Issuer	Crusell Andreas	Approved/Reviewed	2021-06-11
Owner	Simonson Stefan	Valid for site	Global
Issued by	Group Security, AA14300	Version 1.2	Page 1(10)

Volvo Internal Control Standard for IT

Orientation

Originally the Volvo Internal Controls Standard for IT (VICS IT) was developed and applied on the IT landscape critical from a Financial Reporting perspective, part of the Volvo Group Internal Control Programme. From 2017 and onwards, VICS IT is also used as foundation to address critical parts in the IT landscape within the Volvo Group Data Privacy Compliance Programme.

Contents

Definitions and acronyms

VICS IT – Volvo Internal Controls Standard for IT

FCA - Financial Critical Application

PDS – Personal Data Solution

SMD – Solution Management Directive

VGMS – Volvo Group Management System

BSPM – Business Sub-Portfolio Manager

DM – Delivery Manager

Purpose

Financial and Personal Data are information areas impacted by legal requirements. The Volvo Group Internal Control Programme and the Volvo Group Privacy Compliance Programme are established to secure that there is a structured way of measuring and monitoring adherence to the requirements in respective area.

Financial as well as Personal data are generated and managed in different processes throughout the Group. The requirements on the affected processes and activities are derived from the Internal Control Policy and the General Directive regarding Personal Data, respectively. Both consisting of fundamental principles as well as direct requirements on the transactional/ business/ process level.

Affected processes are dependent on the IT landscape to secure that information is available, reliable, and protected from unauthorized disclosure. Hence, the IT landscape is an important part of the Volvo Group Internal Control Programme and the Volvo Group Privacy Compliance Programme.

The purpose of this Directive is to clarify roles and responsibilities, specify applicability and define the control requirements.

Scope and field of application

This Directive applies for all owners of solutions and personnel involved in the development, maintenance and operation of IT solutions and processes specified in the scope below. The Directive must also be considered when purchasing solutions or services from external suppliers, see the Cloud Security SharePoint for further information.

The applicability of this Directive is to all parts of the IT landscape in scope for the Volvo Group Internal Control Programme and the Volvo Group Privacy Compliance Programme.

IT control framework

The IT control framework specifies the control requirements of specific importance from a compliance perspective to secure an appropriate level of information security protection. In addition, the principles and responsibilities for below areas are described:

- the identification and assessment of the parts of the IT landscape in scope for the affected compliance programmes.
- the implementation and continuous adherence to the control requirements.
- monitoring and evaluation of adherence to the requirements.

Identification and assessment of IT components in scope

Applications with supporting infrastructure components in scope for the Volvo Group Internal Control Programme and the Volvo Group Privacy Compliance Programme must be identified and categorized.

- The definition of a Financial Critical Application, and related criticality levels is determined by Group Internal Control and is described in the Internal Control Guideline.
- The definition of a Personal Data Solution, and related criticality levels is determined by the Group Privacy Office and is documented in the Volvo Group Privacy Network SharePoint.

To make sure that the judgments of applications in scope for the respective compliance programme are harmonized throughout the Group and to support and monitor the implementation of the requirements, any change relating to the categorization of:

- Financial Critical Applications must be approved by Group Internal Control.
- Personal Data Solutions must be approved by the Group Privacy Office (delegated to the Data Protection Representative).

Control requirements

Overall protection requirements on the IT landscape are defined in the IT Security Directives, which are based on the global standards for information / IT security. *It is mandatory for all parts of the IT landscape to adhere to the IT Security Directives, based on the applicability.*

The control requirements, set forth below, are based on the IT Security Directives and define requirements of specific importance from a compliance perspective to secure an appropriate level of information security protection.

All control requirements take into account:

- the *value* (sensitivity/impact) of the information in the application context, considering the information it's processing and the purpose/usage of the application in the related process.
- the *information security attributes* (confidentiality, integrity, availability) that are impacting the value above.
- the information security *threats* such as human error, misuse, theft, unauthorized disclosure, external attacks etc.

Structure

The control requirements are grouped into control areas. In each control area, certain control objectives are defined. Control objectives are defining *what* must be achieved in each control area. *How* to meet the control objectives (which activities are required) depends on the context, platform, application, organizational set up, tools used etc. and is decided by the affected IT process management, product/service owners or when applicable by the external IT suppliers.

The control objectives, including applicability, and additional guidance in how to interpret the control objectives are specified in appendix 1 below.

Control areas

Control Area	Description
Access Management	Controls in the Access Management area are fundamental in order to secure that confidential information is only disclosed to authorized individuals (confidentiality) and to limit the risks for erroneous changes of information or usage of functionalities impacting the integrity or availability of the information. In addition individual accountability is secured.
Change Management/	Controls in the Change Management/ Application Development Area are required in order to:

Control Area	Description
Application Development	- provide a secure environment for system development activities - secure that only tested and approved changes are introduced to the live environment - secure that relevant security requirements are met for all changes updated in the live environment Above is essential in order to protect the confidentiality, availability and the integrity of the information and avoid any disruption to business activity.
System Management	Controls in the System Management area are covering a broad range of protection related to: - the documentation of assets and contractual agreements - prevention, identification and mitigation of vulnerabilities and intrusions - quick and effective responses to incidents
Security Architecture	Controls in the Security Architecture area are covering requirements related to enabling: - Volvo Group control over Identities and access rights - protection of information by applying cryptographic solutions - protection of infrastructure in exposed environments - detection of information leakage

Responsibilities

The responsibilities related to the control framework are directed to the IT Community.

