Julius Bär

Document title:	JBG-1007-00 Internal Control Framework
Effective date:	17/06/2020
Version:	5.0
Approved by:	Oliver Bartholet, Oliver Pauly
Author:	Gabriella Stratoti
General scope:	Legal Entities worldwide

Julius Baer Group	Significant regulated entities	All other Advisory Offices	Group WMCs	Other
	Bahamas Germany Guernsey Hong Kong India Luxembourg Monaco (Bank) Singapore Switzerland (Bank) U.A.E. UK	Austria Bahrain Chile Ireland Israel Lebanon Monaco JBWM Russia South Africa Spain Uruguay	Fransad Gestion GPS Brazil JB Fiduciaria (Milano) JBWM Nomura Kairos NSC Wergen & Partner	Small Offices TRCM

SUMMARY

This policy defines minimum standards to effectively design, execute and manage internal controls. In addition, the policy outlines associated processes and clarifies respective roles and responsibilities. Detailed information regarding the topics outlined in this policy can be found in the JBG-G-1007-00 Internal Control Framework Guideline and JBG-G-1007-01 Guideline for 2nd LoD Controls.

Key aspects of this policy

- Explains the standards of the Internal Control Framework in Julius Baer
- Defines Roles and Responsibilities of stakeholders involved in the internal control activities
- Explains the design and maintenance of global minimum controls / key controls
- Defines a global minimum standard for consistent managing of controls; implementation, reporting, escalation of identified issues and documentation
- Defines the self-assessment and quality assurance process of controls

Violation of this policy may result in disciplinary action.

1. DEFINITIONS

The section below provides a glossary for the acronyms and terms used in this policy in relation to the Internal Control Framework (ICF). Further details related to risk types, risk assessments and other terms can be found in the Risk Management Framework (RMF) or respective policies. An overview of the abbreviations used in this policy is included in the appendix.

1.1. Internal Control Framework

The ICF is the sum of controls and processes that operate across the three lines of defence[1] to ensure that risk is being incurred in a deliberate and disciplined manner. The Control Framework team within Monitoring & Operational Risk Control (MORC) is responsible to set and oversee the standards of the ICF and works closely with the Operational Risk Control and the Consolidated Supervision team to ensure alignment.

1.2. Controls

A control is an activity to check that individual policies, guidelines and processes are followed. The definition of a control includes a front-to-back review of a process, spot checks with specific control questions, automated monitoring routines, or checks of first line of defence controls (check-the-checker controls). It can be process-independent or embedded. The control's objective is to identify mistakes, policy breaches, misconduct and other potential risks in order to remediate, sanction and prevent them from reoccurring[2].

The control repository (e.g. BaerControl) shall only include actual controls. Tasks or instructions must not be formulated as GMCs or KCs and not be included in the control plan.

Common non-controls are:

- instructions to implement a process or a concept
- instructions to establish a report
- instruction to send a reminder
- confirmation that a process was followed
- confirmation that specific tasks were fulfilled

Such instructions or tasks are typically requested in a global policy (Global Minimum Standard (GMS)) and not in a control plan.

[1] Refer to section "The three lines of Defence and link to the internal Control System" of the RMF for the definition of the three lines of defence.

[2] Refer to section "Definitions" of the JBG-G-1007-00 Internal Control Framework Guideline

1.3. Global Minimum Controls (GMCs)

Global Minimum Controls are defined by the Risk Type Owner (RTO) to address the global and / or significant inherent risks and to assure compliance with underlying global standards and policies. A risk type or risk scenario is considered as 'significant' if the inherent risk is assessed to be "major" or "severe" in the Risk Type Owner Assessment (RTOA). The global significance is given if the GMC is directly linked to a global policy or has been defined as global by the Risk Type Owner (RTO).

The mandatory attributes[3] are to be applied when defining the GMC. GMCs need to be linked to at least one level-3 risk type and one level-4 risk scenario. GMCs materialize in local key controls.

1.4. Local Key Controls & Non-Key Controls

Local controls are defined at the level of the local entity, branch, business unit, etc. The local controls provide a detailed description and systematic instructions on how to perform the control. Local controls are classified as key controls or non-key controls. The classification of a local control as 'key' is based on three criteria. If one or more of the following three criteria is fulfilled the local control is defined as key-control, if none of the criteria is fulfilled the local control is defined as non-key:

1. Link to GMC: The local control is the implementation of a GMC.
2. Regulatory requirement: The control is implemented to check compliance with a specific regulatory requirement.
3. Link to local major or severe inherent risk: The control is linked to a risk type (level III) or risk scenario (level IV) that is assessed to have a major or severe inherent risk in the Risk-Control-Self-Assessment (RCSA).

