COMMERZBANK

Audit Report Definitions

Group Audit

Table of Content

Audit Rating

Criteria: Ratings reflect the condition of regulations and precautions as well as compliance with them in order to assure or secure:

- Business transactions and assets,
- compliance with business guidance and company principles (including Management conduct),
- an effective internal control system,
- a functioning management of risks and revenue potential including the respective information systems,
- compliance with legal and supervisory regulations,
- Economy and efficiency of banking services.

Result	Good (++)	Satisfactory (+)	Fair (o)	Not satisfactory (-)	Deficient (--)
Definitions	Regulations and precautions are appropriate; the internal control system is functioning and effective. No or only low risk findings were raised.	Regulations and precautions are appropriate; the internal control system is functioning and effective. Only modest weaknesses were noted.	Regulations and precautions show weaknesses. Findings were raised in relation to the functioning and/ or effectiveness of the internal control system. Damage may occur, if the deficiencies are not remedied.	Regulations and precautions as well as the functioning and/or effectiveness of the internal control system show significant deficiencies. There is a risk of substantial losses/damages, if the deficiencies are not remedied.	Regulations and precautions as well as the functioning and effectiveness of the internal control system show serious deficiencies. The safety of business operations and/or further business development is seriously at risk. There is a risk for imminent losses/damages.
Corrective Action	Findings can be remedied within the normal course of business. No particular degree of supervision is required.		Management responsible for the audited area should determine an adequate action plan and supervise timely implementation.	Close supervision and involvement of the management responsible for the audited area are required. Additionally, a deficient result might require fundamental restructuring measures in the audited area.	

The audit result is primarily derived from frequency, characteristic and impact of findings raised. Thereby, the extent to which the findings reveal weaknesses individually, in their combination or in their correlation with other risks is to be considered. Other criteria are the appropriateness of management's dedication to supervising the business, its control awareness, the implementation of agreed corrective actions and the remediation of findings from previous audits, as well as extent, development and management of risks. In view of diverse conditions and requirements encountered in each audited unit, criteria for the allocation of individual audit results might be weighted differently.

Materiality Ranking

The **materiality ranking** in the Audit report reflects the significance of the audited business or project/ initiative in relation to the Bank as a whole on a scale from 1 (low) to 4 (very high).

1	2	3	4
Low	Moderate	High	Very High

The ranking is based on objective, qualitative and quantitative criteria. Both the weighting and selection of the criteria are at the discretion of Group Audit. The materiality ranking should reflect the scope, nature and complexity of the audited business or project/ initiative. Local specifics are considered in the determination of the materiality ranking.
The materiality assessment is independent of the audit rating, does not follow a mathematical model and does not provide an indication of the relevance of individual findings.
The criteria and thresholds applied are made available to the audited unit on request.

The criteria for determining materiality are divided into four categories:

Categories	Regular Audit				Project/ Initiative Audit
Strategic Objectives	• Contribution to Earnings				• Strategic Relevance • Budget/ Invest
Operational Objectives/ Preservation of Assets	• Assets under Management • Number Customers/ Accounts • EaD • Number of Transaction/ Month (Sales & Trading) • VaR	***Entity/ Branch/ Location*** • Strategic Importance/ Tier	***Functional Audits*** • Number of Transactions/ Month • Complexity of Business • Number of Employees	***IT*** • Overall assessment based on SecAM criteria • Criticality of business process	• Complexity and Dependencies
Compliance with Rules and Regulation	• Scope of process ownership and supervisory legislation				• Regulatory Relevance/ Requirement
Reporting	• Importance for the bank's overall reporting				

Evaluation Components for Processes

The **Definition of Evaluation Components for Key Processes is** based on the COSO Model (Enterprise Risk Management).

