VCDM ISO27001 Statement of Applicability - 2025

The Visma Cloud Delivery Model (VCDM) Statement of Applicability (SoA) outlines the security controls implemented within the VCDM framework to ensure compliance with ISO 27001. It provides transparency to our customers, potential customers and auditors, on how security requirements are met across Visma's cloud services onboarded to VCDM, detailing the applicable controls and their implementation status.

Visma Owned: Public

Objective/Control	Status	Overview of Implementation/Remarks
5 Organizational controls		
5.1 Policies for information security	Managed	VCDM information security policy and topic-specific polices: ● PO: VCDM Information security policy ● PO: VCDM Policy - Privileged Access ● Visma Group Security Policies VCDM policies are annually reviewed in addition to continuous updates when needed. The review is done by the VCDM Steering Group and approved by the Visma's Quality Improvement Group (QIG).
5.2 Information security roles and responsibilities	Managed	Specific roles for VCDM are defined in Visma QMS (Quality Management System) ● R: VCDM Security Engineer ● R: VCDM Service Owner ● R: VCDM Process Owner (for Security) ● R: VCDM Area Owner (for Security)
5.3 Segregation of duties	Managed	Segregation of duties in VCDM are described under the RACI matrix in different VCDM procedures. ● VCDM Management system and Certifications - list of all VCDM roles and procedures ● VCDM Organization - describes VCDM roles and processes for SDTs

5.4 Management responsibilities	Managed	The managing director of each Visma company sets a target tier for each of their applications which reflect the risk acceptance for that product and the security requirements they need to fulfill to perform on that target tier. This is communicated through the onboarding process for all employees from the Visma Group. For SDTs personnel, this is handled through the specific VCDM onboarding process. ● P: VCDM Service Onboarding
5.5 Contact with authorities	Managed	Today's practice is formalized through the work descriptions of the Security Director and relevant members of his/her staff. In addition to that, there is a dedicated Visma Cyber Crime Center with close contact to relevant authorities like PST, NSM, NSR, Europol and the police. ● Visma Cyber Crime Center VC3
5.6 Contact with special interest groups	Managed	Several contacts with external security organizations outside Visma. like i.e. Europol, Cloud Security Alliance, Information Security Forum, ISACA, ect. Internally: ● Security Guild - A group of all security engineers working for Visma companies ● VCDM Service Owner Community
5.7 Threat Intelligence	Managed	Cyber Threat Intelligence is provided from the Visma GSOC and is used both on application level and legal unit level. ● CTI - Cyber Threat Intelligence
5.8 Information security in project management	Managed	Security requirements are an integrated part of the whole software development life cycle, regardless if that is managed as a project or not (refer to control 8.25) ● PO: VCDM Information security policy ● VCDM Security Requirements
5.9 Inventory of information and other associated assets	Managed	VCDM assets are categorized in primary and supporting assets. Inventory of VCDM primary assets can be found in

		our internal systems: Hubble and Index. • Visma Hubble • Visma Index • VCDM Risk Management - Asset register including asset ownership
5.10 Acceptable use of information and other associated assets	Managed	Covered by policies mentioned in 5.1, Visma Code of Conduct that gives guidelines for handling assets, and in employee's contracts.
5.11 Return of assets	Managed	Covered by Visma Group policies and implemented through HR processes (like offboarding process) on group level and legal unit level, which ensures that relevant assets are returned prior to the employee's departure. • Personal computer management policy • Acceptable Use Policy • Mobile Device and Removable Storage Policy
5.12 Classification of information	Managed	Group Policy: • Information classification and handling policy Implementation: • Labeling information based on the policy • Checked also in Compliance Self Assessment - Processing activities - Categorization of data
5.13 Labeling of information	Managed	Visma group policy on Information classification and labeling of information, and all VCDM related information/documents are labelled according to this policy. • Information classification and handling policy
5.14 Information transfer	Managed	Requirements have been identified and communicated through group policies: • Information classification and handling policy • Email security policy • Transfer of Personal Data Compliance to this is also checked in:

		Compliance Self Assessment - Data Deletion - export of data
5.14 Information transfer	Managed	Requirements have been identified and communicated through group policies: ● Information classification and handling policy ● Email security policy ● Transfer of Personal Data Compliance to this is also checked in: Compliance Self Assessment - Data Deletion - export of data
5.15 Access control	Managed	VCDM is in context of the products we deliver, and compliance to this control is checked through different security services in VASP, VATP and VCDM such as: ● Compliance Self Assessment - P01 (Access to data) ● Security Self Assessment - - SEC03 - Access Control quality ● PO: VCDM Policy - Privileged Access ● PDAB Public Cloud Architecture Assessment - SEC1. SEC2, SEC3 General access control is covered by policies in 5.1 and other HR procedures, including onboarding , change of employment, and offboarding of personnel. For physical access control, refer to section 7 in this document.
5.16 Identity management	Managed	User registration and de-registration is handled through VOM (Visma Organisation Master) following HR processes. ● VOM - Visma Organization Master ● P: Onboarding ● P: Offboarding ● P: Employee Changes
5.17 Authentication information	Managed	Allocation and management of authentication information is controlled and handled through a managed process. Policies, procedures, and different

		solutions in place to communicate this to users in addition to annual awareness campaigns aimed at raising the level of knowledge and awareness of risks to all users when it comes to this topic. ● PO: VCDM Policy - Privileged Access - Privileged User Access ● Privileged Access Management Templates ● Password policy ● Password manager ● Use of Single Sign on (SSO) - Visma Connect ● 2FA playbook
5.18 Access rights	Managed	Normal user access provisioning, review and removal of user access rights is handled through VOM (Visma Organisation Master) following HR processes such as onboarding and offboarding that covers user registration and access. VOM - Visma Organization Master P: Onboarding P: Offboarding P: Employee Changes VCDM has a specific process and policy when it comes to privileged access. ● PO: VCDM Policy - Privileged Access ● Privileged Access Management Templates
5.19 Information security in supplier relationships	Managed	VCDM has specific processes when it comes to suppliers. ● VCDM Vendor Management Guideline ● VCDM & VASP Coordination Group ● VCDM & VATP Coordination Group ● VCDM Risk Management ● VCDM Risk Methodology In addition to the VCDM specific processes, Visma has a supplier code of conduct and supplier assessment which is sent as part of the yearly assessment from the Procurement team. In addition to that, specific tooling in VASP is used

		to make sure that third party libraries used by our products are not vulnerable and patched. - Visma Code of Business Conduct - Visma's Supplier Code of Conduct - Vendor Management Policy & Procedure - Group level
5.20 Addressing information security within supplier agreements	Managed	Vendor management process of Visma is used for managing Visma licences (part of the process is the security assessment sent to the vendor) - A group wide tool is in place to manage Visma vendors. - VCDM Vendor Management Guideline - Visma's Supplier Code of Conduct - Vendor Management Policy & Procedure - Group level - VCDM & VASP Coordination Group - VCDM & VATP Coordination Group
5.21 Managing information security in the ICT supply chain	Managed	Vendor management process of Visma is used for managing Visma licences (part of the process is the security assessment sent to the vendor) - A group wide tool is in place to manage all Visma vendors. - VCDM Vendor Management Guideline - Visma's Supplier Code of Conduct - Vendor Management Policy & Procedure - Group level - VCDM & VASP Coordination Group - VCDM & VATP Coordination Group
5.22 Monitoring, review and change management of supplier services	Managed	Monitoring, review and evaluation of suppliers services is performed regularly and documented. - VCDM Vendor Management Guideline - VCDM & VASP Coordination Group - VCDM & VATP Coordination Group

		- VCDM Risk Management
5.23 Information security for use of cloud services	Managed	Regular business review meetings are conducted with cloud service providers to monitor and review performance against agreed SLA's. Annual vendor assessment is performed for cloud service providers.
5.24 Information security incident management planning and preparation	Managed	VCDM has established an incident management procedure to ensure that Information security incidents are reported through appropriate channels. Incidents are registered and reviewed as part of the VCDM incident process handling. We have also in place a step by step guidance on how to handle and report a security incident for a VCDM service. - P: VCDM Incident & Problem Management - VCDM Incident Portal - Security Incident Portal
5.25 Assessment and decision on information security events	Managed	VCDM has clear documentation on how to define and categorize information security events. - P: VCDM Incident & Problem Management - VCDM Incidents - Definition and Classification
5.26 Response to information security incidents	Managed	A documented procedure regarding how to respond to information security incidents, can be found both in the VCDM incident portal and security incident portal. - VCDM Incident Portal - Security Incident Portal
5.27 Learning from information security incidents	Managed	As part of the VCDM incident management process, an incident review report needs to be filled, where identifying the root cause and follow-ups and share learning from incidents, are part of the process.
5.28 Collection of evidence	Managed	Visma and VCDM establish and implement standardized procedures for identifying, collecting, acquiring, and preserving evidence related to