1.5. Supervisory Controls

Supervisory controls include monitoring of staff activities and controls assigned to managers on all levels based on their organisational responsibility. Among other, they include the duty to check and enforce adherence to policies, to act on risk information provided by other control bodies, to monitor activities of their subordinates, to follow-up on corrective actions, and to assess and enhance the control framework. Supervisory controls can be key controls as well as non-key controls.

2. ROLES AND RESPONSIBILITIES

2.1. Risk Type Owners (RTO)

The RTO is the owner of the respective GMCs which are mapped to his / her level III risk type. In case the GMC maps to multiple level III risk types, a main risk type has to be agreed and the RTO of the main risk type is the owner of the GMC and coordinates with the other impacted RTO(s).

The RTO is responsible to assess the level of inherent risk of his / her level III risk type and to define a set of GMCs for its mitigation in accordance with JB's Risk

[3] Refer to section "Mandatory Control Attributes" of the JBG-G-1007-00 Internal Control Framework Guideline

Management Framework. The RTO determines the group-wide applicability of his / her GMC across entities and in line with the applicability of the related global policies (global minimum standards (GMS)) and oversees the implementation of the key controls mapped to GMCs.

Whilst the individual tasks (e.g. to design a GMC or to endorse a key control) can be delegated to a Subject Matter Expert, the RTO keeps the accountability for his / her respective risk type.

2.2. Control Owners

Control owners are line managers or senior team members within the 1st or 2nd line of defence who are responsible for managing local risks and controls related to their businesses. It is a person of suitable expertise, experience and seniority related to the controlled topic. The local control owner defines the control design and nominates the appropriate control performer. In case the local key control is linked to a GMC, the local control owner has to ensure that the control achieves the objective that is defined by the GMC or raise a deviation request, which must be formally approved by the respective RTO.

Local control owners are responsible to oversee that the control is executed as designed and in line with the minimum standards described in this policy and respective guidelines, to review control results (4-eye check)[4] and ensure that follow-up actions are being tracked and resolved within an acceptable timeframe.

In addition, they assess the design and operating effectiveness of their controls once a year[5], but also on an ad-hoc basis where required. This activity is coordinated and supported by the respective control plan owner(s).

2.3. Control Performer

The control performer is responsible to perform controls assigned to them based on the control design and within the requested timeframes and in line with the minimum standards described in this policy and respective guidelines. He / she ensures proper documentation of control results, follow-up on defects and escalates issues to the control owner. The control performer has the respective technical knowledge to perform the control. In the significant regulated entities, the control owner and the control performer must not be the same person.

2.4. Control Plan Owner

The plan owner administers a control plan for a specific business unit, location or function and links the appropriate controls to the control plan. This is an administrative activity only. The responsibility for the appropriate set-up of the controls remains with the control owners.

[4] Refer to section 3.6. 4-eye Check of this policy

[5] Refer to JBG-G-1007-00 Internal Control Framework Guideline

2.5. Compliance / Risk Management function

The Compliance / Risk Management function in the location is responsible to maintain an overview regarding:

- All local control plans
- Implementation and reporting of key controls linked to GMCs
- Any additional local key control execution

In addition, they create a quarterly report for senior management including the control results and delay in control execution as a minimum. Local Compliance / Risk Management reports on both (1) GMC implementation status including deviations or non-applicability despite initial assessment of services offered by the legal entity and (2) control execution status and results of all GMC-related key controls to the Consolidated Supervision team in head office on a quarterly basis. Entities, which qualify as “Small Offices” (and therefore have no local Compliance or Risk Management function) the local line management has to implement and maintain controls. Line management also has to ensure compliance with Local Corporate Governance Guidelines and applicable global standards[2].

2.6. Head Office Global Responsibilities

The MORC function serves as a competence centre for the topic of Internal Controls:

The Control Framework team is responsible to set minimum standards, maintains the control framework, monitors the GMC lifecycle and reviews new / changed / deleted GMCs ahead of publication. It initiates the annual Design Effectiveness and Operating Effectiveness (DE / OE) self-assessment of key controls and coordinates in this regard with the entities in the locations.

The results of the self-assessments serve as an input to the RCSA and the RTOA[6]. These are coordinated by Operational Risk Control with the business units, the Group entities and the RTOs respectively.