Components	Definitions	Key Elements
Environment	The internal environment characterises culture and ethical values of an organisation. Organisational structure, especially reporting lines, and powers & authorities as well as staff qualification and personnel management are evaluated. It encompasses formal requirements with regard to the written framework and the evaluation of compliance with external requirements.	• Philosophy & Ethics • Internal Supervisory • Organisational Structure • Powers & Authorities • Professional Qualification & Personnel • Written Framework • External Requirements
Objective Setting	A strategic framework is necessary providing consistent, transparent and comprehensible goals. Based on this framework, operative targets should be defined to facilitate the steering of the organisation. These targets should be achievable given the risk appetite as well as other general conditions.	• Strategic Framework • Operative Targets • Strategic & Operative • Feasibility
Managing Risk	To ensure an adequate process design internal and external events affecting achievement of an entity's objectives must be identified and distinguished between risks and opportunities. In order to enable effective risk steering, risks are analysed and evaluated, considering likelihood and impact. Based on this and the entity's objectives, the risk tolerance and the risk appetite, adequate processes are developed and implemented.	• Identification Process • Assessment and Measurement Process • Response Process and Measures
Control Activities	Defined processes have to be adhered to. In addition, controls need to be developed and performed to ensure compliance with the defined processes.	• Assessment of Internal Control Design • Performance of Internal Controls
Information & Communication	Relevant information is processed timely, communicated and if necessary escalated using appropriate channels. This encompasses internal communication of organisational and process related issues enabling process owners to carry out their responsibilities. Effective communication also occurs bi-directional and within the different levels of the entity's organisation. External Communication includes presentation of internal information to stakeholders outside of Commerzbank Group.	• Internal Information, Communication & Escalation • External Communication

Risk Levels for MaRisk Deficiencies

The **classification of deficiencies according to MaRisk** reflects the relevance of a deficiency (as result of single finding or aggregation of findings) for the Commerzbank-Group.

MaRisk Classification

Particularly Severe Deficiency:
Under consideration of the risk types in accordance with the risk inventory of Commerzbank Group a critical threat potential for the entity's business exists from an overall perspective. An immediate reporting by the Management of the Entity to the Supervisory Body is required.

Severe Deficiency:
Under consideration of the risk types in accordance with the risk inventory of Commerzbank Group a considerable threat potential for the entity's business exist from an overall perspective. An immediate reporting to the Management of the Unit is required.

Material Deficiency:
Under consideration of the risk types in accordance with the risk inventory of Commerzbank Group a collateral threat potential for entity's business exists from an overall perspective. A reporting to the Management of the Entity as well as to the Supervisory Body along with the Audit Annual Report is required.

No Material Deficiency:
Under consideration of the risk types in accordance with the risk inventory of Commerzbank Group a minor threat potential for entity's business exists from an overall perspective. The information of the Management in addition to the individual audit reports is not required.

The classification of the underlying single findings (high, medium, low) reflects the relevance of deficiencies based on a (single) finding with regard to the audited unit.

Risk Classification for Individual Findings

High (↑)
Under consideration of the risk types in accordance with the risk inventory of Commerzbank Group - as far as relevant for the area audited - and based on the finding, significant deficiencies exist for the area audited. These deficiencies affect, for example, critical business processes or have significant reputational or regulatory effects. Strict control over the timely implementation of the agreed corrective action as well as the involvement of the responsible management is necessary.

Medium (→)
Under consideration of the risk types in accordance with the risk inventory of Commerzbank Group - as far as relevant for the area audited - and based on the finding, deficiencies exist for the area audited. These deficiencies concern, for example, the interruption of business processes, lead to customer or supervisory complaints. The responsible management should ensure that evidence over the timely implementation of the agreed corrective action is being provided.

Low (↓)
Under consideration of the risk types in accordance with the risk inventory of Commerzbank Group - as far as relevant for the area audited - and based on the finding, minor deficiencies exist for the area audited. The impact on customer and business processes is limited. The corrective action can be implemented during the regular course of business.

