



Risk Management System and Internal Control System at Volkswagen Autoeuropa

Company instruction or policy no. SQ-ADF-F-0090

Valid from: 01.07.2022

Last Change:

Replaces the: ADF-F-O100 - Risk Management System and Internal Control System

Verification of validity: 31.12.2024

Responsible department

for the process: Integrity, Risk & Compliance - AGC

Name: Integrity, Risk & Compliance Manager (Adélia Felício)

Telephone: +351212112732

Issuing department: Integrity, Risk & Compliance – AGC

Name: Integrity, Risk & Compliance Manager (Adélia Felício)

Telephone: +351212112732



Index

- 1 PURPOSE 3**
- 2 SCOPE..... 3**
- 3 TERMS AND DEFINITIONS AS DEFINED IN THIS POLICY 3**
- 4 PRINCIPLES AND ELEMENTS OF THE RISK MANAGEMENT SYSTEM (RMS) AND INTERNAL CONTROL SYSTEM (ICS) 4**
 - 4.1 RMS AND ICS PRINCIPLES 4
 - 4.2 THE "THREE LINES" APPROACH FOR RMS AND ICS 4
 - 4.3 FRAMEWORK IN ACCORDANCE WITH COSO ERM 5
 - 4.4 RMS AND ICS ELEMENTS 5
- 5 TASKS, AUTHORITIES AND RESPONSIBILITIES (TAR) 7**
 - 5.1 VOLKSWAGEN AUTOEUROPA BOARD OF MANAGEMENT 7
 - 5.2 DEPARTMENTS (FIRST LINE) 7
 - 5.3 INTEGRITY, RISK & COMPLIANCE DEPARTMENT (SECOND LINE) 8
 - 5.4 GROUP AUDIT (THIRD LINE) 8
- 6 RMS AND ICS CORE PROCESSES 9**
 - 6.1 QUARTERLY RISK PROCESS (QRP) 9
 - 6.2 STANDARD INTERNAL CONTROL SYSTEM (STANDARD ICS) 9
 - 6.3 REGULAR GOVERNANCE, RISK AND COMPLIANCE (GRC) PROCESS 10
 - 6.4 BUSINESS CONTINUITY MANAGEMENT (BCM) 11
 - 6.5 ROOT CAUSE ANALYSIS PROCESS (RCA) AND LESSONS LEARNED (LL) PROCESS 11
- 7 RESPONSIBILITY AND PROCUREMENT OF INSURANCE 11**
- 8 RISK ASSESSMENT 11**
- ATTACHMENT 1: TASKS, POWERS AND RESPONSIBILITIES OF THE RISK COORDINATOR 13**
- ATTACHMENT 2: OTHER APPLICABLE DOCUMENTS 15**
- ATTACHMENT 3: NOTIFICATION OF URGENCY 17**
- ATTACHMENT 4: ROOT CAUSE ANALYSIS AND LESSONS LEARNED 19**
- ATTACHMENT 5: REQUIREMENTS FOR REGULAR GRC-PROCESS 26**
- ATTACHMENT 6: REQUIREMENTS FOR QUARTERLY RISK PROCESS 34**
- ATTACHMENT 7: THE VOLKSWAGEN THREE-LINES MODEL 39**

1 Purpose

It is crucial for the sustainable success of the company that we identify risks in our business transactions at an early stage and manage them with foresight. At Volkswagen Autoeuropa, the responsible approach to deal with risks is supported by means of a comprehensive Risk Management and Internal Control System (RMS and ICS).

The purpose of this guideline is to provide additional information on Group Policy 33 "Risk Management and Internal Control System at the Volkswagen Group", ORL 53 "Risk Management System and Internal Control System at Volkswagen AG" and requirements for the Risk Management Organization set out in Group Policy 31 "Organization of the Risk Management, Compliance and Legal (GRC+L) Functions" for Volkswagen Autoeuropa in order to ensure observance of the duties of care imposed by the Volkswagen AG Board of Management with respect to the installation and operation of an appropriate and properly functioning Risk Management System (including Business Continuity Management). Furthermore, it is important to learn from occurred risks in order to be better prepared for future issues. This is supported through the Root Cause Analysis process for major occurred risks ("major problems") and a "Lessons-Learned" process, which is described in this guideline.

This Organizational Guideline defines the binding minimum standards for an effective RMS and ICS as well as for the execution of Root Cause Analyses and Lessons Learned within the Volkswagen Autoeuropa.

2 Scope

This Organizational Guideline applies to all Business Units in Volkswagen Autoeuropa.

3 Terms and definitions as defined in this policy

The term **risk** describes the possibility of events or developments occurring that have a negative impact on achieving corporate or department targets or on adherence to or the viability of corporate processes.

The **Risk Management System (RMS)** covers the principles, procedures and measures specified by company management to identify, assess, manage, control, communicate and monitor risks.

The **Internal Control System (ICS)** is used to safeguard the principles, procedures and measures (regulations) introduced by company management.

The aim of the ICS is to ensure the effectiveness and economic efficiency of business activity (this also covers the protection of assets, including preventing and detecting intentionally damage to assets), the viability of company processes, the correctness and reliability of internal and external accounting as well as adherence to the (legal) regulations that apply for the company.

Risks to achieving corporate or divisional targets are managed by the Risk Management System and risks to viability and observance of company processes are managed within the Internal Control System.

A system is described as effective if it is both appropriately designed and works in practice, i.e. the controls implemented are actually carried out.

The Business Continuity Management System (BCM) is the part of Risk Management that ensures that essential and time-critical business processes can be continued at a predefined minimum level in the event of a failure or non-availability of resources.

4 Principles and elements of the risk management system (RMS) and Internal Control System (ICS)

4.1 RMS and ICS principles

The following five basic principles apply for the Volkswagen as the basis for dealing transparently and appropriately with risks.

I: Integrity, corporate values and compliance are especially important

The statutory regulations, voluntary commitments and internal company guidelines must be observed (compliance). The "Code of Conduct of the Volkswagen Group" is a binding guideline for everyday professional life, offers guidance, advice and support, and summarizes key basic principles. The "Code of Conduct of the Volkswagen Group" also reinforces the personal integrity of every individual. All conduct is based on a common fundamental ethical and moral attitude. This supports each individual based on own personal conviction and with responsibility for Volkswagen to do the right thing and openly address critical topics. A culture of integrity prevents misconduct. The topics of integrity, fairness and transparency are key to create credibility and trust in business practice.

II: Risks are to be dealt actively and openly

Company management, and all employees promote, encourage and practice an active and open risk culture. Risks are to be actively identified, managed and controlled within the existing responsibilities. Major risks that cannot be sufficiently mitigated within the existing responsibilities or in coordination with other affected divisions are to be communicated openly and promptly to the higher-level positions in the company and to IRC Manager.

III: The RMS/ and ICS is aligned to the goals

The RMS/ and ICS is to be designed in such a way that it is suitable to identify developments at an early stage that threaten the achievement of key company and divisional goals and the viability and observance of key company processes. It should also allow appropriate risk response measures to be taken to ensure that the goals can be achieved.

IV: Risks are to be taken deliberately and managed appropriately

Justifiable risks may be accepted to a reasonable extent if they enable opportunities to be seized, but they should be managed and controlled with appropriate risk response measures. Risks that pose a threat to the existence of the company are to be avoided. A risk that poses a threat to the existence of the company is one that threatens a situation of over-indebtedness or illiquidity.

V: The RMS and ICS must be effective

The specific design of the RMS/ and ICS for the Volkswagen brand and respective companies depends on the type, scope, complexity and level of risk of the actual business activity and environment (appropriateness) and is to be further developed regularly and monitored for its effectiveness.

4.2 The "Three Lines" approach for RMS and ICS

The RMS and ICS of Volkswagen Autoeuropa follows the Three Lines approach. Overall responsibility for an effective RMS and ICS in this approach lies with the management board. The departments form the First Line. The Integrity, Risk & Compliance department forms the Second Line for the RMS and ICS at Volkswagen Autoeuropa. There are also other units that perform Second Line tasks for their specific area of responsibility, e.g. Legal department and Group Compliance. The Third and final Line is formed the Group Audit department.

First Line

Risks are to be actively identified, evaluated, managed, controlled and documented appropriately within the respective responsibilities in the divisions. The divisions report on major risks according to the reporting lines.

Second Line

Within the context of the RMS and ICS, risk management (see section 5) sets standards, manages processes and assumes an advisory role. It manages the Quarterly Risk Process and the annual regular GRC process, for instance, and reports regularly to the management board concerning major risks and results.

