Manage Information Security in IT Solutions

Scope

This instruction describes how we manage information security (hereafter: "security") with a risk-based approach in Novo Nordisk and apply security controls to IT systems, IT infrastructure, computerised equipment and Health Software as outlined in instructions [Manage IT systems including digital solutions – Q187219], [Manage IT Infrastructure – Q216301], [Manage Computerised Equipment – Q0300378] and [Health Software (non-SaMD) – Q0730871].

In this document the term "IT solution" covers IT systems, IT infrastructure, computerised equipment and health software products. IT System Managers, IT Infrastructure Managers, IT Responsibles and Solution Managers are collectively referred to as "IT Solution Managers". IT System Owners, IT Infrastructure Owners, Computerised Equipment Owners and Product Owners are collectively referred to as "IT Solution Owners".

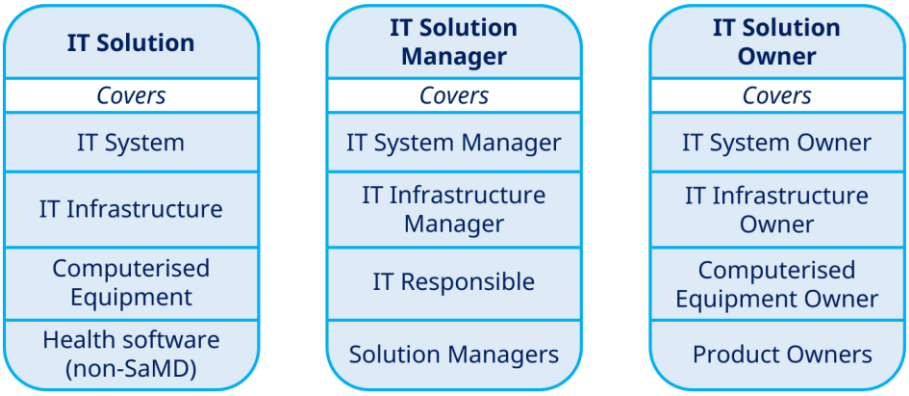

Figure 1

This instruction covers all IT solutions in Novo Nordisk.

In scope for this instruction and related tools and guidelines are:

- Any IT solutions where implementation is initiated after the effective date of the instruction.
- Existing IT solutions, where any of the following conditions apply:
  - a change has been initiated after the effective date of this instruction with an impact on the IT solution's risk posture - such as change of technological components; changes in the way the IT solution or its data are used; or changes to security control implementation
  - the IT Risk Assessment has previously been performed in the ITRA excel tool or any other IT risk assessment template[1]
  - it is chosen to implement the risk-based approach outlined in this instruction.

[1] IT solutions are granted until April 1st 2025 to complete the IT risk assessment in ServiceNow IRM. IT solutions which become supported by ServiceNow IRM after this instruction's effective date will have a grace period communicated by the IRM team.

Applies to

This instruction applies to roles with responsibilities for managing an IT solution during its life cycle, for example:

- IT Project Manager or other Project managers responsible for IT or Technology projects.
- IT Solution Manager (as defined above) responsible for the day-to-day operation of an IT solution
- Product Owners
- IT Roles with delegated responsibilities, for example a consultant who performs IT tasks or a Subject Matter Expert (SME) involved in security related activities
- QA responsible supporting the IT solution or area (if applicable)
- Professional- and Citizen Developers
- Risk managers (central or local)

Introduction

In Novo Nordisk we apply a risk-based approach to security, meaning security controls are implemented at a level which matches the risks they are mitigating.

The following steps cover the risk-based approach to how we manage security in Novo Nordisk's IT solutions:

Figure 2

This instruction is aligned with the following procedures and instructions:

- [Quality Requirements for the IT Process – Q0307516]
- [Ownership of IT solutions – Q187218]
- [Manage IT Systems – Q187219]
- [Manage IT infrastructure – Q216301]
- [Manage Computerised Equipment – Q0300378]
- [Novo Nordisk Group Risk Management Procedure – Q107066]
- [Protecting and handling information - Q190751]
- [Health Software (non-SaMD) - Q0730871]

Table of contents

1 Manage information security in IT solutions

We must protect our IT solutions and data against threats to confidentiality, integrity, and availability by ensuring a balanced level of security controls in our IT solutions.

