, process, equipment, material, activity or system actually leads to the expected results. ***Within the IT process:*** *See 'Verification'.*	EU GMP
Validation deviation	Validation deviations during validation activities could be: • Issues, errors, mistakes or defects that affect the validated state • Deviating significantly from the approved protocol during execution, for example, acceptance criteria for critical aspects, operating parameters. • Results which fail to meet the acceptance criteria or expected results.	Q0300381
Verification	Verification confirms that specifications have been met. This may involve multiple stages of reviews and testing depending on the type of the system, the development method applied, and its use. *Note: In NN the term 'validation' is also used for GxP critical solutions.*	GAMP 5
Work recovery time (WRT)	The maximum tolerable amount of time that is needed to verify the IT solution and the data integrity.	-

2. Reference table: External sources

Short name	Complete name
21 CFR Part 11	FDA 21 CFR (Code of Federal Regulations) – Chapter I - Part 11 'Electronic Records; Electronic Signatures'
EU GMP	EudraLex - Volume 4 - Good Manufacturing Practice (GMP) guidelines
GAMP 5	GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems (Second edition)
GDPR	REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation.
ISO 24765	ISO 24765: 2017 'Systems and software engineering – Vocabulary'
ISO 27000	ISO 27000: 2020 'Information security management systems – Overview and vocabulary'
ITIL	Information Technology Infrastructure Library (ITIL) - A set of practices and a framework for IT activities such as IT service management (ITSM) - ITIL Service Design, ITIL Continual Service Improvement and ITIL Service Operation.

3. Reference table: Internal sources

QualityDocs ID	QualityDocs title
Q019473	Audits
Q054929	Good Documentation Practice and Data Integrity
Q127938	IT Code of Conduct
Q147644	Handling of the Sarbox Process in Novo Nordisk
Q153763	Archiving business-critical electronic records
Q166087	Novo Nordisk Quality Manual
Q169237	Inspections from Health Authorities and audits from Notified Bodies
Q176354	Quality Risk Management in Novo Nordisk
Q187219	Manage IT systems including digital solutions
Q187655	Manage Information Security in IT Solutions

QualityDocs ID	QualityDocs title
Q190751	Protecting and handling information
Q204010	Manage data integrity in IT solutions
Q205479	Deviations
Q216301	Manage IT infrastructure
Q218515	Science- and Risk-based Validation
Q0300381	Validation Deviations

Document Approvals

Approved Date: 27 Sep 2024

Approval Task Verdict: Approve	EGJE (Eirik Holm Gjerstad), (EGJE@novonordisk.com) Content Responsible 27-Sep-2024 08:43:19 GMT+0000

Approval Task Verdict: Approve	KAL (Kristian Alkjærsig), (kal@novonordisk.com) QA/QC 27-Sep-2024 09:10:34 GMT+0000

Approval Task Verdict: Approve	RMPO (Rasmus Poulsen), (RMPO@novonordisk.com) Manager 27-Sep-2024 10:01:25 GMT+0000