Third Line

The Audit department takes an independent audit function on behalf of the board of management and reports to the board of management. The Audit department is the independent Third Line within the risk management system and responsible for the internal control structure as well for the management and monitoring processes.



Further details on the tasks of Group Audit are described in Group Policy 28 of Group Audit (ADM ADM-F-O090 - KRL_28_Revision_en_V1.0



Further explanations of the Three Lines model are described in Attachment 7 "The Volkswagen Three-Lines Model" of this Organizational Guideline

4.3 Framework in accordance with COSO ERM

The RMS and ICS at Volkswagen Autoeuropa is based on the internationally acknowledged enterprise risk management framework "COSO ERM" developed by the Committee of Sponsoring Organizations of the Treadway Commission¹. COSO ERM calls for implementation of the RMS and ICS across all organizational levels in Volkswagen Autoeuropa.

4.4 RMS and ICS elements

Basic elements are to be observed when implementing an appropriate and functioning RMS and ICS. For this purpose, appropriate implementation of RMS and ICS does not necessarily mean that all the basic elements described below must be implemented in all departments or for every process.

The overall implementation of all elements described must rather be ensured for the Volkswagen Autoeuropa. The participation on the RMS and ICS core processes as described in section 6 is obligatory for all departments within Volkswagen Autoeuropa. Any exception must be justified and approved by IRC Manager. This covers the basic elements, i.e. risk identification, risk analysis and evaluation and risk response as well as control activities. Moreover, departments may in their discretion identify, evaluate and manage further operational risks or set additional control activities and documentation requirements depending on type and complexity of the business environment and business activities (local RMS and ICS).

¹ COSO's 2013 "Internal Control- Integrated Framework" is a significant complementing element of the enterprise risk management framework and provides the primary framework for ICS.

Internal environment

The internal environment is the basis for a functioning RMS/ICS. The organizational and operational structure provides the organizational framework, the structure of which is to be properly documented in the internal rules and regulations (e.g. guidelines, process standards). The internal environment is shaped primarily by the company values, the codes of conduct and the risk culture.

Objective setting

The clear definition of targets for the department is the basis and starting point for identifying and assessing risks and deriving measures to respond to them. Specific targets for the departments are formulated on the basis of the corporate strategy, legal requirements and the value system through, for example, planning sessions and target agreement processes.

Risk identification

The aim of risk identification is to identify internal and external risks that jeopardize the achievement of company and divisional targets and the viability of business processes being the focus being on major risks. Materiality thresholds in the divisions and/or committees should be defined by the heads of the divisions with due regard for economic conditions, e.g. in the form of fixed escalation levels according to damage or score value. Strategic and operational risks are also to be included in the risk identification process along with reporting, compliance, fraud, environmental and human rights risks.

Risk assessment

Identified risks are to be assessed in terms of their probability of occurrence or relevance and impact. This calls for a meaningful description of the risk including an indication of its cause and consequences. An analysis and evaluation of risks and, where applicable, a comprehensive description (e.g. rankings, risk matrix, risk complexes) permits a basic appraisal of the overall extent of the risk to be made.

Risk response

An appropriate risk response strategy is to be defined for major risks. This can mean avoiding, transferring, mitigating or accepting risks.

A clear assignment of responsibility for the risk response measures is extremely important. Likewise, the exact object of the risk response measure and the timeframe or frequency of implementation of the risk response measure is to be determined. It is always important to ensure that the chosen risk response measure is designed in such a way that is also actually suitable for implementing the chosen risk response strategy.

Risk response measures in connection with relevant time-critical business processes are to be designed in such a way that the interrupted processes can be continued at a predefined minimum level (business continuity) as quickly as possible and as planned.

Control activities

Control activities must be carried out either at management or process/transaction level and properly documented. The management level is responsible for the control activities. The control activities serve to safeguard business activities, to ensure the truth and fairness of internal and external accounting, to ensure observance of all legal regulations that apply to the company, and to check conformity with strategies.

Information and communication

A crucial success factor for ensuring the effectiveness of an RMS and ICS is adequate and timely information on major

risks, risks that pose a threat to the continued existence of the company, missing risk response measures, and identified control weaknesses.

Among other things, regular reporting can include results (including a description of the effectiveness) of RMS and ICS processes, status reports with regard to the implementation of follow-up measures and/or lists of the implementation progress for projects. Regardless of this, notifications of urgency must be issued on an ad-hoc basis.

Monitoring

The objective of monitoring is to ensure the effectiveness (appropriateness and viability) of the RMS/ and ICS. Monitoring can be carried out through process-integrated and/or process-independent activities. Weaknesses discovered in the RMS/ and ICS are to be corrected promptly; major weaknesses are to be communicated to the relevant committee and/or to the management board.

5 Tasks, authorities and responsibilities (TAR)

5.1 Volkswagen Autoeuropa Board of Management

The Volkswagen Autoeuropa Board of Management is responsible for implementation, operation and further development of an appropriate, functioning and documented RMS, ICS and BCM. To this end, the Board of Management must ensure within its area of responsibility that there is harmony between applicable legislation, internal regulations and organizational instructions, taking into account the basic principles of the RMS/ICS (see section 4). BoM receives regular reports on major risks and how they are being managed as well on the effectiveness of the RMS and ICS.

The Board of Management is responsible for specifying the guidelines, processes and measures required for this and for issuing suitable instructions. The Board of Management also ensures compliance with these specifications and that their effectiveness is regularly reviewed. The Board of Management delegates the activities described in section 5.3 to Integrity, Risk & Compliance Manager. For delegation purposes, it is necessary to ensure that employees performing RMS and ICS tasks are sufficiently qualified and have access to the necessary information and that risk organizational resources are available in the requisite quality and quantity.

5.2 Departments (first line)

The departments within Volkswagen Autoeuropa must implement and execute appropriate measures for their business activities and processes to actively identify, manage and control risks, taking into account the specifications of Volkswagen Autoeuropa Board of Management as well as Volkswagen Brand Board of Management.

In addition to the Group-wide core processes, this also applies to local RMS and ICS, although the extent of formal structuring lies within the discretion of those responsible for the department. Guidance on this is provided by the principles and elements of RMS and ICS outlined in sections 4.1 and 4.4. Clear responsibilities for major risks are to be determined by the departments, particularly risk owner, person responsible for the risk and person recording the risk (see other applicable documents in attachment 2) for the major risks.

The departments must actively participate in the Group-wide RMS and ICS processes (see section 6) and work together with Integrity, Risk & Compliance department (Second Line). To this end, the departments name risk coordinators as an interface with the second line (see attachment 1 on the tasks, authorities and responsibilities of risk coordinators). Major risks must be reported openly and promptly to the higher-level bodies within Volkswagen Autoeuropa and within Group Volkswagen in accordance with reporting thresholds in the Quarterly Risk Process.

It must be ensured that all employees with tasks within the RMS, ICS or BCM are technically qualified for the RMS, ICS, BCM respectively and have sufficient experience in their respective field of expertise. As well those that fulfills the

tasks for RMS, ICS, BCM respectively must have the necessary skills and resources and have access to the necessary information. The requirements with regard to the roles within the Risk Management processes are specified in the Attachment 5 (requirements for Regular GRC process) and Attachment 6 (requirements Quarterly Risk Process).

Notification of urgency

The department managers inform the responsible Board Member of Volkswagen Autoeuropa and if necessary the responsible member in the Brand Board of Management of any risks threatening the going-concern status without delay and in a readily understandable manner - notification of urgency-. Risks threatening the going-concern status particularly include matters involving a heightened risk exposure, accounting errors and breaches of statutory provisions liable to materially affect Volkswagen Autoeuropa assets, financial position and earnings. In addition, a notification of urgency is compulsory if a risk materially impacting earnings is likely to occur within the next 24 months despite the risk management measures taken. The thresholds and addressees for notifications of urgency are set out in the applicable documents (attachment 3). Although the notification of urgency is submitted outside the normal reporting processes, must subsequently be included in the established risk management processes with minimum delay so that all relevant units are informed in this process.

5.3 Integrity, Risk & Compliance department (Second Line)

Integrity, Risk & Compliance department as a part of the second line supports the Board of Directors of Volkswagen Autoeuropa in establishing, operating and further developing an effective RMS and ICS within the company. The tasks, authorities and responsibilities of Integrity, Risk & Compliance department include among others (specified in Group Policy 33) defining and further developing suitable and appropriate minimum standards for the RMS and ICS (including BCM), providing, managing and monitoring the Group-wide risk management processes and preparing regular and, if necessary, event-related reports on major risks, the status of risk response measures and control activities as well as weaknesses to the Volkswagen Autoeuropa Board of Directors, Investment Committee and other relevant committees. For disciplinary and operational purposes, Integrity, Risk & Compliance reports to the Chairman of the Board of Directors of Volkswagen Autoeuropa.