Consolidated Supervision is responsible for the global coordination of the GMC process with all locations of the Julius Baer Group. The team is the key point of contact for the locations for the GMC implementation and execution status including control results. Consolidated Supervision is responsible to report the implementation status and quarterly execution and results of key controls linked to GMCs to RTOs. They coordinate with the locations and inform about updates of the GMCs. Consolidated Supervision coordinates and maintains a quality assurance plan to review the DE / OE self-assessment of implemented key controls mapped to GMCs.

[6] Refer to section “Instruments” of the D-1027-00 Group Operational Risk Policy

3. CONTROL STANDARDS

3.1. GMC Design and Maintenance

GMCs are defined on control objective level, specifying the precise purpose and goal of the control and the result that is to be achieved by executing the related local controls. The control objective must be formulated[7] in a way that the design effectiveness can be tested against it (i.e. to answer the question whether the local control is designed in a way to achieve the control objective).

The RTOs design and are responsible to maintain the set of GMCs of their respective risk type. GMCs have to be reviewed at least annually by the RTO before the DE / OE Self-Assessment. The RTO shall consider the RCSA and the RTOA results from the previous cycle when updating the GMCs. However, in case ad-hoc changes are required the RTO is responsible to update the design of the GMC within an acceptable timeframe (e.g. in case of regulatory changes).

Amongst others, the RTO defines the applicability of the GMC by applying the “toolbox approach”[8] including the entities and services dimensions and in line with the applicability of the related global policy (GMS).

New GMCs / updated GMCs shall be implemented by the entities as key controls within 6 months after the change is published / communicated, or raise a deviation (refer to section 3.3).

3.2. Key Control Design, Implementation and Maintenance

Local controls are designed by local control owners. The control owner needs to give an unambiguous and concise description on how to perform the control. The information shall give the local control performer a clear understanding, how the control needs to be executed (e.g. what steps are to be taken, where does the data come from) and how the control objective can be obtained.

To ensure an up-to-date inventory of key controls, all controls are re-classified annually based on the three key-control criteria described in section 1.4. The re-classification is part of the annual DE / OE self-assessment process stated in section 3.10. of this policy.

3.3. Deviations to GMCs

The applicability of a GMC for an entity depends on the respective business model and activities. If a GMC is (1) not applicable despite initial assessment based on the “Toolbox Approach” or (2) not implemented as per GMC design in a local entity, branch or business unit, a non-applicability / deviation request has to be raised by the location with the respective local or regional CRO for endorsement and the RTO for formal approval.

The entity has the possibility to raise a minor or a significant deviation. Minor deviations are more formal in nature and no additional risk is related to the deviation. Minor

[7] Refer to section “Mandatory Control Attributes” of the JBG-G-1007-00 Internal Control Framework Guideline
[8] Refer to section “Group-wide Policy and Control Framework” of the RMF

deviations are changes of methodology with regards to the control execution (other sources or tools use), minor deviation from control design (e.g. sampling methodology) and frequency deviations. Significant deviations are all other deviations which create additional risk such as the non-execution of controls due to low risk in the respective entity, partial non-execution of the control, non-execution due to missing data sources or tools. Both types of deviations, minor and significant require an annual review.

If a GMC is not applicable to an entity (e.g. if service / business activity is not provide locally), the local Risk or Compliance teams have to coordinate the documentation of a non-applicability request. The request needs to be approved by the RTO or his/her delegate and documented locally for audit purposes (incl. rationale).

All approved deviations and non-applicability need to be reported to the Consolidated Supervision team in head office for information to the central deviation and non-applicability repository.

3.4. Control Plan

The control plan consists of the inventory of controls for a business unit or entity. A control plan contains at least the following elements: control name, control reference number, control objective and description, scope / coverage, related risk type(s) and policies/regulations, definition of sampling methodology, control owner, control performer, time and frequency of the control execution and reporting.

3.5. Control Execution

Generally, controls must be performed within 21 calendar days after the execution start date. Exceptions are made for Check-the-Checker Controls[9] (2nd LoD only) or controls where there is a consistent delay in execution due to data dependencies. Where exceptions are made, the control description must include the information about the time lag, which can be one additional control period, but not more than one quarter.

The gap between execution frequency and task frequency (reporting frequency) shall not be significant i.e. daily / weekly and monthly controls to be reported at least quarterly. For less frequent controls, a 1:1 reporting frequency is expected[10].