		information security events, ensuring integrity, compliance, and transparency throughout the process. ● VCDM Incident Portal ● VCDM Incident Reports ● Security Incident Portal ● Security Log Management ● Cyber Threat Intelligence Service
5.29 Information security during disruption	Managed	All VCDM services are required to have a Business Continuity Plan in place, which is followed up through yearly compliance reviews with every VCDM team. ● Business Continuity Portal ● P: VCDM Incident & Problem Management
5.30 ICT readiness for business continuity	Managed	All VCDM services are required to have Business Continuity Plan recovery strategy in place which is assessed minimum once a year. ● Business Continuity Portal ● VCDM Compliance Review template
5.31 Legal, statutory, regulatory and contractual requirements	Managed	Identification of applicable legislation and contractual requirements ● Compliance Self Assessment for products - ○ GDPR, ePrivacy directive, Accessibility directive, AI act - main focusing objectives. ● Trust Centre Regulation of cryptographic controls ● Security Self Assessment - SEC05 Crypto/hash algorithms
5.32 Intellectual property rights	Managed	Intellectual property, such as trademarks, copyrights and trade secrets, are handled through the Compliance Self Assessment, CSAP-03 - IPR Compliance Self Assessment for products
5.33 Protection of records	Managed	Visma has implemented comprehensive security measures and services to ensure that all records are protected from loss, destruction, falsification,

		unauthorized access, and unauthorized release. - VASP security services - VCDM Security Requirements
5.34 Privacy and protection of PII	Managed	Each product team should document (in the compliance assessment) how the product has taken Privacy by design and default into consideration as part of the development life cycle. - Privacy by Design and Default guideline - Compliance Self Assessment for products - Data Protection - Privacy by Design and Default - Security Self Assessment
5.35 Independent review of information security	Managed	Our approach to managing information security is reviewed independently at planned intervals through external audits, including ISO 27001 and ISAE 3402 audits, in addition to our VCDM yearly compliance review - External ISO 27001 audit - External ISAE 3402 type II report More information about this can be found in Visma Trust Center: https://www.visma.com/trust-centre/vismaclouddelivery
5.36 Conformance with policies, rule and standards for information security	Managed	All employees are responsible for respecting general security policies and the security provisions of their roles and the procedures they perform. - P: VCDM Compliance Review - P: VCDM Services - How to followup on Maturity Indexes
5.37 Documented operating procedures	Managed	All the documents related to the VCDM operating procedures are published in the VCDM portal. - VCDM Portal
A.6 People controls		
6.1 Screening	Managed	Recruitment process and guidelines in place to provide leaders in Visma with the necessary information and tools to carry out professional and efficient recruitment processes.

		● P: Recruitment process ○ Recruitment Guidelines - Screening
6.2 Terms and conditions of employment	Managed	Employee obligations for information security are included in employment contracts which are handled locally from Visma companies, and, in addition to that, all Visma employees need to align with Visma Code of Conduct where responsibilities for information security are also mentioned. ● Visma employee contract sample ● Visma Code of Conduct
6.3 Information security awareness, education and training	Managed	Visma ensures that all personnel and relevant interested parties receive appropriate information security awareness, education, and training tailored to their job functions. Each VCDM service has a designated security engineer who is a permanent member of the Security Engineer Guild, which meets twice a month to discuss security matters. Developers and engineers regularly receive training on secure coding practices and emerging security trends, reinforcing compliance with established principles, and all VCDM services are required to enroll in Secure Code Training. Additionally, for all Visma employees we provide security courses and GDPR/data protection training. We also conduct security self-assessments to identify improvements in application design, implementation, deployment, and operations. To mitigate the risks of social engineering, we conduct phishing simulations and provide a password manager tool to ensure secure best practices.
6.4 Disciplinary process	Managed	A disciplinary process is formalized through the HR process, and this is described in the personnel handbook. ● Personnel handbook ● HR process