Additional Details on the Findings

Classification	Additional Details
(A) New Findings	Findings that relate to new issues, i.e. not reported by Group Audit before.
(B) Repeated Findings	Findings that have previously reported by Group Audit or external authorities.
(B1) Repeated Findings (narrower sense)	This category covers findings for which the risks disclosed in a previous audit report were not addressed and therefore remain in the same way for following reasons: • Non-observance, gross negligence or (deliberate) deficient/lacking diligence of management • Overdue high risk actions from previous audits with inadequate progress • Findings relating to same issues as in the previous audit, which need to be re-opened due to risks that have not been sustainable mitigated.
(B2) Management has taken measures to implement corrective actions as agreed in the previous audit, though key risks raised remain largely unchanged	This category covers findings for which management has substantially addressed the original issues and risks. However, there is the need for further remediation as additional risks have come up in the meantime. This category also covers actions that have been assessed as overdue but reasons are comprehensible. It applies for overdue high and medium risk issues where progress is assessed to be adequate.
(C) Open Findings	Open findings where implementation of corrective actions (including milestone plan as applicable) is on track as planned (due date in the future).

Root Cause Categories

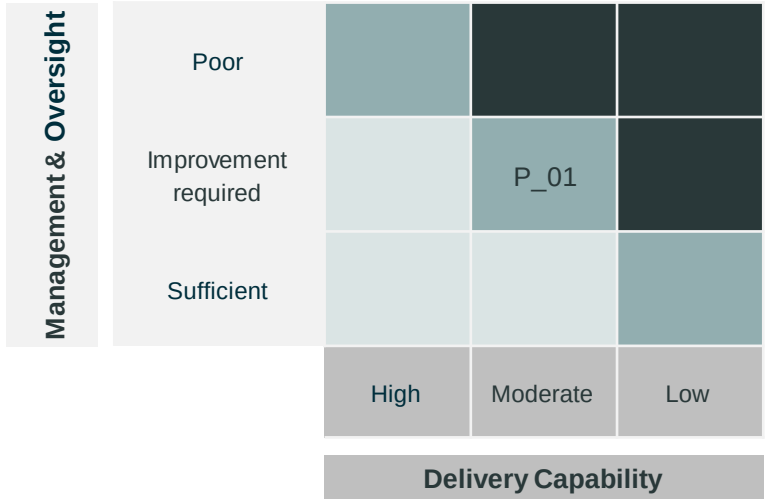
Category	Description
Policies & Guidelines	The cause of the identified issue is due to incomplete, outdated, unclear or inappropriate instructions (written framework, policies, guidelines, procedural instructions, misinterpretation of regulatory and/ or internal guidelines).
Process Design	The cause of the identified issue lies in the fact that the defined processes are not appropriate to handle the business associated with the processes adequately and to identify and manage the associated risks in order to comply with internal and external regulatory/legal requirements. (Definition, design of a process, misinterpretation of regulatory and/ or internal guidelines)
Process Execution	The cause of the identified issue is due to a lack of process execution, e.g. due to improper diligence, lack of understanding of the process.
Control Environment	The cause of the identified issue is due to an inappropriate control environment, including, but not limited to, lack of controls or incorrect, inadequate or missing control mechanisms, approvals, etc.
Roles & Responsibilities	The cause of the identified issue is due to organizational reasons, e.g. unclear responsibilities, interfaces, (perception of) responsibilities & competencies. Issues are due to structural changes in the bank, e.g. in the context of digitalization or transformation, without (sufficient) consideration of dependencies (including on projects of the bank).
Skills & Competencies	The cause of the identified issue is due to insufficient skills, specialist knowledge, training (of the executing employees).
Human Error	The cause of the identified issue is due to individual, personal errors, e.g. "fat fingers", individual transient errors, etc.
Technical Issue	The cause of the identified issue is related to IT, software and hardware without direct human fault.
Insufficient Resources & Equipment	The cause of the identified issue is due to a lack of quantity of resources, e.g. personnel, equipment, budget, technology.
Priorisation/ Management Decision	The cause of the identified issue is due to (direct) (inappropriate) management decisions, e.g. de- or reprioritization of topics.
Inadequate Risk Awareness	The cause of the identified issue is due to a lack of risk awareness, including a lack of competence to identify, assess, treat and mitigate potential risks and their (potential) impacts.
Other	Everything that can not be allocated to the above mentioned categories.

Project Rating Definitions

Project rating definitions are applied in project reports and when projects/initiatives are taken into account in regular reports.

The weaknesses and risks identified through the performed audit procedures are the basis for assessing the "management & oversight" and the "delivery capability" of a project at the time of the audit.

