



# Charter for Group Internal Audit

2017

Approved by the Chairman on behalf of  
the Board of Directors on 26 January 2017.

## Table of contents

1.	Introduction .....	3
1.1	GIA Charter .....	3
1.2	Purpose and objectives .....	3
2.	GIA's role in UBS's governance.....	3
2.1	Introduction .....	3
2.2	Independence and objectivity.....	3
2.3	Reporting line and supervision .....	3
3.	Scope, objectives and responsibilities .....	4
3.1	Scope .....	4
3.2	Objectives .....	4
3.3	Responsibilities .....	4
3.4	Authority .....	5
4.	Standards, organization and performance measurement .....	5
4.1	Standards .....	5
4.2	Organization .....	5
4.3	Performance measurement .....	5
5.	Annual review and entry into force .....	5
	Appendix: Performance criteria and measurement.....	6
	Position .....	6
	People .....	7
	Process .....	8
	Contact information .....	9

## 1. Introduction

### 1.1 GIA Charter

In line with the Organization Regulations (OR) of UBS Group AG, this charter describes the role, responsibilities and authorities as well as the scope, objectives and position of Group Internal Audit (GIA).

### 1.2 Purpose and objectives

GIA is an independent and objective function that supports both the firm in achieving its defined strategic, operational, financial and compliance objectives, and the Board of Directors (BoD) and its committees in discharging their governance responsibilities.

## 2. GIA's role in UBS's governance

### 2.1 Introduction

Effective risk management, control and governance processes are the responsibility of the respective business management and risk control functions, i.e. the first two "lines of defense". As the "third line of defense", GIA independently assesses whether risk management, control and governance processes are designed and operate sustainably and effectively. GIA also evaluates the independence of the risk control functions.

Remediating issues is the responsibility of management. GIA assures whether management has effectively and sustainably addressed relevant issues raised from all sources (i.e. issues rated 3 and above, self-identified by business management, by control functions (legal, compliance and risk), GIA, external audit or regulators).

The existence of internal audit does not relieve management of its responsibility regarding the risk management and control processes.

### 2.2 Independence and objectivity

GIA is independent in determining its activities (e.g. when defining audit scope and executing audit engagements). GIA reports are not subject to any instructions or restrictions, and its authority to audit is unrestricted.

To maintain objectivity, GIA has no operational responsibility or authority over any business activities, day-to-day risk management or control process.

### 2.3 Reporting line and supervision

The Head of GIA reports directly to the Chairman of the BoD. In addition, GIA has a functional reporting line to the Audit Committee. The Chairman, in conjunction with the Audit Committee, monitors GIA's performance in accordance with the terms of the OR. The Audit Committee (i) assesses the independence and the performance of GIA, in order to provide recommendations to the Chairman in relation to the effectiveness of both the Head of GIA and of GIA as an organization; (ii) assesses and approves the appropriateness of GIA's annual audit plan and audit objectives, including subsequent important amendments; and (iii) monitors GIA's discharge of its annual audit objectives, including being informed of the results of the annual audit plan. The Audit Committee is in regular contact with the Head of GIA.

## 3. Scope, objectives and responsibilities

### 3.1 Scope

GIA performs the internal auditing function for the entire UBS Group.

### 3.2 Objectives

To support the achievement of UBS's objectives, GIA independently, objectively and systematically assesses:

- effectiveness of processes to define strategy and risk appetite as well as the overall adherence to the approved strategy;
- effectiveness of governance processes;
- effectiveness of risk management, including whether risks are appropriately identified and managed;
- effectiveness of internal controls, specifically whether they are commensurate with the risks taken;
- soundness of the risk and control culture;
- effectiveness and sustainability of remediation activities, originating from any source;
- reliability and integrity of financial and operational information, i.e. whether activities are properly, accurately and completely recorded, and the quality of underlying data and models; and
- effectiveness of processes to comply with legal, regulatory and statutory requirements (such as the provisions of the Articles of Association) as well as with internal policies (including the OR), and contracts, i.e. assessing whether such requirements are met, and the adequacy of processes to sustainably meet them.

The Audit Committee may order special audits to be conducted. Separately, other BOD members, Committees or the Group CEO may also request such audits in consultation with the Audit Committee. The Audit Committee may also mandate third parties with the execution of special audits and informs GIA as appropriate.