		All Visma employees need to align with the Visma Information Security Policy and it is clearly stated that violations of this policy can be subject to disciplinary action, up to and including termination of employment or contract. This is clearly described also in the Visma Code of Conduct and employee contract. ● Visma Information Security Policy | Visma ● Visma Code of Conduct ● Visma Employee contract Security incidents and violations of Visma's security policies should be reported to the nearest manager, security contact or via security@visma.com.
6.5 Responsibilities after termination or change of employment	Managed	All employees are bound by the confidentiality clauses in the employment contract. This responsibility also continues even if the employee leaves Visma. ● Visma Code of Conduct
6.6 Confidentiality or non-disclosure agreements	Managed	All employees are bound by the confidentiality clauses in the employment contract. This responsibility also continues even if the employee leaves Visma.
6.7 Remote working	Managed	Group policy for remote working ● Remote Access Policy
6.8 Information security event reporting	Managed	Visma group has a Global Security Operation Center which is available 24/7 where these things should be reported, while reporting information security incidents can be done either through VCDM incident portal or security incident portal. ● VCDM Incident Portal ● Security Incident Portal In addition to that, Visma has a responsible disclosure (RD) program that allows security researchers and ethical hackers to report vulnerabilities they discover in an organisation's systems, applications, or products.

		This service provides a secure and legal channel for external parties to communicate potential security issues responsibly. - Responsible Disclosure service
A.7 Physical controls		
7.1 Physical security perimeters	Managed	Visma has a group policy for physical access, and physical access is handled locally from Visma companies according to their needs. The Code of Conduct also describes how all Visma employees should protect Visma's physical property. - Visma Code of Conduct - Physical access policy
7.2 Physical entry	Managed	Visma has a group policy for physical access, and physical access is handled locally from Visma companies according to their needs. The Code of Conduct also describes how all Visma employees should protect Visma's physical property. - Visma Code of Conduct - Physical access policy
7.3 Securing offices, rooms and facilities	Managed	Visma locations must be protected based on the risk profile of the location, area and assets, to minimize unauthorized access and ensure the safety of both employees and company assets. Group policy: - Physical access policy
7.4 Physical security monitoring	Managed	Visma has a group policy for physical access, and physical access is handled locally from Visma companies according to their needs. - Physical access policy
7.5 Protecting against external and environmental threats	Managed	All VCDM services are hosted in the public cloud (Google, Amazon and Azure), and this is handled through our cloud suppliers. - AWS Compliance - Azure Compliance

		- GCP Compliance
7.6 Working in secure areas	Managed	Visma has a group policy for physical access, and measures for secure areas are handled locally from Visma's companies according to their needs. - Physical access policy
7.7 Clear desk and clear screen	Managed	This is handled from several group policies (Mobile device and removable storage policy, information classification and handling policy, etc) - Visma Group Security Policies
7.8 Equipment siting and protection	Managed	In addition to protecting Visma's intellectual property, it is important to maintain sufficient security routines to protect Visma's equipment and facilities, and this is clearly stated in the Visma code of conduct. - Visma Code of Conduct - How do I protect Visma's intellectual property? In addition to that, organizational and technical control such as: group policies and encryption, MDM solutions, access controls, etc, are in place. ○ Personal computer management policy. ○ Mobile Device and Removable Storage policy
7.9 Security of assets off-premises	Managed	Visma Group Security has established group policies for securing off-site assets, which applies to remote work, mobile devices, and external data storage. In addition to that, technical measures such as encryption of devices, MDM solutions, access controls, are implemented. - Mobile Device and removable storage policy - Remote access policy - Working in public areas policy
7.10 Storage media	Managed	Visma ensures secure management of storage media across its entire lifecycle by enforcing policies that align with the organization's information classification scheme and handling requirements.