Integrity, Risk & Compliance department is tasked with supporting the departments (first line) in the early identification, assessment and management of risks in line with their responsibilities.

For the performance of these tasks, Volkswagen Autoeuropa Board of Management has appointed the Integrity, Risk & Compliance Manager (see annex 8: TAR plus Local Risk Officer of SQ-ADF-F-0018_KRL 31 – Organization of governance functions – Integrity, Risk Management, Compliance and Legal (IRC+L).

5.4 Group Audit (third line)

Group Audit supports the organization to achieve its goals by assessing and improving the effectiveness of risk management, management and monitoring processes through a systematic, focused and risk-based approach. The Group Audit activity covers all business areas and processes (including outsourced activities). Within the scope of its activities, Internal Audit checks the organizational and operational structures and the related processes of the Risk Managements on group, brand and entity level. Please see the Group Policy 28 of Group Audit for further details on tasks on Group Audit.



Further details on the tasks of Group Audit are described in the document ADM-F-0090-GP_28_Revision_en_V1.0 available in Quality Management system

6 RMS and ICS core processes

In addition to the required measures for actively identifying, managing and monitoring risks in the departments (First Line), standardized processes for the RMS and ICS are to be implemented at Volkswagen Autoeuropa.

6.1 Quarterly Risk Process (QRP)

For the purpose of early risk recognition and monitoring of measures, the Quarterly Risk Process (QRP) identifies, records, assesses and reports acute risks, particularly those impairing the achievement of strategic, derived operating goals and goals relevant to reporting and compliance.

Strategic risks entail possible future developments or events which are liable to cause a negative deviation from Volkswagen Autoeuropa **strategic goals**.

Operating risks entail possible future developments or events that are liable to cause a negative deviation from the **operating goals** derived from Volkswagen Autoeuropa strategic goals with respect to business performance or productive processes.

The process incorporates all departments of Volkswagen Autoeuropa. The risk assessments are to be closely coordinated with Controlling and Accounting in order to share any information for necessary provisions and update the budget planning and forecast processes.

Key process steps of the Quarterly Risk Process

Acute risks are recorded quarterly. This entails identifying, describing and assessing risks and managing them by taking countermeasures.

In this regard, the top risks are determined by Board of Directors and Integrity, Risk & Compliance department at Volkswagen Autoeuropa.

The departments are responsible for identifying, assessing and reporting the risks. Risks are evaluated by means of a risk scoring system consisting of the following four elements:

Probability of occurrence

Financial loss

Reputational damage

Potential threat to compliance with external legal requirements

In this way, the risk score takes account of both quantitative and qualitative elements. The process also includes a plausibility check of selected risks.

The risks reported are incorporated into the corresponding quarterly risk reports. The reports are presented and approved by Board of Directors at Volkswagen Autoeuropa. After it has been approved, the quarterly risk report is forwarded to the Brand Risk Management.

6.2 Standard Internal Control System (Standard ICS)

The Standard ICS defines Group-wide minimum requirements for the internal control system with regard to major process risks. Furthermore, the ICS standard clearly assigns responsibilities for process risks and controls for essential processes in the company. Required efficacy tests are carried out and evaluated in a standardized form and process weaknesses are remedied.

This process will be implemented at Volkswagen Autoeuropa by way of the rollout (wave 3), defined by Group Risk

Management.

Key process steps of the Standard ICS

The standard ICS consists of the process steps preparation and recording, release recording, testing, release testing, reporting and MCC (Master Control Catalogue) update. These steps are supplemented by higher-level scoping, process-independent monitoring and vulnerability correction.

In scoping, the **Group Risk Management** defines which companies participate in the standard ICS.

The asset-user MCC inventory (AUM inventory) is used to prepare for the capture phase. By means of the AUM inventory, the organizational and responsibility structure, the MCC assignment as well as the relevance of process risks in the areas are defined.

In the areas, existing controls are updated and new controls are recorded and **released** by the managers responsible for the process at the end of the **registration phase**.

With the completion of the acquisition phase, the **testing** starts in the areas. The test-relevant controls are checked. In the event of ineffective controls, the procedural weaknesses with regard to their extent of damage are assessed in accordance with the criteria defined by the Group Risk Management and substantiated with measures.

The proof of efficacy is **released** by the process-responsible managers after completion of the testing.

The responsible **Risk management** checks the quality of the test results in accordance with the **plausibility check concepts** defined by Group Risk Management.

After successful completion of the test phase, the responsible **risk management** will report to the relevant brand and group committees.

The weaknesses identified in the **testing** must be remedied by the areas within the defined implementation period by means of relevant measures.

In the **MCC-update phase**, responsible departmental experts update the MCCs using Group Risk Management. The updated MCCs are made available to the brands by Group Risk Management for the preparation of the regular process in the following year.



The Regular GRC process will be replaced by the standard ICS by way of the rollout (wave 3), defined by Group Risk Management.

6.3 Regular Governance, Risk and Compliance (GRC) process

The regular GRC process records and assesses major systemic risks including counter-measures and management controls and determines whether they are being managed effectively in order to monitor the effectiveness of enterprise-wide RMS and ICS.

Key process steps of the regular GRC process

The annual GRC process is divided into five key process steps which follow one in another in a cyclical pattern.

The purpose of scoping is to identify the Business Units of Volkswagen Autoeuropa to be included in the regular GRC process (hereinafter referred to as "units"). The units record and assess the relevant risks, risk management measures

and management controls. During the confirmation of effectiveness phase, the effectiveness of the risk control measures and management controls to be assessed is reviewed. The responsible management of the respective unit defines and implements measures to address the weaknesses identified in the confirmation of effectiveness phase. From the risks reported, the major risks and weaknesses are identified and part of the reporting to the Board of Directors of Volkswagen Autoeuropa.

6.4 Business Continuity Management (BCM)

BCM prepares the company on a structured and systematic basis for any disruptions to business as part of operational risk management. The measures for limit possible consequences of failures are aimed at essential and time-critical business processes, strengthen the resilience of the company and thus secure the strategic and derived operational corporate and business unit goals in addition to preventive risk management.

Key process steps of the Business Continuity Management

As part of the rollout of BCM, the principles underlying operational implementation are being defined, communicated and prepared. During the operational implementation, relevant business processes will be identified in a business impact analysis (BIA) and the possible consequence of their interruption evaluated. For the identified time-critical business processes, solutions for various failure scenarios will be developed and submitted to the responsible management for a decision. The approved solutions will then be recorded in a business continuity plan and subsequently tested.

The BCM process steps are performed cyclically by the departments. As part of the continuous improvement process, this BCM cycle is monitored and maintained by Integrity, Risk & Compliance department.

6.5 Root Cause Analysis Process (RCA) and Lessons Learned (LL) Process

In addition to avoid risks, it is in the interest of Volkswagen Group to learn from the risks occurred. The aim is, if possible, to avoid reoccurrence of the risk or to reduce the likelihood of occurrence or its effects appropriately. A systemic Root Cause Analysis and a systematic Lessons Learned process contribute to this. Minimum requirements for the RCA process and for the creation and communication of LL are presented in attachment 4.

7 Responsibility and procurement of insurance

As part of a holistic risk management system all brands and companies must use Volkswagen Insurance Brokers GmbH (VIB) for the risk transfer to insurance companies unless otherwise specified in the internal document "SQ-DF-G-O160 – Responsibility and purchasing of insurance". VIB procures and manages insurances for the Volkswagen Group thus ensuring a uniform risk transfer optimized under a cost and risk perspective. Details of VIB's processes and responsibilities are set out in internal document "SQ-DF-G-O160 – Responsibility and purchasing of insurance".



Further details on the responsibilities and procurement of insurance are described in the document SQ-DF-G-O160 – "Responsibility and procurement of insurance", available in Quality Management system

8 Risk assessment

The organizational instruction supports the Board of Directors of Volkswagen Autoeuropa in implementing the "Group Policy 33 - Risk Management System and Internal Control System within the Volkswagen Group". Improper

implementation of this organizational instruction may result in a lack of transparency regarding the risk situation, the risk response measures and the effectiveness of the RMS/ICS, which may lead to significant legal or financial risks and/or risks to reputation. In order to reduce these risks, internal control activities are implemented to ensure the accuracy of analyses or reporting as well as the timely implementation or execution of processes or projects.