Security controls must be considered for all components (for instance configuration items), services and integrations within scope of the IT solution (including those provided by external suppliers). All environments (such as production, validation, development, and sandbox) must have sufficient security controls implemented.

IT solutions that function as IT platforms enabling other IT solutions to deliver a business service must define and communicate the roles and responsibilities of using the IT platform and establish technical or procedural security controls to implement the split of responsibility.

> ***Example:*** *A low code/no code (LCNC) platform allows users of the IT platform to develop apps – often to support a business process. To reduce the risk of security breaches the IT platform transparently informs its users of which security controls are implemented on platform level – such as at-rest data encryption and segregation of apps, and what security controls must be implemented in the individual LCNC apps - such as code-review and access review.*

ServiceNow IRM[2] is to be used as the general IT system to document IT solutions' security risks and -controls. In special circumstances this instruction may be implemented outside of ServiceNow IRM if approved by Global Information Security (GIS) and if it follows the process steps described in this instruction.

1.1 Assess security risks and identify relevant information security controls

Information security risks are determined by the confluence of two key factors: the realistic worst-case impact (or harm) that could result from a security threat, and the likelihood of such a threat materializing into a significant (not necessarily worst-case) impact. Such threats include attempts to compromise the confidentiality, integrity, or availability of the IT solution and/or its data.

Impact and likelihood are to be considered from both a gross and net perspective.

- Gross risks (also known as inherent risks) are assessed as the impact and likelihood of a risk materialising without mitigating security controls implemented.
  Gross risks are used to identify the degree to which security controls should be implemented, but also to assess the potential impact of a risk, if an implemented control fails.

  > ***Example:*** *IT solutions run by external IT suppliers (such as cloud services) typically enforces some security controls as a default part of the service, such as encryption of network traffic or data-backup. The impact of such security controls should be considered part of the gross risk assessment, thereby lowering the gross risk. This emphasises the importance to understand what security controls come out-of-the-box when engaging with IT suppliers.*
  >
  > ***Example:*** Global Infrastructure Standardisation Programme (GISP*) applies IT standards to many types of IT on the general network, however as it's possible to get a dispensation to the GISP standard the security controls introduced as part of GISP should not be considered when assessing the gross risk.*
  >
  > ***Example:*** *On-premise IT solutions protected by corporate firewall(s) and IDS/IDP lowers the gross risk because these are general solution on network and cannot be omitted.*

[2] Areas exempted from IRM are listed in the ITQ portal [https://novonordisk.sharepoint.com/sites/ITQ/SitePages/ManageITRisks.aspx]

- Net risks (also known as residual risks) are assessed as the impact and likelihood of a risk materialising, after mitigating security controls have been implemented.
  Net risks give insight into the actual risk picture of the IT solution with current security controls in place, assuming implemented controls are working as intended.

Use the IT risk management system to identify security risks and identify relevant controls to the IT solution. The risk assessment should be initiated as early in the process as possible – such as in the analysis phase. That way, security requirements can be identified, designed, developed, and tested early on. The assessment must be updated on an ongoing basis as the requirements for the IT solution change and become more well-defined.

Guidance material is provided to assist in the implementation of security controls. References to the guidance are illustrated by light bulb symbols (💡). Guidance material is adjusted on an ongoing basis and are GIS' recommendations to effective implementation of the security controls.

Step 1 - 'Assessing information security risks and identify relevant information security controls' consists of the following steps:

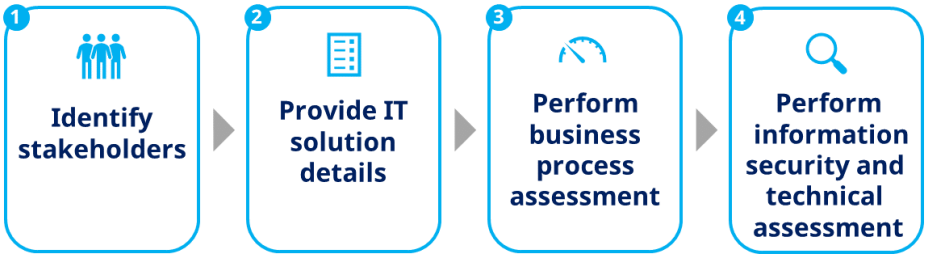

Figure 3

Responsible: Project/IT Solution Manager or delegate		
Action		**Description**
1	Identify stakeholders	All business processes supported by the IT solution should be listed to identify the relevant stakeholders to ensure that the right set of security risks and security controls are identified. Relevant stakeholders with knowledge about the IT solution, data, security and business processes could include: • Process Owner/other relevant process roles and IT Solution Owner (or delegate) who represent and know the business process(es) the IT solution is going to support • Data owner (or delegates) with insight into how business critical information is received, created and kept during the information life cycle. • IT solution Subject Matter Experts (SMEs) who have insight into the IT solution's technical setup • Line of Business SMEs who understand the business processes and data • Quality Assurance • Risk managers • GIS security advisors/partners or local security coordinators

		• Local Data Protection Responsible (DPR)[3] should be consulted if the IT solution processes confidential, sensitive or other special categories of personal data.
2	Provide IT solution details	The following information must be available or provided to support the IT risk assessment: • Solution design diagram or IT architecture overview to outline each IT solution component along with the internal/external interfaces that will be implemented. • The scope of the IT risk assessment. In this step, the boundaries of the IT solution are identified, along with the resources and the information that constitute the solution.
3	Perform business process assessment	Determine and record the classification level of the information/data managed in the IT solution according to [Protecting and handling information - Q190751]. Perform a business process assessment of the IT solution assessing the potential impact of breaches to the confidentiality, loss of integrity, and unavailability of the IT solution and/or its data. Consider the realistic worst-case scenario that could occur during a three-year period to come. For each of the three impact categories (Confidentiality, Integrity & Availability), assess which of the following impact types would be most severely impacted[4]: • Financial • Reputational • Business Ethics • Product Quality • Regulatory Compliance Once the most severely impacted impact area has been determined, assess the severity of the worst-case gross impact before mitigating security controls. Rate the impact severity by selecting "Minor", "Moderate", "Major" or "Critical" for non-financial impacts. For financial impacts, select the appropriate numerical category based on the estimated financial impact. The impact types and severity ratings included in the IT risk management system are defined by Enterprise Risk Management function in Novo Nordisk and available from ITQ[5]. Consider any impact to the supported business processes, IT solutions, devices, and possible impact on other parts of the Novo Nordisk IT landscape, such as shared IT infrastructure, if a threat materialises in your IT solution.

[3] DPR list [https://novonordisk.sharepoint.com/:x:/r/sites/BusinessAssuranceV0012/_layouts/15/Doc.aspx?sourcedoc=%7B6C75B37A-10EB-44A6-881F-4E883ED4CC04%7D]

[4] It is also possible to select "None" if there is no impact associated with either a breach to confidentiality, loss of integrity, or unavailability.

[5] [https://novonordisk.sharepoint.com/sites/ITQ/SitePages/ManageITRisks.aspx]

		Example: *A breach of confidentiality involving personal data could have both a regulatory, financial and a reputational impact. In such cases the most severe impact type (highest rated) should be chosen as the impact type, or if multiple impact types are rated similar, the impact type that is considered most relevant for a confidentiality impact.*
4	Perform information security and technical assessment	Perform a technical scoping and assessment of the IT solution to identify the appropriate security controls. Based on the business- and technical assessment an analysis should be made to assess the likelihood that specific threat scenarios[6] will materialise within the next three years. The assessment must be based on assumptions: Security trends, historical data and personal experience. Many situations cannot be predicted with certainty, especially if a threat has never happened historically but could materialise in the future. In that case, the assessment can be a qualified guess. Include rationales for your selections. This analysis is used to determine which security controls are relevant to implement, and should therefore consider the *gross* likelihood, i.e. before controls are applied. ***Example:*** *Assessing risks without controls applied (such as anti-malware) is assessing the gross risk. Anti-malware cannot block all malicious software; hence we need to assess risks considering situations where the mitigating security control fails or is absent.* Rate the likelihood by selecting the probability of the threat materialising with a significant impact within the next three-year period: • Very likely (more than 50% risk of happening) • Likely (between 25 and 50% risk of happening) • Possible (between 10 and 25% risk of happening) • Unlikely (less than 10% risk of happening) ***Example:*** *An IT solution that can be accessed from the internet may be considered "Very Likely" to have an unauthorised access threat scenario materialise if no security controls are implemented, while IT solutions that cannot be accessed from the internet would have a lower likelihood of an unauthorised access threat scenario materialising.*

1.2 Determine implementation of security controls

Global Information Security is responsible for defining and maintaining security controls and associated applicability ruleset based on security threat patterns, good security practice, regulatory requirements etc. As security threats dynamically change over time, GIS may request IT solution managers to re-assess their completed IT risk assessment either in full or for specific security controls.