		• Mobile Device and removable storage policy • Information classification and handling policy
7.11 Supporting utilities	Managed	All VCDM onboarded services are hosted in public cloud environments. The risk of power failures and disruptions is managed as part of the Service Level Agreements (SLAs) established with these providers. • AWS Compliance • Azure Compliance • GCP Compliance
7.12 Cabling security	Managed	All VCDM onboarded services are hosted in public cloud environments, and this is managed as part of the Service Level Agreements (SLAs) established with these providers. • AWS Compliance • Azure Compliance • GCP Compliance
7.13 Equipment maintenance	Managed	To ensure the availability, integrity, and confidentiality of information, our organization has implemented policies and procedures that emphasize proper equipment maintenance. • Personal computer management policy • Acceptable Use Policy In addition to that, the responsibility of maintaining information security extends to all employees and is clearly outlined in the organization's Code of Conduct. • Visma Code of Conduct
7.14 Secure disposal or re-use of equipment	Managed	All VCDM onboarded services are hosted in public cloud environments. • AWS Compliance • Azure Compliance • GCP Compliance Local equipment are handled according to group policies and procedures for safe deletion
A.8 Technological controls		

8.1 User end point devices	Managed	Visma Group policies such as Mobile Device and Removable Storage policy and Personal computer management policy. ● Mobile Device and Removable Storage Policy ● Personal computer management policy In addition to that, Group Security offers Endpoint protection as a service for all Visma companies (products). ● Endpoint protection service
8.2 Privileged access rights	Managed	A privileged user management tool is implemented to implement the principle of least privileged and 'time-based' privileged access to the VCDM services. Privileged user access is granted based on approved requests by the service owner and the same is logged in the PUM tool for administration of the access.
8.3 Information access restriction	Managed	Access to information and associated assets is restricted and enforced through the policies, in addition to controls for privileged access defined in VCDM policy for Privileged Access. Periodic evaluations using the Security Self-Assessment – Access Control Quality is performed, to ensure ongoing compliance and effectiveness of access control measures. ● PO: VCDM Policy - Privileged Access ● Security Self Assessment - SEC03 - Access control quality
8.4 Access to source code	Managed	Read and write access to source code, development tools, and software libraries is appropriately managed and verified through our assessments. This includes the Public Cloud Architecture Assessment (SEC1 and SEC2), which evaluates access controls within cloud environments, and the Security Self-Assessment (SEC03) which checks the implementation of access control for a product. ● Public Cloud Architecture Assessment - SEC1 and SEC2 ● Security Self Assessment -

		- SEC03
8.5 Secure authentication	Managed	Secure authentication technologies and procedures are implemented using multi-factor authentication (MFA), role-based access control (RBAC), and policy-driven identity management, with access restricted based on the principle of least privilege. We utilize a privileged user management (PUM) tool for enhanced control over privileged accounts and offer a password manager to all employees. Access is monitored through audit logs and alerts, with policies and regular reviews ensuring compliance with security standards. ● PO: VCDM Policy - Privileged Access ● Password manager service ● Password policy
8.6 Capacity management	Managed	This is implemented in: ● Public Cloud Architecture Assessment and it is followed up and evaluated yearly in the compliance review with each team in VCDM, to ensure ongoing compliance and effectiveness of access control measures. ● VCDM Compliance Review Portal
8.7 Protection against malware	Managed	Local devices can be centrally managed and controlled with End Point Protection (Sentinel One) to protect against malware. In addition to that, we have continuous phishing simulation for all Vismas' employees and companies, and .awareness training to recognize Phishing and malware. ● Visma Group Security Policies ● Security Guild ● Training Portal ● Phishing simulation
8.8 Management of technical vulnerabilities	Managed	Vulnerability assessments are covered through different security testing services. Vulnerabilities identified are tracked as part of the maturity indexes and deviations if any, are handled through the follow-up process. ● Bug bounty

		- Pentest - Visma Index
8.9 Configuration management	Managed	Configurations, including security configurations, of hardware, software, services, and networks are established, documented, implemented, monitored, and reviewed through a variety of controls. The Public Cloud Architecture Assessment tracks cloud-managed services and configuration changes using tools like AWS Config, GCP Audit Logs, and Azure Activity Logs to ensure proper configuration management. Additionally, host hardening and security configurations are monitored and reviewed in the Security Self-Assessment. The VCDM Compliance Review, conducted annually by all VCDM teams, confirms that these configurations are up-to-date and properly maintained.
8.10 Information deletion	Managed	Each Visma product must have a data deletion policy for the specific product (and the link is inserted in the Compliance Self Assessment - Data deletion part) that is aligned with the group policy. - Compliance Self Assessment - Data deletion - Visma data deletion policy - Internal privacy control - Deletion
8.11 Data masking	Managed	To meet the control requiring the use of data masking, our organization has established comprehensive guidelines for pseudonymization and anonymization. - Guideline - Pseudonymization and anonymization - Google Docs We ensure compliance through a review process that is included in: - Compliance Self Assessment - Data protection - Anonymization/Pseudonymisation
8.12 Data leakage	Managed	Data leakage prevention measures are