Board of Directors of Volkswagen Autoeuropa

Thomas Hegel Gunther
(Plant Manager)

Marko Sebastian
(Finance and IT Director)

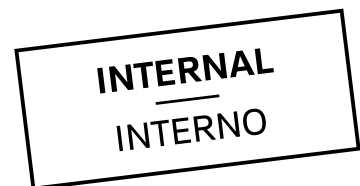
Dieter Neuhaeuser
(Human Resources & Organization
Director)



Attachment 1: Tasks, powers and responsibilities of the Risk Coordinator

Valid from:	03.12.2019
Last Change:	02.05.2022
Replaces the:	
Verification of validity:	31.12.2024
Responsible department for the process:	Integrity, Risk & Compliance - AGC
Name:	Integrity, Risk & Compliance Manager (Adélia Felício)
Telephone:	+351212112732
Issuing department:	Integrity, Risk & Compliance – AGC
Name:	Integrity, Risk & Compliance Manager (Adélia Felício)
Telephone:	+351212112732

Tasks, powers and responsibilities of the Risk Coordinator



1. Tasks, authorities and responsibilities of the Risk Coordinator

The tasks, authorities and responsibilities of the Risk Coordinator appointed at the level of the departments (first line) include:

1.1 Tasks:

- Manage the flow of the risk management and internal control system processes within the area of responsibility, as well as support the supervised departments to ensure the effectiveness of local control activities and monitoring the implementation progress of the risk management measures in order to fully meet the requirements of ORL 53.

1.2 Authorities:

- Management of RMS core processes (including BCM) and ICS in the department.
- Approval of plausibility checked results from the RMS core processes (including BCM) and ICS issuing reports to the Board of Directors and to the responsible risk management.

1.3 Responsibilities:

Ensuring prompt, appropriate and comprehensive reporting on RMS (including BCM where applicable) and ICS to the responsible member of the Board of Directors and responsible Risk Management.

The above-called tasks, competencies and responsibilities are to be included in the corresponding job descriptions according to the local organizational standards.



Attachment 2: Other applicable documents

Valid from:	03.12.2019
Last Change:	02.05.2022
Replaces the:	
Verification of validity:	31.12.2024
Responsible department for the process:	Integrity, Risk & Compliance - AGC
Name:	Integrity, Risk & Compliance Manager (Adélia Felício)
Telephone:	+351212112732
Issuing department:	Integrity, Risk & Compliance – AGC
Name:	Integrity, Risk & Compliance Manager (Adélia Felício)
Telephone:	+351212112732

Other applicable documents



Other documents that apply alongside SQ-ADF-F-O090:

- ADM-F-O101 Methodology manual for the regular GRC process
- SQ-ADF-F-O017 Methodology Manual QRP
- SQ-ADF-F-S103__Notification of Urgency
- SQ-ADF-F-O006 - Business Continuity Management (BCM)_ Group minimum requirements
- SQ-ADF-F-O004 Handbook for Root Cause Analysis (RCA)
- SQ-ADF-F-S060 _Delegação para a realização de análise da causa raiz
- ADF-F-S140 _Root Cause Analysis (RCA) - Reporting Template
- SQ-ADF-F-P020 _ Gestão de risco - processo de análise da causa raiz

Further documents:

The Risk Wiki contains further documents (e.g. training documents) that provide supplementary support for implementing the risk management processes in the departments.



Link to Risk Wiki: <https://group-wiki.wob.vw.vwg/wikis/display/RISKWIKI>



Attachment 3: Notification of urgency

Valid from:	03.12.2019
Last Change:	02.05.2022
Replaces the:	
Verification of validity:	31.12.2024
Responsible department for the process:	Integrity, Risk & Compliance - AGC
Name:	Integrity, Risk & Compliance Manager (Adélia Felício)
Telephone:	+351212112732
Issuing department:	Integrity, Risk & Compliance – AGC
Name:	Integrity, Risk & Compliance Manager (Adélia Felício)
Telephone:	+351212112732

Notification of urgency



1. Notification of urgency

The urgent notification ensures that the respective member of Board of Directors is informed immediately in the event of risks endangering the existence of the company and/or exceeding specified threshold values.

Although the notification of urgency is submitted outside the normal reporting processes, it must be subsequently included in the established risk management processes with minimum delay.

An urgent notification to the respective member of Board of Directors is mandatory if, despite the control measures taken, the probability of the risk occurring in the next 24 months is above 50% (urgent notification) and a negative effect on earnings in accordance with the following reporting thresholds is to be expected. In addition to new risks, this also applies to existing risks that meet the criteria of an urgent notification due to significant changes.

The following thresholds apply to such notification:

- Board of Management members of Volkswagen AG: €1,000 million
- Volkswagen Passenger Cars Brand Board of Management members: €500 million
- Volkswagen Autoeuropa Board of Management members: €5 million



For the urgent notification is applicable the standard template SQ-ADF-F-S103 - "Notification of Urgency" available in Quality Management system.
For any questions, you can contact: Integrity, Risk & Compliance Manager (Adélia Felício).



Attachment 4: Root Cause Analysis and Lessons Learned

Valid from:	03.12.2019
Last Change:	02.05.2022
Replaces the:	
Verification of validity:	31.12.2024
Responsible department for the process:	Integrity, Risk & Compliance - AGC
Name:	Integrity, Risk & Compliance Manager (Adélia Felício)
Telephone:	+351212112732
Issuing department:	Integrity, Risk & Compliance – AGC
Name:	Integrity, Risk & Compliance Manager (Adélia Felício)
Telephone:	+351212112732

Root Cause Analysis and Lessons Learned



Root Cause Analysis and Lessons Learned

1. Terms and definitions

Problem: Confirmed negative deviation between actual status and target status.

Major problem (as trigger): A major problem exists when

- a finding by Internal Audit (as 3rd Line) leads to a red traffic light (trigger 1) and/or
- a serious regulatory violation (according to KRL 3) results in a disciplinary action (trigger 2) and/or
- there is a significant financial loss or damage to the reputation of the respective brand/entity (trigger 3) and/or
- the Group Board Committee for Risk Management (K-VAR) commissions a department to conduct a RCA for a specific topic (trigger 4)

Root cause analysis (RCA): A RCA is a structured examination aimed at identifying the root cause(s) of a problem and measures for remedying that problem.

Root cause: A root cause is the origin of a problem. The identification of a root cause(s) is expressly not confined to technical causes and their immediate remedial measures. Rather, the aim in identifying root cause(s) is to analyze case-dependent which cultural, processual and structural factors have led or contributed to the problem.

Lessons learned: Valuable insights/experience gained from a process or project.

Best practices: Procedures that are correct and/or recognized as most effective and/or prescribed.

Regulatory violation: A regulatory violation is defined as non-compliance with laws, internal and external regulations and voluntary commitments.

2. Roles and responsibilities

The following roles and responsibilities apply within the Volkswagen Group as part of the RCA and lessons learned analysis.

1. **First line (working on trigger 2, 3, 4)**: Organizational Unit (OU) (OU in which a major problem has occurred)

- Performance and documentation of RCA for processual, structural and cultural problems with standardized reporting template
- Elimination of problems in the own field of responsibility by defining and executing reasonable measures
- Provide lessons learned proposals based on RCA results that can be used on Group level to define lessons learned, if possible
- Reporting the results of RCAs to the directly responsible Risk Management
- Implementation of the communicated lessons learned and best practices, according to the professional responsibility
- Identification of problems within own field of responsibility in case of voluntary RCAs below the threshold of major problems

2. **Second line** :

Group Risk Management (K-IR)

- Content design of the processes and maintenance of the regulations for RCAs and lessons learned

analyses on Group level in the event of major problems

- Provide event-related trainings and consultation for RCAs on Group level
- Identification and evaluation of major problems on Group level with the inclusion of process partners in case of a significant financial loss or damage to the reputation (trigger 3) based on Controlling reports and reports of materialized risks
- Tracking and monitoring of ongoing and finalized RCAs on Group level (except for trigger 1)
- Perform a plausibility check for RCAs on Group level (except for trigger 1)
- Tracking and monitoring of mitigating actions defined on Group level (except for trigger 1)
- Forwarding the RCA decisions by K-VAR (trigger 4) to the responsible Brand Risk Management
- Central collection of results from RCAs for major problems
- Clustering of the results from the RCAs into useful subject areas and providing information to the responsible Group units for further derivation of lessons learned
- Supporting the Group functions in their task to identify lessons learned and best practices, if necessary
- Forwarding insights from RCAs, meaning lessons learned and, if necessary, best practices to the Risk Managements on brand/entity level
- Monitoring the communication of identified lessons learned and best practices at brands/entities