3.6. 4-eye check

In significant regulated entities, the control owner has to review and approve the control execution made by the control performer. In the review he / she includes as a minimum whether the control was executed as designed and whether the standards of this policy were met (e.g. documentation and control results rating).

[9] Refer to section “Definitions” of the JBG-G-1007-01 Guideline for 2nd LoD Controls

[10] Refer to section “Control Execution” of the JBG-G-1007-00 Internal Control Framework Guideline

3.7. Control Results

The control results are made available by control performers to relevant control owners (e.g. line managers) for review and assessment in a comprehensive and standardized manner.

The control result rating is either Red, Amber or Green (RAG) and has to be selected based on the severity of the control results.

Although a quantitative threshold can be defined for each control, the qualitative perspective when selecting the RAG control result always prevails.

The overall result is based on the individual control samples result which are either 'pass', 'minor', 'moderate' or 'major' in nature. If a control result is Amber or Red, the control performer has to document a summary of the identified findings and the actions taken / recommendations made to the controlled party.

The key control results are aggregated and a consolidated rating is established on an entity or risk type level also applying a qualitative view. A detailed description of controls results ratings can be found in the JBG-G-1007-00 Internal Control Framework Guideline.

3.8. Reporting of Control Execution and Results

A quarterly control report is established by Local Risk or Compliance teams for the Business Unit Heads / RTOs. As a minimum requirement the report contains the consolidated key control results and the status of the key control execution.

3.9. Control Documentation

For every control, an adequate documentation of the control evidence (information / data that is used as a basis for the control performance, sample methodology, documentation allowing traceability (audit trail) of date and scope of performed control activities, location of storage of the information, tracking of follow-ups, control results and names of the control owner and performer) has to be maintained.

The documented details shall enable an informed third party to fully understand the control performance with only limited prior knowledge of the process. The control owners are responsible to ensure proper control documentation, retention and archiving.

The control owner has to ensure that all control related documents (definition, changes, execution, and reporting of results) are retained in accordance with local retention requirements (reference is made to policy D-1109-00 Global Archiving Policy for physical and electronic documents).

Control documentation has to be made available to Internal and External Audit and relevant CRO units upon request.

Where the BaerControl tool is available, the documentation has to be captured and uploaded into the tool. Please note that only C1-C3 and P1-P3 data is allowed to be in the tool (reference is made to the JBG-2202-00 Information Classification Policy).

3.10. DE / OE Self-Assessment

On an annual basis, the local control owner performs a “self-assessment” to assess the design and operating effectiveness of their key controls based on specific criteria[11] to ensure appropriate quality of the controls. Where the assessment reveals that the design or operation of a control is ‘not effective’, appropriate measures have to be defined by the control owner to make the control effective again.

3.11. Quality Assurance of key controls linked to GMC

The Consolidated Supervision team in head office coordinates the quality assurance with regards to the implementation and execution of key controls linked to GMC applying a risk-based approach.

4. CONTROL IMPLEMENTATION IN THE LOCATIONS

In cases where local regulations prescribe more stringent or extensive requirements than those defined in this policy, the local regulations have priority. With respect to “Small Offices”, reference is made to the policy D-1184-00 Small Offices section “Local Corporate Governance Guidelines and Global Standards” and especially to its appendix.

For newly acquired entities with majority participation, a grace period of 12 months after closing date for the formal implementation of the control framework is granted, unless another timeline was agreed with a regulator. The full implementation of the relevant controls must be signed off by the entity and reported to the Consolidated Supervision team in head office.

Where change projects such as the implementation of a new tool, change of processes or frameworks have an impact on the controls, control owners are responsible to timely update their controls accordingly. At the same time, project leads are responsible to consider the ICF and potential changes as part of their projects.

5. GRACE PERIOD

Due to the substantial changes to the previous version a transition period applies until 31 December 2020. As of 1st January 2021, this policy fully applies to all new and existing control activities.

FS JBG-1007 Internal Control Framework

Reference to the Internal Controls Framework Guidelines:

- JBG-G-1007-00 Internal Control Framework Guideline
- JBG-G-1007-01 Guideline for 2nd LoD Controls

[11] Refer to section “Design and Operating Effectiveness Self-Assessment” of the JBG-G-1007-00 Internal Control Framework Guideline

APPENDIX

Abbreviations

GMC	Global Minimum Control
ICF	Internal Control Framework
LOD	Line of Defence
MORC	Monitoring & Operational Risk Control
RCSA	Risk-Control-Self-Assessment
RMF	Risk Management Framework
RTO	Risk Type Owner
RTOA	Risk Type Owner Assessment