Project Rating



Result		Definition
Management & Oversight	Sufficient	The project management and oversight are **suitable and effective** at the time of the audit**.**
	Improvement required	The project management and oversight are **generally suitable** at the time of the audit. However, the achievement of the objectives must be supported by **additional measures**.
	Poor	There are significant weaknesses in the project management and oversight at the time of the audit. The overall achievement of the project goal is at risk.
Delivery Capability	High	Based on the audit procedures performed, **no weaknesses** have been identified at the time of the audit time that could jeopardize the successful delivery of the target solution, provided that the remaining deliveries are implemented and that the project management continues to work with the same discipline.
	Moderate	Based on the audit procedures performed, the project is **delayed for partial deliveries** at the time of the audit or there is a **risk** of **not achieving some or all targets** if no additional actions are taken. The problems must be remedied in order to increase the delivery capability.
	Low	Based on the audit procedures performed, the project is not able to achieve its targets. The identified problems indicate **a significant risk of a succesful delivery**.

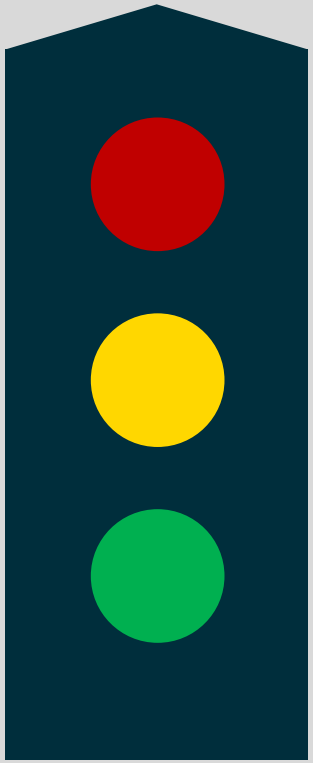
Change Assurance Types

Change Assurance Types are assessed in project reports and when projects/initiatives are taken into account in regular audit reports. They are defined along the lifecycle of a project and their consideration depends on the scope of the audit.

Change Assurance Types	Key Elements
Governance	Focuses on the set-up, steering and risk management of initiatives e.g. Stakeholder Relations; Risk & Issue Management, Dependency Management; Scope, Cost & Benefit Definition; Boards & Committee Structure as well as Reporting.
Requirements & Design	Focuses on the management of requirements and the process of developing the target solution, e.g. assessing if functional requirements are sufficiently defined and considered in the target design, regulatory requirements are adequately implemented, and IT-solutions are in accordance with the architectural target design.
Development	Focuses on the methodological approach, the selected development method, the handling of IT changes as well as supplier management.
Testing	Focuses on test activities within the project such as test strategy, planning, test design as well as test performance to assess if the target solution works as designed.
Transition	Focuses on processes of transferring project activities into business-as-usual processes e.g. roll-out and transfer processes, Business Readiness & Business Contingency Planning, Training & Communication as well as handling of Lessons Learned.

Audit Rating (Project Report)

The **Definitions of Evaluation Levels (Project)** are as follows:



Red
High risks regarding the overall project were noted which, depending on the focus of the audit, are derived from the implementation of business requirements and/or from project management/organisation. The overall project target is substantially endangered, in case there is no appropriate counteraction for the identified risks. The risk of significant/direct substantial losses/damages is imminent. An unchanged continuation of the project seriously endangers the security of the business process and the further business development. The project requires close supervision and the involvement of management of the units participating in the project. After performing a comprehensive risk analysis, the persons in charge of the project should set up a risk action plan and a subsequent risk controlling. Re-engineering of the project may be necessary.

Yellow
Risks regarding the project organisation and/or risks from the project were noted. The overall project target is endangered, in case there is no appropriate counteraction for the identified risks. After performing a comprehensive risk analysis, the persons in charge of the project should set up a risk action plan and a subsequent risk controlling.

Green
No or only modest risks regarding the project organisation and/or risks from the project were noted. The identified risks can be reduced/eliminated/remedied within the normal course of the project. No particular degree of supervision is required.