### 3.3 Responsibilities

GIA is responsible for:

- Developing and maintaining an agile and flexible internal auditing function that considers the changing environment and emerging risks.
- Developing an annual audit plan based on an annual risk assessment, considering input from the business, senior management as well as the members of the Audit and the Risk Committees. The Annual Audit Objectives are approved by the Audit Committee after their discussion with GIA. The Chairman of the BoD, members of the Risk Committee and of the Group Executive Board (GEB) as well as further stakeholders receive a copy for their information.
- Continuously considering the firm's risk profile and audit universe, including new or emerging risks, business changes, new initiatives and business trends. Reviewing and assessing at least quarterly their impact on the audit plan. Subsequent important changes to the Annual Audit Objectives are approved by the Audit Committee.
- Implementing the approved annual audit plan (including any changes and special projects) and covering the audit universe in a risk-based 4-year audit cycle, i.e. to plan, conduct, report and assure individual audit engagements according to the procedures defined in the Audit Standards Manual.
- Implementing a risk-based approach to assure the effective and sustainable remediation of issues rated 3 and above from all sources.
- Issuing quarterly governance and annual activity reports providing a broad overview of significant audit results and key issues, control themes and trends based on individual audit results, continuous risk assessment and issue assurance results. The reports are provided to the Chairman of the BoD, members of the Audit and the Risk Committees, the GEB and other stakeholders.
- Coordinating its scope of work with external auditors to provide optimal audit coverage. GIA senior management regularly meets with the external auditors to exchange information and coordinate their activities. External auditors receive copies of all audit reports, the approved Annual Audit Objectives and the quarterly governance reports.
- Maintaining effective relationships with UBS's regulators, responding to their requirements and supporting them in carrying out their supervisory function regarding UBS. GIA provides UBS's main regulators with a copy of the approved Annual Audit Objectives, the quarterly governance and annual activity reports and, on request, copies of individual audit reports.
- Leveraging its own audit results with the activities of other control functions within UBS, while maintaining its independence.
- Maintaining and developing a professional audit team with sufficient knowledge, skills and experience to meet the requirements of this charter and future challenges.

### 3.4 Authority

GIA possesses unrestricted auditing rights within the UBS Group. At all times it has access to all accounts, books, records, systems, property and personnel to fulfill its auditing responsibilities.

The Head of GIA has open, direct and unrestricted access to the Chairman, to the Audit and the Risk Committees as well as to the Group CEO. The Head of GIA regularly meets with the Chairman of the BoD and participates in the meetings of the Audit and Risk Committees. Separately, the Head of GIA also regularly meets with the Group CEO and presents the quarterly governance and annual activity reports to the GEB.

GIA is authorized to obtain assistance of specialists from within or outside of UBS when necessary to achieve its objectives.

## 4. Standards, organization and performance measurement

### 4.1 Standards

GIA must adhere to the best professional and ethical practices, such as the mandatory elements of the International Professional Practices Framework<sup>1</sup> of Internal Auditing of the Institute of Internal Auditors, and must comply with all legal and regulatory requirements affecting an internal audit function in the jurisdictions in which it operates (e.g. the Swiss Banking Law, its Ordinance and the Circulars issued by FINMA).

GIA defines its policies, working procedures and methods in the Audit Standards Manual and related documents. Together, they provide comprehensive guidance regarding the internal auditing processes, such as the annual risk assessment and planning, individual audit engagement planning, execution, reporting, issue assurance as well as quality assurance and improvement programs and training requirements.

### 4.2 Organization

GIA maintains an adequate organization structure in compliance with the applicable regulations capable of effectively fulfilling its objectives. It is led by GIA's Executive Committee.

### 4.3 Performance measurement

Criteria against which GIA's performance is measured are included in the appendix to this charter.

## 5. Annual review and entry into force

GIA will review annually whether the purpose, authority, responsibility and performance criteria, as defined in this charter, continue to enable GIA to accomplish its role. The results of this assessment, which will include input from senior management as well as key measures agreed with the Audit and the Risk Committees, will be submitted to the Audit Committee for review and decision, together with possible proposals to amend the charter. The results of this assessment are also provided for information to the Risk Committee.