In addition, Group Internal Control, Group Privacy Office and Group Security have specific responsibilities as outlined below.

TD/BA/GF IT department

As defined in the Volvo Group Management System (VGMS) role descriptions the business/demand side (BSPMs) is:

- Accountable for the categorization of Personal Data Solutions (PDS) and Financial Critical applications (FCA).
- Accountable to secure that Volvo Internal Controls Standards for IT (VICS IT) are adhered to for FCAs & PDSs.
- Accountable that support is given to compliance activities and that identified gaps are remediated.

In addition, TD/BA/GF has an overall accountability to continuously monitor the VICS IT compliance status for all critical solutions (FCA & PDS).

Group IT

Solution Delivery Units

For Financial Critical Applications (FCAs), Personal Data Solutions (PDSs) and other critical solutions the solution delivery units (DMs) are accountable for:

- that the Volvo Internal Control Standard for IT (VICS IT) requirements are included in established agreements.
- adherence of the control requirements for which Group IT as supplier organization is responsible.
- that compliance requests are delivered, and remediation plans are defined, executed upon and reported.

IT Process/Service owners

VICS IT are mandatory requirements that must be secured when designing processes and services. The Process and Service management respectively have the responsibility to design processes and services that meet VICS IT.

Group Security

Group Security has a responsibility to:

- define the IT control requirements, in agreement with Group Internal Control and the Group Privacy Office.
- support and monitor the implementation of the requirements.

Group Internal Control and the Group Privacy Office

Group Internal Control and the Group Privacy Office are the owners of respective Compliance programmes and are responsible to:

- define the scope of the Compliance programme and the definition of an FCA and PDS.
- ensure that the applications are categorized in a harmonized way in the Group.
- define the overall compliance requirements.
- determine the overall evaluation scope and methods.

Measurement of compliance

Measurement of compliance to this Directive provides the basis for yearly evaluation of the IT landscape in scope for the Group Internal Control Programme and the Group Privacy Compliance Programme.

Responsibility for compliance

Responsibilities to secure adherence to this Directive are defined above.

Deviations

Any exemption for VICS IT requirements must follow the IT Exemption Management Process.

Instructions on requesting an IT Exemption can be found on the IT Exemption SharePoint.

Supporting documents

In VGMS:

- Internal Control Directive (VGMS 0001-27-137)
- IT Security Directive (VGMS 0001-27-441)
- IT Security for system access (VGMS 0001-27-443)
- IT Security for physical asset management (VGMS 0001-27-444)
- IT Security for business application management (VGMS 0001-27-445)
- IT Security for networks and communication (VGMS 0001-27-450)
- IT Security for system development (VGMS 0001-27-451)
- IT Security for system management (VGMS 0001-27-453)
- IT Security for technical security management (VGMS 0001-27-454)
- IT Security for threat and incident management (VGMS 0001-27-455)
- IT Security performance (VGMS 0001-27-457)

- IT Security for information risk assessment (VGMS 0001-27-458)
- Business continuity for IT (VGMS 0001-27-463)
- IT Security for supply chain management (VGMS 0001-27-570)
- IT Security identity and access management (VGMS 0001-14-25037)
- Role description of BSPM
- Role description of DM
- Role description of SL

Other:

- Cloud Security SharePoint
- IT Exemption SharePoint
- Volvo Group IT Infrastructure Architecture Policy (VIAP)
- Volvo Group Data Privacy Network SharePoint

Version History

Date	Description of change
2018-11-12	First version.
2021-01-15	Change of owner
2021-08-16	Change of ownership, update on deviations, update of the appendix (control descriptions)

Appendix 1 – Control requirements

Below control objectives are requirements of importance from a compliance perspective and are mandatory for all Critical Solutions, based on the applicability. Clicking on the control ID will guide you to the detailed control description in VGMS.

Access management

Control ID	Control description	FCA Medium	FCA High	PDS Medium	PDS High
AM01	**Separation of activities in access administration** The following conditions within access management are met to ensure separation of activities in access administration: a) Approval of access rights and provisioning of access rights cannot be performed by the same individual. b) An individual cannot provision access rights while having business roles in the target system (If the business roles exceed read/view privileges).	X	X	X	X
AM02	**Access rights approval** All access rights must be approved by an authorized individual. One individual cannot be the sole approver of his/her own access rights.	X	X	X	X
AM04	**Access rights review and removal** Access rights to critical information and system functions are reviewed regularly to ensure individual access rights are commensurate with job responsibilities. Deviations noted are investigated and resolved in a timely manner.	X	X	X	X
AM05	**Defining authorization rules** Authorization rules for application and supporting infrastructure components must be defined and documented.	X	X	X	X
AM06	**Traceability of critical activities** Individual accountability is ensured for the accounts that can perform critical activities.	X	X	X	X
AM07	**Connect service from untrusted networks** Access from untrusted zones to applications must be subject to a sign-on process in a connect service before access is granted.	X	X	X	X
AM08	**Multiple factor authentication** Applications and supporting infrastructure components must be set up to only allow access via multi-factor authentication (MFA) for privileged users.		X		X