[6] [https://novonordisk.sharepoint.com/sites/InformationSecurity-ITSecCentral/SitePages/Manage%20IT%20Security/Threats/SecurityThreats.aspx]

Based on the IT solution profile – such as that provided in the business and technical assessment - the IT risk management system will determine the applicable security controls that are to be implemented.

The IT solution manager must apply a risk-based approach by matching the level of implementation of a given security control to the criticality and likelihood of the risk that is being mitigated by the control. Preventive security controls are usually preferred above detective or corrective controls as they are proactive in nature.

Selected security controls are marked as mandatory or indicated as an add-on control with an asterisk (*) due to the general impact that GIS assesses a security control failure may potentially have on Novo Nordisk data or operations; or to set a lower threshold on implementation of the security control. These mandatory controls must be implemented as a minimum to the standard described.

Step 2 - 'Determine implementation of security controls' consists of the following steps:

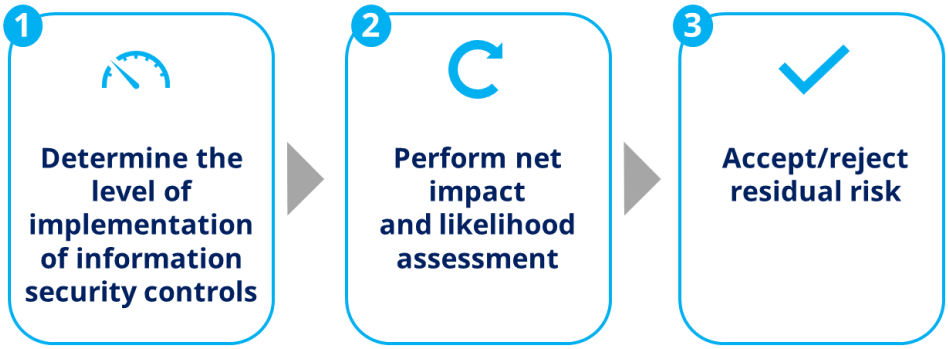

Figure 4

Responsible: Risk manager, Project/IT Solution Manager, IT Solution Owner		
Action		**Description**
1	Determine the level of implementation of security controls	Based on the input provided in the previous sections the IT risk management system will output the security controls that are relevant to address. For each security control, determine the extent to which the control will be implemented. The security controls should be implemented to the level that ensures that: • The IT solution is developed, implemented and operated in a secure and robust manner • The data handled in the IT solution is kept secure • Other Novo Nordisk IT solutions are protected from threats that could be caused by the IT solution being assessed **If a mandatory or add-on control cannot be implemented:** Security controls marked as mandatory or indicated with an asterisk (*) must be implemented in full for all applicable parts of the security control. Provide clear rationale if parts of the controls are not applicable. If the control cannot be implemented, or can only partially be implemented, clearly state this in the "Implementation considerations" field. In this case