This charter has been approved by the Chairman on behalf of the BoD, based on the advice of the Audit Committee, and becomes effective as of 26 January 2017.

---

<sup>1</sup> Mandatory guidance of the IPPF:

- Core Principles for the Professional Practice of Internal Auditing
- Definition of Internal Auditing
- Code of Ethics
- International Standards for the Professional Practice of Internal Auditing (Standards)

## Appendix: Performance criteria and measurement

The Audit Committee measures GIA's overall success on whether or not GIA supported both the firm in achieving its defined strategic, operational, financial and compliance objectives, and the BoD and its committees in discharging their governance responsibilities, i.e. whether or not GIA did everything it could to avoid that our stakeholders were surprised by an unexpected significant loss or damage to the firm's reputation ("**no surprises aim**").

In assessing GIA, the Audit Committee may consider the overarching principles detailed in the "Aspiration / best practice" column of the table below, grouped into the dimensions Position, People and Process. The performance criteria / measurement are indicative of metrics that GIA uses to monitor its performance.

Aspiration / best practice	Performance criteria / measurement
<b>Position</b>	
<b>Mission</b>	
Be recognized by business leaders as more than a compliance function by providing quality challenge (e.g. by telling them what they did not already know, identifying root causes of breakdowns and opportunities for improving control design, or trends in risks and controls).	<ul style="list-style-type: none"> <li>– Annual stakeholder feedback through a questionnaire.</li> <li>– External quality assessment (at least every 5 years)</li> <li>– Assessment of Head of GIA through Chairman supported by Chair of Audit Committee</li> </ul>
Have a sound understanding of business strategy and the associated risks and be able and willing to challenge the control environment and infrastructure supporting the strategy. Be able to connect across one part of the organization to another.	<ul style="list-style-type: none"> <li>– Assessments / feedback from regulators</li> <li>– Internal Quality Assessment results</li> <li>– Attendance of respective relevant meetings at GEB, divisional and regional level</li> </ul>
Play an integral role in the governance structure (as the "third line of defense"), which is clearly aligned with stakeholders, clearly articulated in its mandate and widely understood throughout the firm.	
<b>Organization and structure</b>	
Be truly independent from the business and have clear and unfettered reporting into an appropriate BoD Committee and direct access to the Chairman of the BoD.	<ul style="list-style-type: none"> <li>– As granted by OR of the firm</li> </ul>
Be structured to maintain both independence and objectivity on the one hand and proximity to the business on the other in order to establish and maintain relationships with and comprehensive understanding of the business.	<ul style="list-style-type: none"> <li>– Alignment of GIA organization structure to that of the firm</li> <li>– Periodic stakeholder feedback</li> <li>– Regular external assessment</li> </ul>
<b>Stakeholders and services</b>	
Be characterized by proactively managing relationships with key stakeholders, e.g. the Head of GIA and direct reports should have direct and strong relationships with BoD members, business heads and senior management.	<ul style="list-style-type: none"> <li>– Periodic stakeholder feedback</li> <li>– Regular external assessment</li> </ul>
Be able to articulate to senior management through its activities the risks of their actions in a structured and balanced manner and provide credible recommendations to mitigate the risks.	<ul style="list-style-type: none"> <li>– Quarterly Governance Report</li> <li>– Periodic stakeholder feedback</li> <li>– Regular external assessment</li> </ul>
Regularly attend executive meetings to present audit findings, trends and current views, extending above and beyond the control environment.	<ul style="list-style-type: none"> <li>– Attendance of relevant meetings at GEB, divisional and regional level</li> </ul>
Have a presence in major governance and controlling bodies (e.g. risk and other committees).	<ul style="list-style-type: none"> <li>– Attendance of relevant meetings at GEB, divisional and regional level</li> </ul>
Maintain strong relationships with key external stakeholders (in particular, regulators and external auditors).	<ul style="list-style-type: none"> <li>– Feedback / assessments from regulators and external auditors</li> </ul>