Change Management / Application Development

Control ID	Control description	FCA Medium	FCA High	PDS Medium	PDS High
AD01	**Logical separation of IT environments** The production environment is logically separated from the development, QA, and test environments.	X	X	X	X
AD02	**Information protection outside production environment** System development and other operational routines must be set up to secure that confidential/strictly confidential or sensitive information that is moved or copied outside of production environment is protected against unauthorized disclosure.		X		X
AD05	**Security test approval** Systems under development should be subject to security testing before being approved and promoted into the production environment.	X	X	X	X
CM01	**Separation of activities in change management** The following conflicting activities related to change management should be segregated: a) Development of change and related approval to implement into production should not be done by the same individual. b) Development of change and implementation of change in production should not be done by the same individual. c) Approval to implement and implementation of related change in the production environment should not be done by the same individual.	X	X	X	X
CM02	**Change approval** Changes to applications, databases or infrastructure components must be approved by an authorized individual before they are implemented in the production environment, with the exception of emergency changes which need to receive a post-approval within 4 weeks after deployment.	X	X	X	X
CM03	**Approval of test** Review or test of changes to applications, databases or infrastructure components must be performed and approved before the changes are implemented to production except for emergency changes which need to be reviewed/tested and approved within a timely manner after the implementation to production environment.	X	X	X	X
CM06	**Time period restrictions for changes** Changes to applications and supporting infrastructure components must be restricted during critical time periods to prevent information from being unavailable or corrupted		X		

Security Architecture

Control ID	Control description	FCA Medium	FCA High	PDS Medium	PDS High
SA01	**Access management for externally hosted solutions** Externally hosted solutions/services that requires authentication must be authenticated through Volvo identity and access management, in order to prevent unauthorized access to sensitive information.	X	X	X	X
SA02	**Encryption of information in transit** Data/information in transit (based on information applicability) must always be encrypted prior to moving and encrypted connections should be used to protect the content of the information in transit.			X	X
SA03	**Intrusion detection and monitoring** Intrusion detection and monitoring must be in place to identify suspected or malicious attacks to enable the organization to respond before serious damage is done.		X		X
SA04	**Information leakage** Information leakage protection shall be in place and include registration and monitoring of sensitive personal data, detection of disclosure, prevention and reporting of breaches.				X
SA06	**Servers in trusted and restricted network zones** Servers that contain sensitive personal data/information must be placed in trusted or restricted network zones.				X
SA07	**Browser based application protection** Internet-facing browser-based applications must be continuously monitored for external malicious activities as well as scanned for security vulnerabilities. Vulnerabilities noted must be remediated in a timely manner to ensure adequate protection from security threats.	X	X	X	X
SA08	**Encryption of strictly confidential information at rest** Strictly confidential data at rest (not actively moving from device to device or network to network) must be secured by encryption techniques to avoid unauthorized disclosure.				X

System Management

Control ID	Control description	FCA Medium	FCA High	PDS Medium	PDS High
SM01	**IT Continuity planning** IT continuity plans (covering information, applications and infrastructure components) based on business requirements must exist and be tested periodically to minimize the effect disruptions have on critical business functions.	X	X	X	X
SM02	**Backup and restore routines** Back-up and restore strategy and routines must exist and reflect the business needs. Restoration tests must be performed on a regular basis to ensure the availability and integrity of backed up information.	X	X	X	X
SM04	**Infrastructure monitoring** Infrastructure components must be monitored to ensure that system malfunctions are identified and acted upon to assure availability of critical information and functionality. Monitoring routines must cover the aspects of recording, responding and resolving.	X	X	X	X
SM05	**Critical automated batch job monitoring** Critical automated batch jobs must be monitored to ensure successful and timely completion according to business requirements. Processing routines must include the aspects of definition, detection, response, resolution, documentation, and retention.	X	X		
SM06	**Security configuration** Security configuration must be aligned with the security configuration requirements and be approved by authorized individual.	X	X	X	X
SM08	**Patching of system and software vulnerabilities** Patches must be applied in a timely manner to remediate system and software vulnerabilities.	X	X	X	X
SM09	**Accurate and up to date asset register** Solutions and underlying infrastructure components must be recorded in a centralized asset register with accurate and up-to-date information.	X	X	X	X
SM10	**Documented agreements** A documented agreement must be in place reflecting the Volvo Group IT requirements when using an external supplier and/or service provider. The agreement shall be derived from the categorization of the solution, the Business Impact Assessment and must include a “right to audit” clause.	X	X	X	X
SM11	**Data destruction** Data destruction in relation to retention, data subject rights or data found inadequate/ irrelevant at review must be secured either by physical deletion or anonymization.			X	X

= = = End of document = = =