Brand/Entity Risk Management

- Content design of the processes and maintenance of the regulations for RCAs and lessons learned analyses in the event of major problems. Local Risk Management can be involved in the design as necessary
- Identification and evaluation of major problems on brand/entity level with the inclusion of process partners in case of a significant financial loss or damage to the reputation (trigger 3) based on Controlling reports and reports of materialized risks (recommended for brand level)
- Provide event-related trainings and consultation for RCAs on brand/entity level
- Tracking and monitoring of ongoing and finalized RCAs on brand/entity level (except for trigger 1)
- Perform a plausibility check for RCAs on brand/entity level (except for trigger 1)
- Provide lessons learned proposals based on RCA results on brand/entity level that can be used on Group level to define lessons learned, if possible
- Reporting the results of RCAs to next higher level of Risk Management
- Tracking and monitoring of mitigating actions within brand/entity (except for trigger 1)
- Supporting the Group functions in their task to identify lessons learned and best practices, if necessary as well as the dissemination of these information within the brand/entity
- Communication of identified lessons learned and best practices, if relevant, towards business units as well as tracking of implementation

Group business units (e.g. Group quality)

- Performance of lessons learned analyses and, if necessary the identification of best practices for occurred major problems based on performed RCAs
- Lessons learned analyses and, if necessary best practices are reported to Group Risk Management

Compliance

- For trigger 2, informing the RCA responsible about the necessity to conduct a RCA (depending on coordinated approach between Investigation Office and Human Resources)
- For trigger 2, support the RCA-responsible during the completion of the RCA to ensure availability of relevant information and independence

- Group Compliance (K-IC) regularly provides an overview of sanctioned serious regulatory violations to Group Risk Management to support the Risk Management's task to track and monitor ongoing RCAs for trigger 2
- Incorporate results from RCAs in Compliance trainings, if reasonable

Human Resources

- For trigger 2, informing the RCA responsible about the necessity to conduct a RCA (depending on coordinated approach between Investigation Office and Human Resources).

3. Third line (working on trigger 1): Internal Audit

- Content design of the Internal Audit-specific processes and maintenance of the regulations for RCA for trigger 1
- Identification of major problems during audits as part of the third line function (trigger 1)
- Create and provide trainings as well as consultation for RCAs specifically for Internal Auditors
- Performance of RCAs for processual, structural and cultural problems that are identified during audits (trigger 1)
- Documentation of RCAs with standardized reporting template
- Perform a plausibility check for RCAs conducted by Internal Audit based on a four-eye principle
- Forwarding the final results from RCAs to the responsible Risk Management
- Tracking and monitoring of ongoing and finalized RCAs for trigger 1
- Tracking and monitoring of mitigating actions for trigger 1
- Supporting the Group functions in their task to identify lessons learned and best practices, if necessary
- Implicitly including results of RCAs in the input parameters for the audit program planning.

3. Identification of major problems and performance of root cause analyses

The starting point for a RCA is the identification of a major problem. The identification of major problems depends on the specific trigger:

Trigger 1: Internal Audit finding with high criticality

When a finding during an audit by Internal Audit leads to a red traffic light, Internal Audit will conduct a RCA. Internal Audit is responsible for the identification of the trigger 1 and for the conduction of the respective RCA.

Trigger 2: Serious regulatory violation (SRV)

In case of a confirmed SRV pursuant to Group Policy 3 that leads to a disciplinary measure, the CEO of the respective entity conducts a RCA and bears the responsibility for the analysis.

With the imposition of personnel measures, the CEO of the respective entity (in case of affected member of top management circle the supervisory body) will be asked via email to perform a RCA. The initiation of the RCA takes place in coordination between the responsible Investigation Offices and Human Resources. The CEO will be advised that the responsible Compliance Officer of the respective entity supports during the completion of the RCA – in particular by clarifying questions about the circumstances and by critically assessing the independence of the RCA responsible. In exceptional cases, namely if the protection of the Whistleblower or the implicated person could not be guaranteed or a potential conflict of interest of the specific Compliance Officer would interfere with the completion of the RCA, the RCA is supported by the relevant DCO/RCO (Divisional/Regional Compliance Officer), or an appointed member of its team respectively (e.g. the Chief Compliance Officer of the concerned controlling brand entity). A conflict of interest may be identified during case procession by the respective case handler or the respective investigating unit.

The CEO of the respective entity shall involve the responsible Compliance Officer, the head of the respective department and/or another second line function of the respective entity to support with the completion of the RCA. If a disciplinary sanction was imposed on a member of the Board of Management or Managing Director of a Group company, if he is a member of the top management or higher, the supervisory body performs the RCA with the support of Konzern Personal Top Management (K-GT). The supervisory body can also decide to assign the performance of the RCA to the CEO or the head of department (upper management level) while the responsibility remains with the supervisory body.

In case local circumstances request certain adjustments to the approach, they need to be aligned together with Group Compliance, Group Risk Management and Brand Risk Management.

Trigger 3: Major “financial loss“ and or “damage to reputation”

Problems with considerable financial losses or damage to reputation can also require a RCA.

The thresholds for significant “financial loss” or “damage to reputation” are set by the Group Executive Board Risk Management Committee (K-VAR). The thresholds are currently defined as followed:

- **Major financial loss:** at least 100 Mio. EUR net operating profit (detailed criteria on Risk Wiki)
- **Major reputational damage:** international loss of reputation (in line with the highest level of the Quarterly Risk Process, detailed criteria on Risk Wiki)

Brand Risk Management is responsible for the identification of the trigger 3 based on controlling reports (for financial damages) and reported materialized risks (for reputational damages). In addition, Brand Risk Management identifies a suitable OU to conduct the RCA. The defined OU is responsible for the conduction of the RCA.

Trigger 4: Mandate by Group Executive Board Risk Management Committee (K-VAR)

The K-VAR can discuss identified problems and may come to the conclusion that a RCA can help to better understand the issue. For example, identified cultural deficiencies that might not reach the thresholds for trigger 1, 2 or 3 can still be defined as RCA-relevant by the K-VAR. The committee can define a brand/entity or OU that is responsible to conduct a RCA for this specific identified problem. Group Risk Management informs the responsible Brand/Entity Risk Management and they inform the responsible OU.

Each regular member of the K-VAR is responsible for the identification of the trigger 4 in her/his field of responsibility as well as the identification of a suitable OU to conduct the RCA. The defined OU is responsible for the conduction of the RCA.

Additional Trigger: Voluntary RCAs

In addition, any OU has the possibility to conduct a RCA even below the thresholds for mandatory triggers. The decision to conduct a RCA for an identified problem lies with the head of the OU. In particular, the following aspects can be considered during the decision-making process:

- Has the problem a Group-wide effect even if it does not reach the threshold for major problems?
- Can a voluntary RCA lead to a sustainable improvement regarding structure, culture or processes?

Prioritizations in case of more than one RCA processes or trigger are in place

If a problem identified in the context of any RCA in the company (e.g. RCA on environmental audits) corresponds to at least one of the four triggers for a major problem in accordance with this KRL, a RCA must be carried out for this problem in accordance with the procedure listed within this KRL. For these specific cases, the RCA responsible has

to decide if she/he continues the RCA based on her/his requirements besides following the KRL 33 process.

4. Local measures resulting from root cause analyses

Based on the conducted RCAs, local measures must be defined and followed up by the responsible OUs in order to prevent the recurrence of the major problem in their own field of responsibility. In addition to immediate measures to remedy the concrete, existing major problem, the OU must also define and implement higher-level measures involving relevant partners that go beyond the technical solution, if required (e.g. departmental culture, Code of Conduct). Here, multiple measures that complement one another sensibly should be considered. Brand/Entity Risk Management will track and monitor the mitigating actions for trigger 2, 3, 4 and voluntary RCAs (if informed by OU). In case of trigger 1, Internal Audit will define the mitigating actions and track and monitor the mitigating actions.

5. Documentation and further processing of results from root cause analyses

After a RCA has been performed, its results need to be documented in a standardized reporting template and reported to the responsible Brand/Entity Risk Management.

A plausibility check will be performed by Risk Management based on standardized criteria for trigger 2, 3, 4 and voluntary RCAs (if informed by OU). In case of trigger 1, Internal Audit performs the plausibility check on their own before reporting the final reporting template to Risk Management. Final results have to be reported from local Risk Management to Group Risk Management. Group Risk Management functions as a central point of collection for the results of root cause analyses in the Group and clusters these information into meaningful topic areas.