Responsible: Risk manager, Project/IT Solution Manager, IT Solution Owner		
Action		**Description**
		it is required to obtain approval from the CISO[7] or delegate and hereby list compensating controls that are implemented. The guidance to obtain a security exception (type 1) is found at GIS sharepoint site[8]. **Connections between Novo Nordisk IT infrastructure and third parties:** The CISO must approve security controls of connections between Novo Nordisk IT infrastructure and third parties that would allow the third party to establish connections directly into Novo Nordisk IT infrastructure. This includes connections for remote maintenance. The guidance to obtain a security exception (type 2) is found at GIS sharepoint site[9]. **If the IT solution is connected to other Novo Nordisk IT solutions:** Implement relevant security controls necessary to protect the Novo Nordisk IT landscape, not just the specific IT solution being assessed. ***Example:*** *An IT solution has a minor impact of unauthorised access. Therefore, strict security controls related to user management, such as multifactor user authentication, are not considered relevant for the solution in isolation. However, as it is connected to other IT solutions, weak user management controls may pose a significant risk to other IT systems or services in Novo Nordisk, as attackers may use the weakest one as an entry point into other IT solutions on the same network.* **IT solutions relying on external IT suppliers:** For each security control to be implemented for the IT solution, define who is responsible. This may be Novo Nordisk, one or more IT suppliers, or a split. Where IT supplier is responsible, request information from the IT supplier(s) on how they handle implementation of the identified relevant controls in the IT solution. Describe if this is sufficient to mitigate the risks to an acceptable level and identify additional controls if necessary. For IT suppliers, ensure all security controls are included in the contract security appendix[10], Service Level Agreements (SLAs), or other system documentation.
2	Perform net impact and likelihood assessment	Assess *net impact* and *net likelihood* for the listed security threat scenarios in the IT risk management system. *Net impact* and *net likelihood* are assessed based on the assumption that the security controls are implemented as described. Provide comments to justify the selected net impact and net likelihood ratings, e.g. referring to implemented security controls. As security controls are implemented with the purpose of lowering the impact and/or likelihood of security threats, it is only possible to select values that are equal to or lower than the respective gross ratings.

[7] Chief Information Security Officer, the CVP of Global Information Security in Novo Nordisk
[8] [https://novonordisk.sharepoint.com/sites/InformationSecurity]
[9] [https://novonordisk.sharepoint.com/sites/InformationSecurity]
[10] Located in Information Security Toolboxes under [https://novonordisk.sharepoint.com/sites/InformationSecurity]

Responsible: Risk manager, Project/IT Solution Manager, IT Solution Owner		
Action		**Description**
3	Accept/reject Residual risk	Following completion of the IT Risk Assessment the IT Solution Owner must accept or reject the residual risk of the solution as this role holds accountability of the IT solution. Evidence of owner approval must be documented.

1.3 Implement and maintain security controls

Implement the security controls as identified and described in section 1.2 to mitigate the gross risk to an acceptable net risk. For risk-based controls the threshold is set by the IT Solution Owner whereas for mandatory or add-on controls the minimum threshold is defined by GIS.

Security controls must be implemented in a secure and robust manner that remains effective throughout the IT solution's lifecycle. This includes proper configuration, continuous monitoring, and testing to detect and prevent security incidents.

It is recommended to use the security controls to supplement the list of user requirements for IT solutions - in particular before engaging with outsourcing-, partnering- or cloud services.

Step 3 - 'Implement and maintain security controls' consists of the following steps:

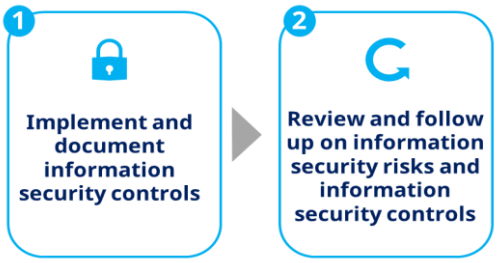

Figure 5

Responsible: Project/IT Solution Manager or delegate		
Action		**Description**
1	Implement and document security controls	Information security controls must be implemented and documented in relevant IT solution documentation. To investigate or implement security controls delivered by GIS, review the IT Security Service Catalogue on the GIS sharepoint site[11]. Depending on the control objective, document control implementation in relevant documentation, such as: • Requirement specification • Functional / technical design specification • Operation and maintenance SOP • SLAs / contracts with IT suppliers • Internal interface agreements The stated implementation of security controls must be (re-)attested in ServiceNow IRM on a frequency determined by GIS at individual security control level.

[11] [https://novonordisk.sharepoint.com/sites/InformationSecurity]

		During (re-)attestation it must be attested that the control is still implemented and effective to the level described and required to reduce the risk. If this is not the case then the control implementation must be updated just as any changes to net/residual risk must be documented. Evidence of (re-)attestation must be documented for later review.

2	Review and follow up on security threat scenarios and information security controls	Review and follow up on business impact assessment and security threat scenarios every three years (minimum) or when there are changes to the risk of the IT Solution, such as:
		• Changes in the technological components of the IT solution
		• Changes in the way the IT solution and its data are used, which may pose new risks to the IT solution, such as:
		  ○ Upgrades of the technical platform or landscape
		  ○ Major change in the number of users
		  ○ Change in geographical use of the IT solution
		  ○ Change of vendor or hosting environment
		  ○ Change of data classification handled by the IT solution
		The review may lead to either implementation of new, update of existing, or removal of irrelevant security controls if the security risks to the IT solution have changed, for instance if new security threat scenarios have emerged, or if security threats are no longer relevant.
		