prevention		applied to systems, networks, and devices that process, store, or transmit sensitive information through a combination of organizational and technical controls. ● PO: VCDM Policy - Privileged Access ● Privileged Access Management Templates ● Information classification and handling policy ● Visma Code of Conduct ● Security Log Management ● Compliance Self Assessment - Log data
8.13 Information backup	Managed	Backup and restoration procedures are implemented by VCDM services and reviewed as part of the annual compliance review. ● Public Cloud Architecture Assesment - REL8 Regular testing of restore of the production data and the code is also checked in: ● Compliance Self Assessment - Data restore ● Public Cloud Architecture Assesment - REL10
8.14 Redundancy of information processing facilities	Managed	All VCDM onboarded products are hosted on three biggest cloud providers (AWS, GCP, and Microsoft Azure) , which provides robust redundancy features, including geographic replication, automated failover, and high-availability zones. These measures align with our availability requirements and fulfill ISO 27001 redundancy control. We continuously monitor and configure resources to ensure resilience according to the cloud provider's best practices and service-level agreements. ● Public Cloud Architecture Assesment - REL9 ● VCDM Risk Management
8.15 Logging	Managed	Visma GSOC provides a Security Log Management service available for all products. Onboarding to this service is a mandatory requirement under the Visma

		Cloud Delivery Model (VCDM). - Security Log Management service Compliance with this logging requirement is continuously monitored and enforced through: - Security Self Assessment - SEC16 Security Logging - Product teams evaluate their logging practices against established security criteria. - Public Cloud Architecture Assesment - SEC6 - Reviews ensure proper integration of logging within cloud-based solutions to align with security best practices. - Compliance Self Assessment - Log data - Teams validate that compliance-related logging is correctly implemented and maintained.
8.16 Monitoring activities	Managed	Cyber Security Monitoring Service is a function in Visma Security which enables monitoring, detection and response to threats 24/7/365, thus improving the security posture. Cyber Security Monitoring is part of Global Security Operations Center (Global SOC) together with the Cyber Security Incident Response Team - Security Log Management - Cyber Threat Intelligence - Cyber Security Monitoring service
8.17 Clock synchronization	Managed	Time synchronization from a common predefined source applies for all VCDM services. - V-ISMS POL: Information Logging Policy
8.18 Use of privileged utility programs	Managed	Visma ensures access control and monitoring for Visma managed devices through comprehensive Mobile Device Management (MDM) and Intune services. These services enforce policies that limit unauthorized access, regulate the installation of applications, and prevent the use of unapproved utility

		programs that can compromise system integrity (based on our group policies). - Personal computer management policy - Acceptable Use Policy When changes to the production environment are required, all SDTs of services onboarded to VCDM follows a structured and tightly controlled process using the Privileged User Management (PUM) system based on PUM policy: - PO: VCDM Policy - Privileged Access
8.19 Installation of software on operational systems	Managed	Visma ensures access control and monitoring for Visma managed devices through comprehensive Mobile Device Management (MDM) and Intune service. Group policy: - Acceptable use policy | Visma
8.20 Network security	Managed	VCDM is in the context of the product we develop and for the products this is followed up through: - Security Self Assessment - SEC15: Host and Network Security basics - Public Cloud Architecture Assessment - SE7: Secure network protection implementation Internal network infrastructure in Visma is handled through another internal department.
8.21 Security of network services	Managed	VCDM operated within the context of the product we develop and for the products this is followed up through: - Security Self Assessment - SEC15: Host and Network Security basics - Public Cloud Architecture Assessment - SE7: Secure network protection implementation Internal network infrastructure in Visma is handled through another internal department.