Identified topic areas from RCAs will be sent from Group Risk Management to the responsible Group business units for further assessment. The Group business unit decides together with the affected OUs of the brand/entity whether a lessons learned analysis and the elaboration of best practices should be undertaken and which responsibilities the respective parties will bear for these specific tasks. In this process step, both Group Risk Management and the local Risk Management on brand and entity level shall be involved in the identification of lessons learned and best practices when this is a helpful addition to the topic (i.e. define lessons learned proposals). The results of the lessons learned analysis and the elaborated best practices are communicated by the Group business units to Group Risk Management.

Group Risk Management checks the plausibility and documents the obtained results.

When disseminating lessons learned and best practices, Group Risk Management decides which communication measures are sufficient on the basis of the relevant stakeholder groups and the content to be communicated.

Communication on lessons learned take place on a regular basis, e.g. quarterly. The information can be communicated, for example, via online portal/intranet or e-mail. Alternatively, results of the lessons learned analysis can be communicated by the Group business unit directly to the affected OUs. Communication can be immediate in cases of particular urgency. If reasonable, relevant information from lessons learned is provided additionally as part of compliance training.

6. Method of defining root causes

In order to document the RCA, the use of a standardized reporting template is mandatory. To conduct the RCA, the "5 Why Method" is used. Here, the repetition of the question "Why?" clearly identifies the cause of the problem. Case-specific, multiple root causes might be identified for one problem. Because a problem can have diverse

reasons, it is important to consider and identify potential deficiencies in the areas of culture, structure and processes. If helpful, multiple sources and OUs can be involved to achieve optimal results.

7. Timing parameters of Root Cause Analyses and Lessons Learned

In case of trigger 1, Internal Audit includes the RCA as part of the audit time frame of 120 days. For trigger 2, 3, 4, the duration of a RCA is defined as a 4 week period starting after the training was executed. Lessons Learned from RCAs are derived on a quarterly basis.

In case there is the necessity to prolong the above mentioned timing parameters for a specific case (i.e. due to high complexity of problem), a longer period can be defined and documented together with Risk Management.

A detailed timeline for the RCA and lessons learned steps is available on Risk Wiki.

8. Access to relevant documents and supporting information

The Risk Wiki contains further documents that provide supplementary support for implementing the Root Cause Analysis and Lessons Learned process in the departments.



Link to Risk Wiki: <https://group-wiki.wob.vw.vwg/wikis/display/RISKWIKI>



For the Root Cause Analysis and Lessons Learned process is applicable the standard template "SQ- ADF-F-S140 _Root Cause Analysis (RCA) - Reporting Template" available in Quality Management system.



Attachment 5: Requirements for regular GRC-process

Valid from:	03.12.2019
Last Change:	02.05.2022
Replaces the:	
Verification of validity:	31.12.2024
Responsible department for the process:	Integrity, Risk & Compliance - AGC
Name:	Integrity, Risk & Compliance Manager (Adélia Felício)
Telephone:	+351212112732
Issuing department:	Integrity, Risk & Compliance – AGC
Name:	Integrity, Risk & Compliance Manager (Adélia Felício)
Telephone:	+351212112732

Requirements for regular GRC-process



1. Roles in the Regular GRC Process

1.1. Risk Recorder

Role:	Risk Recorder
Expected level:	Employee
Responsibility:	Responsible for technical incl. evaluation of all relevant risks in RICORS
Tasks:	<ul style="list-style-type: none"> • Identification of risks (in collaboration with owners/responsibles) • Technical recording incl. evaluation of all relevant risks in RICORS • Coordination of risks (outside RICORS) with the risk responsible • Documentation of the approval after reconciliation with the risk responsible and/ or the risk owner
Relevant skills	
Method skills:	<ul style="list-style-type: none"> • Knowledge about the methods of the GRC process with regards to identification and evaluation • Understand of the GRC process (Recording phase) incl. Roles & Responsibilities • Risk identification methods
Technical skills:	<ul style="list-style-type: none"> • Handling of RICORS (Recording Phase)
Relevant trainings:	<ul style="list-style-type: none"> • Basic Training for New Risk Recorders • Refresher Training for Existing Risk Recorders
Qualification and experience:	<ul style="list-style-type: none"> • In general a minimum of 1 year experience within the relevant business process (internally or externally)
Soft skills:	<ul style="list-style-type: none"> • Communication skills • Planning and moderation of workshops

1.2. Risk Responsible

Role:	Risk Responsible
Expected level:	MK/OMK
Responsibility:	Responsible for identifying the major individual risks, ensuring their completeness and the comprehensible description and assessment of all recorded risks in the area of responsibility
Tasks:	<ul style="list-style-type: none"> • Identification of risks and information to the Risk Recorder • Identification of the major individual risks, ensuring completeness and the comprehensible description and assessment of all recorded risks in the area of responsibility • Qualification of the persons involved in the process in the area of responsibility • Management and control of the (individual) risks in the area of responsibility • Reconciliation of risks (outside RICORS) with Risk Owner
Relevant skills	
Method skills:	<ul style="list-style-type: none"> • Understanding of process, roles and responsibilities
Technical skills:	<ul style="list-style-type: none"> • N/A
Relevant trainings:	<ul style="list-style-type: none"> • Training for Risk Owner & Risk Responsible
Qualification and experience:	<ul style="list-style-type: none"> • In general a minimum of 3 years experience within the relevant business process (internally or externally) or similar expertise. • The Risk Responsible should have: <ul style="list-style-type: none"> - Knowledge of the local processes - Knowledge about the business and the local situation
Soft skills:	<ul style="list-style-type: none"> • Critical thinking;

1.3. Risk Owner

Role:	Risk Owner
Expected level:	TMK/OMK
Responsibility:	Overall responsible for the management of risks (identifying, evaluation, monitoring) in the area of responsibility and responsible for quality assurance of the results from the GRC effectiveness process
Tasks:	<ul style="list-style-type: none"> • Identification of risks and information to the Risk Recorder • Qualification of the persons involved in the process • Monitoring the risk situation in the area of responsibility • Confirmation of risk recording and risk assessment in the area of responsibility
Relevant skills	
Method skills:	<ul style="list-style-type: none"> • Understanding of process, roles and responsibilities
Technical skills:	<ul style="list-style-type: none"> • N/A
Relevant trainings:	<ul style="list-style-type: none"> • Training for Risk Owner & Risk Responsible
Qualification and experience:	<ul style="list-style-type: none"> • In general a minimum of 3 years experience within the relevant business process (internally or externally) or similar expertise. • The Risk Responsible should have: <ul style="list-style-type: none"> - An overview of the local processes - Knowledge about the business and the local situation
Soft skills:	<ul style="list-style-type: none"> • Critical thinking;

1.4. Control Responsible

Role:	Control Responsible
Expected level:	MK/OMK
Responsibility:	Operationally responsible for the execution of the management control in the business unit
Tasks:	<ul style="list-style-type: none"> • Determination of follow-up measures incl. date and responsibility for implementation • Receipt the ICS report from Test Responsible or Division GRC and evaluation
Relevant skills	
Method skills:	<ul style="list-style-type: none"> • Understanding of process, roles and responsibilities • Methodology on confirmation of effectiveness phase
Technical skills:	<ul style="list-style-type: none"> • N/A
Relevant trainings:	<ul style="list-style-type: none"> • Training for Control Owner & Control Responsible
Qualification and experience:	<ul style="list-style-type: none"> • In general a minimum of 3 years experience within the relevant business process (internally or externally) or similar expertise.
Soft skills:	<ul style="list-style-type: none"> • Critical thinking;

1.5. Control Owner

Role:	Control Owner
Expected level:	TMK/OMK
Responsibility:	Overall responsibility for the execution of the management control and its documentation in the respective area
Tasks:	<ul style="list-style-type: none"> • Documentation of management control • Receipt the ICS report from Test Responsible or Division GRC and evaluation • Reconciliation with Test Responsible on the basis of the ICS report
Relevant skills	
Method skills:	<ul style="list-style-type: none"> • Understanding of process, roles and responsibilities • Methodology on confirmation of effectiveness phase
Technical skills:	<ul style="list-style-type: none"> • N/A
Relevant trainings:	<ul style="list-style-type: none"> • Training for Control Owner & Control Responsible
Qualification and experience:	<ul style="list-style-type: none"> • In general a minimum of 3 years experience within the relevant business process (internally or externally) or similar expertise.
Soft skills:	<ul style="list-style-type: none"> • Critical thinking;