		Update the IT risk management documentation to reflect these changes. Even though no changes have occurred, evidence of review must still be documented.

2. Overview of approvals and risk review

Required approvals and risk reviews	
Type of approval or decision	**Who**
Accept or reject the net risk of the solution [Ownership of IT solutions - Q187218]	IT Solution Owner
Implementation of information security controls	IT Solution Manager or delegate
Mandatory security controls not implemented in full or partially (Type 1 security exception)	CISO or delegate
Connections between Novo Nordisk IT infrastructure and third parties (Type 2 security exception)	CISO

3. Definitions

Below are listed the definitions of specific security related terms. Refer to the IT definitions on ITQ for general IT terms and definitions.[12]

Term	Definition
CISO	Chief Information Security Officer, the CVP of Global Information Security.
DPR	Data protection Responsible [13]
GIS	Global Information Security [14]
Gross risk (Inherent risk)	Gross risk is the risk assessed *without* mitigating security controls applied, however considering controls in place that the IT solution manager cannot affect. Examples of controls *not* to include when assessing gross risk often includes user access controls, logging and monitoring, vulnerability and patch management etc.
IDS/IPS	Intrusion detection systems (IDS) are security tools that monitor network or system activity and alert administrators to potential security breaches, while intrusion prevention systems (IPS) are security tools that not only detect but also prevent intrusions on a network or system by actively blocking malicious activity.
Information Security	The protection of information and information technology (IT) systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability.
IT risk management system	IT risk management system refers to the IT system chosen to implement the IT risk management process. In Novo Nordisk the general IT risk management system is ServiceNow IRM and only in special cases can other systems be used after approval from GIS.
IT solution	Covers IT system, IT infrastructure and Computerised equipment.
IT solution manager	Covers IT system manager, IT Infrastructure Manager and IT responsible. See IT Roles & Responsibilities on ITQ [https://novonordisk.sharepoint.com/sites/ITQ/SitePages/Roles.aspx]
IT Solution Owner	Covers IT system owner, IT infrastructure owner and Computerised Equipment Owner. See IT Roles & Responsibilities on ITQ [https://novonordisk.sharepoint.com/sites/ITQ/SitePages/Roles.aspx]
Net risk (Residual risk)	Net risk is the risk assessed *with* all implemented mitigating security controls taken into consideration. Any security controls that are planned, but not yet implemented, are not to be included, as they do not mitigate the risk before they have been implemented.
Preventive, detective and corrective security controls	Preventive security controls are measures put in place to prevent or deter security breaches, Detective controls are measures used to detect security breaches, Corrective controls are measures

[12] [https://novonordisk.sharepoint.com/sites/ITQ/SitePages/Definitions.aspx]
[13] [https://novonordisk.sharepoint.com/sites/BusinessAssuranceV0012/SitePages/Data-Protection-Office(1).aspx]
[14] [https://novonordisk.sharepoint.com/sites/InformationSecurity]

	implemented to reduce the impact of security breaches and restore normal operations.
Professional and Citizen developers	Professional developers are individuals who have formal training and experience in software development, while citizen developers are typically end-users, who use development and programming tools to create or customize business applications.
Risk Manager (Central and local)	See IT Roles & Responsibilities on ITQ [https://novonordisk.sharepoint.com/sites/ITQ/SitePages/Roles.aspx]

Document Approvals

Approved Date: 24 Aug 2023

Task: Approval Verdict: Approve changes & release	ERJP (Erling Jepsen), (ERJP@novonordisk.com) Content Responsible 24-Aug-2023 08:38:01 GMT+0000

Task: Approval Verdict: Approve changes & release	LRSF (Lars Falch), (LrsF@novonordisk.com) Content Owner 24-Aug-2023 12:28:42 GMT+0000

Task: QA Approval Verdict: Approval changes & release	SUPO (Susanne Poulsen), (supo@novonordisk.com) QA 24-Aug-2023 12:41:12 GMT+0000