8.22 Segregation of networks	Managed	VCDM operates within the context of the products we develop, all of which are hosted on public cloud platforms such as Azure, AWS, and GCP. The networks for our cloud-based products are also hosted on these platforms and are securely segregated. Local devices and networks are handled by another internal department in Visma.
8.23 Web filtering	Managed	DNS blacklisting on the Visma DNS servers based on the Technical Threat Feeds service
8.24 Use of cryptography	Managed	Rules for the effective use of cryptography, including cryptographic key management, are defined in the Security Policy and evaluated periodically through the Security Self-Assessment to ensure proper implementation and compliance with security requirements. ● PO: VCDM Information security policy ● SSA - Security Self Assessment - SEC 05 (Crypto/hash algorithms)
8.25 Secure development life cycle	Managed	All services onboarded to VCDM, must adhere to a 'Security by design and default' approach by integrating security measures into every stage of their product development lifecycle. System security testing is covered through mandatory security testing services and compliance is measured as part of the maturity indexes. ● PO: VCDM Information security policy ● Visma Hubble - SSA, SAST, SCA, Pentest, etc ● Implementation of security in SDLC
8.26 Application security requirements	Managed	Visma Application Security Program addresses security requirements for an application and all VCDM services are onboarded to this program and adhere to these requirements. ● PO: VCDM Information security policy
8.27 Secure system	Managed	All VCDM services follow well-defined

architecture and engineering principles		security engineering principles that guide the development and deployment of secure systems. - PO: VCDM Information security policy - Security Self Assessment - Security services
8.28 Secure coding	Managed	Secure development practices are embedded during the whole software development lifecycle (SDLC), including secure development guidelines, code reviews, and security testing at various stages. Teams utilize automated security testing tools for static and dynamic code analysis to detect and fix vulnerabilities before release. Security Services: - SAST - Static Application Security Testing - SCA - Software Composition Analysis - Pentest - Penetration Testing - SSA -Security Self Assessment Also, developers and engineers receive regular training on secure coding practices and emerging security trends to reinforce compliance with documented principles. - SCT - Secure Coding Training Service
8.29 Security testing in development and acceptance	Managed	The policy: - PO: VCDM Information security policy Security Services: - SAST - Static Application Security Testing - SCA- Software Composition Analysis - Pentest - Penetration Testing
8.30 Outsourced development	Not applicable	VCDM teams do not outsource development; development activities must be carried out by VCDM service delivery teams (SDTs). All employees and, where applicable, consultants within the SDT are required to adhere to VCDM processes,

		requirements and defined roles. SDT teams must assume full responsibility for the development and delivery of their products.
8.31 Separation of development, test and production environments	Managed	VCDM implements separate test and production environments to reduce the risks of unauthorized access or changes to the operational environments. ● VCDM Onboarding Portal ● VCDM Test Environments
8.32 Change management	Managed	A VCDM change management procedure is implemented and releases to production are logged. Release failures are logged and monitored as part of the VCDM maturity indexes. The release failures that trigger an incident, are resolved as part of the incident management process, if any. ● P: VCDM Development Test and Release ● P: VCDM Change Management ● D: VCDM JIRA Workflows
8.33 Test information	Managed	Visma does not use customer data for testing. Exception is when specially agreed with the customer, for specific purpose, typically support cases ● Compliance Self Assessment - Data protection - Anonymization/Pseudonymisation ● Guideline - Pseudonymization and anonymization - Google Docs
8.34 Protection of information systems during audit testing	Managed	All the audit tests are planned and agreed in advance, and when needed, access to data is executed by our personnel who have the necessary rights on behalf of the auditor.

Acronyms

VCDM - Visma Cloud Delivery Model

SDT - Service Delivery Team

QIG - Quality Improvement Group

PO: - policy

R: - Role

P: - Process

QMS - Quality Management System

CTI - Cyber Threat Intelligence

VASP - Visma Application Security Program

VATP - Visma Architecture & Technology Program

Visma Hubble

Visma Index

DPSA - Data Protection Self Assessment

CSA-P - Compliance Self Assessment for Products

VOM - Visma Organization Master

AD - Active Directory

GSOC - Global Security Operations Center

SLA - Service Level Agreement

BCP - Business continuity plan

EDR - Endpoint Detection and Response

SSA - Security self-assessment

SAST - Static Application Security Testing

SCA - Software Composition Analysis

SCT - Secure Code Training

SLM - Security Log Management

DNS - Domain Name System

AWS - Amazon Web Services

GCP - Google Cloud Platform