1.6. Test Responsible

Role:	Test Responsible
Expected level:	Employee
Responsibility:	Responsibility for performing the confirmation of effectiveness and the documentation of the test results in RICORS
Tasks:	<ul style="list-style-type: none"> • Performance of confirmation of effectiveness and documentation of the results • Recording of follow-up measures, if necessary, in reconciliation with the Control Responsible • Performing the preliminary plausibility check of the test results with the Division IRC • Reconciliation with Risk Owner or Control Owner, if necessary with Division IRC • Release of all collected data for the verification (for which the Test Responsible is Responsible)
Relevant skills	
Method skills:	<ul style="list-style-type: none"> • Knowledge about the methods of the GRC process with regards to testing and test documentation • Understanding of the GRC process (testing phase) incl. Roles & Responsibilities • Understanding of Management Control
Technical skills:	<ul style="list-style-type: none"> • Handling of RICORS (Testing phase)
Relevant trainings:	<ul style="list-style-type: none"> • Basic Training for New Test Responsible • Refresher Training for existing Test Responsible
Qualification and experience:	<ul style="list-style-type: none"> • In general a minimum of 3 years experience within the relevant business process or similar expertise.
Soft skills:	<ul style="list-style-type: none"> • Critical thinking; • Communication skills; • Planning and coordination

1.7. GRC Responsible

Role:	GRC Responsible
Expected level:	Employee
Responsibility:	Responsible for controlling the regular GRC process within the business unit
Tasks:	<ul style="list-style-type: none"> • Coordination of the regular GRC process in the business unit • Check of all data from the entry phase • Granting release for all data entered within business unit • Appointing Test Responsible (s) • Validation of all results data for the confirmation of effectiveness for the business unit • Reconciliation of the results for the confirmation of effectiveness with Company GRC
Relevant skills	
Method skills:	<ul style="list-style-type: none"> • Knowledge about the methods of the GRC process • Knowledge of the GRC process (Testing and Recording phase) incl. Roles & Responsibilities
Technical skills:	<ul style="list-style-type: none"> • Handling of RICORS (Recording and Testing Phase)
Relevant trainings:	<ul style="list-style-type: none"> • Update slides and attending all other trainings
Qualification and experience:	<ul style="list-style-type: none"> • In general a minimum of 1 year experience within the relevant business process (internally or externally)
Soft skills:	<ul style="list-style-type: none"> • Critical thinking; • Communication skills



Attachment 6: Requirements for Quarterly Risk Process

Valid from:	03.12.2019
Last Change:	02.05.2022
Replaces the:	
Verification of validity:	31.12.2024
Responsible department for the process:	Integrity, Risk & Compliance - AGC
Name:	Integrity, Risk & Compliance Manager (Adélia Felício)
Telephone:	+351212112732
Issuing department:	Integrity, Risk & Compliance – AGC
Name:	Integrity, Risk & Compliance Manager (Adélia Felício)
Telephone:	+351212112732

Requirements for Quarterly Risk Process



1. Roles in the Quarterly Risk Process

1.1. Identifier

Role:	Identifier
Expected level:	Employee
Responsibility:	Identification and evaluation of risks in the own area of responsibility
Tasks:	<ul style="list-style-type: none">• Identification and assessment of risks (in collaboration with approver and releaser)• Recording of identified risks (in Risk Radar)• Coordination of the identified risks with other departments
Relevant skills	
Method skills:	<ul style="list-style-type: none">• Knowledge about the methods of the RQP with regards to identification and evaluation of acute risks• Knowledge about risk identification methods• Understanding of process, roles and responsibilities
Technical skills:	<ul style="list-style-type: none">• Handling Risk Radar (Advanced Knowledge)
Relevant trainings:	<ul style="list-style-type: none">• Basic Training for Risk Identifier
Qualification and experience:	<ul style="list-style-type: none">• In general a minimum of 1 year experience within the relevant business process (internally or externally)
Soft skills:	<ul style="list-style-type: none">• Good communication;• Critical thinking;• Planning and moderation of workshops

1.2. Approver

Role:	Approver
Expected level:	MK/OMK
Responsibility:	Overall responsibility for the risk situation (identification, evaluation, monitoring) in the area of responsibility and responsible for quality assurance of results
Tasks:	<ul style="list-style-type: none"> • Plausibility check of the completeness, comprehensibility, and accuracy of the content of the risk reports • Approval of risks in Risk Radar
Relevant skills	
Method skills:	<ul style="list-style-type: none"> • Understanding of process, roles and responsibilities
Technical skills:	<ul style="list-style-type: none"> • Handling Risk Radar (Basic Knowledge)
Relevant trainings:	<ul style="list-style-type: none"> • Training for Releaser / Approver
Qualification and experience:	<ul style="list-style-type: none"> • In general a minimum of 3 years experience within the relevant business process (internally or externally) or similar expertise. • The Approver should have: <ul style="list-style-type: none"> - Knowledge of the local processes - Knowledge about the business and the local situation
Soft skills:	<ul style="list-style-type: none"> • Critical thinking;

1.3. Releaser

Role:	Releaser
Expected level:	OMK/TMK
Responsibility:	Responsible for identifying the major individual risks, ensuring their completeness and the comprehensible description and assessment of all recorded risks in the area of responsibility
Tasks:	<ul style="list-style-type: none"> • Plausibility check of the completeness, comprehensibility, and accuracy of the content of the risk reports • Approval of risks in Risk Radar
Relevant skills	
Method skills:	<ul style="list-style-type: none"> • Understanding of process, roles and responsibilities
Technical skills:	<ul style="list-style-type: none"> • Handling Risk Radar (Basic Knowledge)
Relevant trainings:	<ul style="list-style-type: none"> • Training for Releaser / Approver
Qualification and experience:	<ul style="list-style-type: none"> • In general a minimum of 3 years experience within the relevant business process (internally or externally) or similar expertise. • The Approver should have: <ul style="list-style-type: none"> - Knowledge of the local processes - Knowledge about the business and the local situation
Soft skills:	<ul style="list-style-type: none"> • Critical thinking;

1.4. Local Risk Management

Role:	Local Risk Management
Expected level:	Employee
Responsibility:	Plausibility check of the risks at local level with regard to the methodological specifications
Tasks:	<ul style="list-style-type: none"> • Plausibility check of the released risks at local level regarding completeness, comprehensibility and method conformity • The local RMA identifies multiple reported risks (risk duplicates) from different collectors and coordinates the reconciliation between them • Forwarding the risks to finance, if necessary
Relevant skills	
Method skills:	<ul style="list-style-type: none"> • Understanding of process, roles and responsibilities • Knowledge about the methods of the RQP with regards to identification and evaluation of acute risks • Methodology on Plausibility Check
Technical skills:	<ul style="list-style-type: none"> • Basic Training for Risk Identifier • Training for Releaser/ Approver
Relevant trainings:	<ul style="list-style-type: none"> • Training for Releaser/ Approver
Qualification and experience:	<ul style="list-style-type: none"> • In general a minimum of 1 year experience within the relevant business process (internally or externally)
Soft skills:	<ul style="list-style-type: none"> • Critical thinking;



Attachment 7: The Volkswagen Three-Lines Model

Valid from:	02.05.2022
Last Change:	
Replaces the:	
Verification of validity:	31.12.2024
Responsible department for the process:	Integrity, Risk & Compliance - AGC
Name:	Integrity, Risk & Compliance Manager (Adélia Felício)
Telephone:	+351212112732
Issuing department:	Integrity, Risk & Compliance – AGC
Name:	Integrity, Risk & Compliance Manager (Adélia Felício)
Telephone:	+351212112732

The Volkswagen Three - Lines Model



1. The Three-Lines-Model

A central element of any governance is the definition and allocation of clear roles. The allocation of roles at Volkswagen Autoeuropa in the implementation of compliance management systems is carried out according to the Volkswagen Group's Three-Lines-Model which is closely based on the Three-Lines-Model of the Institute of Internal Auditors (IIA).

In addition to the roles of the three lines that give the model its title the Volkswagen Three Lines-Model also defines the roles of the Board of Directors of Volkswagen Autoeuropa, the so-called management bodies, in interaction with the three Lines.

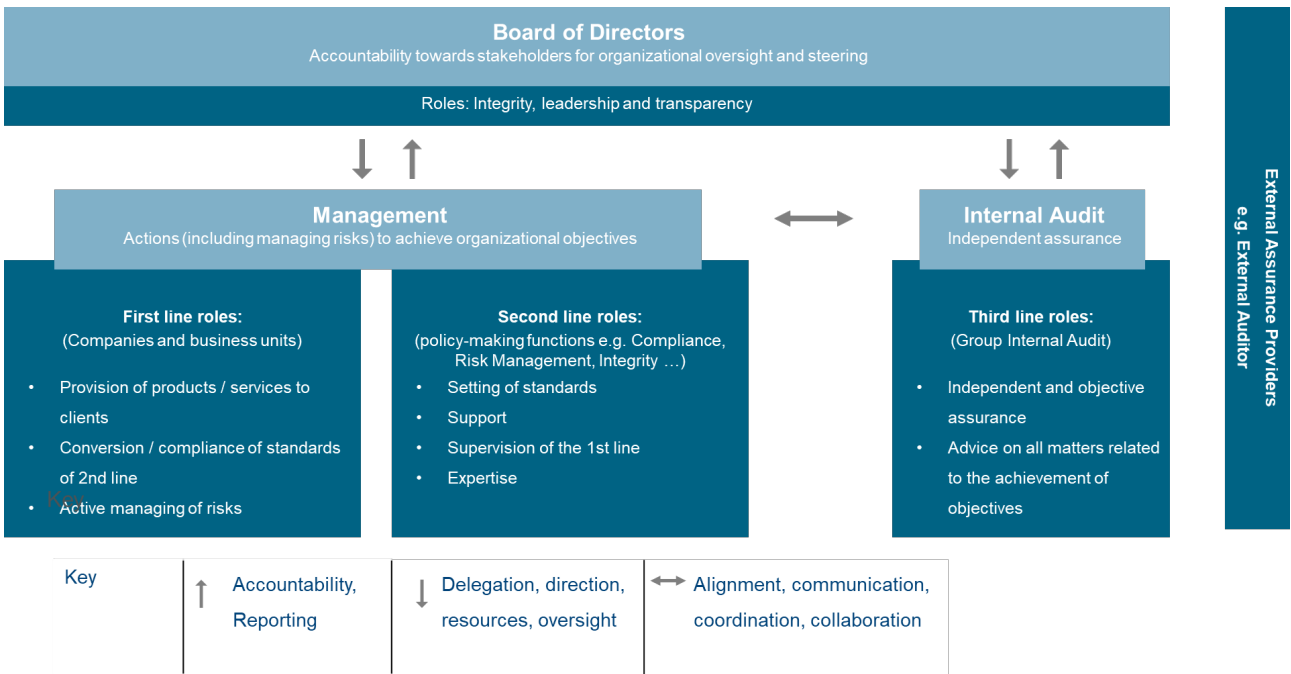


Figure 1: The Three-Lines-Model at Volkswagen Group

2. The Principles of the Three-Lines-Model

The Volkswagen Three-Lines Model rests on the following six principles:

1. Governance

Governance of an organization takes into account *accountability*, *commitment* to action as well as assurance and advice.

Accountability is exercised by the management bodies (cf. principle 3) towards relevant internal and external stakeholders. Through this, integrity, leadership and transparency are exemplified.

The *obligation* to act is delegated to the responsible management of the first line and the second line - also with regard to risk management in the respective area of responsibility. The management has the task of ensuring the achievement of objectives through risk-oriented decision-making using the resources made available.

Assurance and *advice* is ensured by the internal audit (cf. principles 5 and 6).

2. Creating and Protecting Value

Collaboration between the roles of all three lines contributes to value creation and value protection through mutual agreement on a common approach, also in terms of prioritizing stakeholder interests. Alignment of activities is

achieved through communication, collaboration and common alignment on the overall goals. This ensures reliability, coherence and transparency in the flow of information necessary for decision-making.

3. Management, First and Second Line Roles

The management of the 1st line and the 2nd line are responsible for achieving the goals of the organization. The roles of the 1st line are mainly focused on the production of products (material and services before the customer and internally), including corresponding support services. The roles of the 2nd Line provide support with regard to the risks to be mitigated.

1st Line and 2nd Line can be mixed or set up separately. In any case, with regard to the monitoring of the 1st line by the 2nd line, which is necessary for successful governance, clear organizational safeguards must be established (e.g. four-eyes-principle for relevant decisions, segregation of duties, clear allocation of responsibilities of the 1st and 2nd line management e.g. in TAR / TAR Plus, separation of group and brand responsibility).

4. Governing Body Roles

The management bodies (cf. principle 3) ensure that appropriate structures and processes for effective governance are in place within the company and that the company's objectives and activities are aligned with the prioritized interests of the stakeholders.

To this end, governing bodies delegate responsibility to management to achieve the objectives of the organization while ensuring legal, regulatory, and ethical expectations are met.

Furthermore, they establish and oversee an independent, objective, and competent internal audit function to provide clarity and confidence on progress toward the achievement of objectives.

5. Third Line Roles

Internal audit provides independent and objective assurance and advice on the adequacy and effectiveness of governance and risk management. It reports its findings to management and to the governing body to promote and facilitate continuous improvement.

6. Third Line Independence

Internal audit's independence from the responsibilities of management of 1st and 2nd lines is critical to its objectivity, authority, and credibility within Volkswagen Autoeuropa. It is established through accountability to the governing body, unfettered access to people, resources and data needed to complete its work, as well freedom from bias or interference in the planning and delivery of audit services. The tasks of the internal audit are described in more detail in ADM-F-O090- "GP_28_Revision".

3. Application of the Three-Lines-Model at Volkswagen Autoeuropa

The Three-Lines-Model at Volkswagen Autoeuropa defines the three roles, e.g. in connection with the governance of compliance management systems. In this context, the roles in an individual compliance management system or against the background of an individual risk topic area are distributed as follows:

The Governing Bodies

The Board of Directors of Volkswagen Autoeuropa are to be regarded as management bodies within the meaning of the Three Lines-Model. They are responsible for providing the company with appropriate structures and resources to ensure the successful management of Volkswagen Autoeuropa. In doing so, the company's objectives are aligned to the various stakeholder interests with integrity and transparency. The management bodies define an appropriate organizational structure and process organization along the Three-Lines detailed below.

First Line / “1st Line“

The 1st Line forms the group of users of a management system. In this context, the first line implements the valid guidelines with the aim of mitigating defined compliance risks. Through measures to promote integrity, all operational users contribute to compliance with measures and values within the Group.

The 1st Line is made up of the majority of the operational business and specialist departments at Volkswagen Autoeuropa. The 1st Line reports to superiors in accordance with its defined organizational reporting lines. In addition, the 1st Line reports to the 2nd Line in connection with the reporting obligations defined, e.g. on the respective Compliance Management System.

Second Line / „2nd Line“

The topic specific 2nd Line is the policy making or method and standard setting, process controlling, supporting and advisory function of Volkswagen Autoeuropa that is responsible for a specific topic, e.g. a compliance risk topic area. In addition, the 2nd Line performs a monitoring function vis-à-vis with the 1st Line. Unless otherwise defined, this function at Volkswagen Autoeuropa, which is also referred to as the policy-making body is identical to the policy making body for the Volkswagen Group. It is responsible for defining and structuring the topic specific rules and regulations as well as the respective compliance management system, exercises governance accordingly and reports to the Board of Directors of Volkswagen Autoeuropa, if necessary via defined committees and reporting lines.

The responsibility of the 2nd Line is to be delegated by Board of Directors of Volkswagen Autoeuropa to Integrity, Risk & Compliance Manager.

The 2nd Line thus effectively assumes the duty to act from the Board of Directors of Volkswagen Autoeuropa, who in turn remains responsible for monitoring and controlling the compliance risk topic area through the non-delegable organizational duty and to whom the 2nd Line must report in this context. For legal reasons, the responsibility for monitoring and control of the compliance management system or the risk topic area cannot be delegated to a second line.

The delegation of the duty to act to a unit responsible for covering the risk topic area is intended to reduce the probability of occurrence of overarching risks and to effectively mitigate damage in the event of possible violations by Volkswagen Autoeuropa of applicable laws and regulations. The establishment and maintenance of an effective compliance management system is an important step towards risk mitigation.

Third Line / „3rd Line“

The 3rd line is formed by the independently and objective Group Internal Audit, which can be supported by external auditors. The tasks of the internal audit are described in more detail in ADM-F-O090- “KRL_28_Revision”.



Further details on the tasks of Group Audit are described in the document ADM-F-O090-KRL_28_Revision_en_V1.0 available in Quality Management system