Aspiration / best practice	Performance criteria / measurement
<b>Funding</b>	
Have no unreasonable budgetary constraints that limit the ability to deliver on its mandate, given the risk appetite of the organization.	<ul style="list-style-type: none"> <li>– Annual verification of alignment between audit plan / mandate and resources</li> <li>– Audit backlog due to resource constraints</li> </ul>
<b>Success criteria</b>	
Be subject to regular review of its effectiveness by the governing bodies to which it reports and be held accountable for its performance (with clear and measurable performance criteria).	<ul style="list-style-type: none"> <li>– Results of KPI analysis as defined in this document</li> </ul>
<b>People</b>	
<b>Competencies</b>	
Contain a diverse talent pool with a broad mix of skills and experience gained within internal audit and in business.	Qualitative measures: <ul style="list-style-type: none"> <li>– Stakeholder survey feedback</li> </ul>
Contain sufficient individuals who are senior and experienced enough, with sufficient business understanding to provide independent views and challenge the business on a broad array of topics.	Quantitative measures: <ul style="list-style-type: none"> <li>– Rate of internal transfers to / from business</li> <li>– Years of experience in financial industry</li> <li>– Years of audit experience</li> </ul>
Contain recognized (by the business) experts in governance, control and risk mitigation.	<ul style="list-style-type: none"> <li>– Years with UBS</li> <li>– Seniority (rank) mix</li> </ul>
Have effective means of identifying skills and competencies required to deliver its annual plan, identifying and filling gaps and being responsive to the rapidly changing risk profile of the firm.	<ul style="list-style-type: none"> <li>– Availability of tools and processes to systematically assess existing skills and contrast them with requirement to fulfil mandate / 4-year audit plan</li> <li>– Progress achieved in eliminating identified gaps</li> </ul>
Be characterized by a willingness to take ownership, responsibility for their work and ability to engage with the business actively before, during and after the audit.	<ul style="list-style-type: none"> <li>– Stakeholder survey feedback</li> <li>– Business feedback through challenge sessions</li> <li>– Staff survey results</li> </ul>
<b>Staffing strategy</b>	
Be forward thinking in its medium to longer term staffing strategy (e.g. by taking into account growth areas in the business, new and emerging risk areas).	<ul style="list-style-type: none"> <li>– Existence of staffing strategy (part of strategy document)</li> <li>– Ability to systematically measure and assess expertise in risks and products</li> </ul>
Attract and retain quality professionals from within and outside UBS by providing value-adding career development opportunities to top talents.	<ul style="list-style-type: none"> <li>– Headcount numbers as close as possible to target level at all time (HC report)</li> <li>– Low fluctuation rates vs. firm average and peers, specifically for regretted leavers</li> <li>– Ratio of external / internal joiners</li> <li>– Staff survey results</li> </ul>
<b>Talent / career development</b>	
Develop its personnel through comprehensive training and development and advanced knowledge management.	<ul style="list-style-type: none"> <li>– Breadth and scope of training offerings (GIA, firm internal, external)</li> <li>– Number of training hours consumed</li> <li>– Existence and quality of succession list, including elapsed time to fill line management vacancies</li> <li>– Rate of positions filled with succession candidates</li> <li>– Completion rate of Individual Development Plans</li> <li>– Staff survey results</li> </ul>
<b>Reward / appraisal</b>	
Offer competitive remuneration policies based on the achievement of transparent performance metrics (e.g. based on quality of work and impact upon the business, and not simply delivery against plan and business performance).	<ul style="list-style-type: none"> <li>– Existence of transparent performance targets which combine qualitative and quantitative performance aspects</li> <li>– Strong compensation differentiation, fully aligned with performance assessment</li> <li>– Market comparisons</li> </ul>

Aspiration / best practice	Performance criteria / measurement
<b>Process</b>	
<b>Risk assessment, planning, execution and assurance</b>	
Maintain a medium-term strategy document that defines the high-level direction the function intends to develop in light of the firm's risk profile and market environment.	<ul style="list-style-type: none"> <li>– Availability and annual update of strategy document</li> </ul>
Be forward looking in its risk assessment process, through extensive use of continuous risk assessment processes, with strong awareness of the external environment, and be flexible in adapting its planned activities, sometimes rapidly, in the face of new and emerging risks.	<ul style="list-style-type: none"> <li>– Existence and quality of execution of respective processes</li> <li>– Number of unplanned audits / targeted reviews and their results</li> </ul>
Develop annual audit objectives based on a risk assessment accepted and approved by GIA's governing bodies. Maintain a risk-based 4-year plan that covers the entire audit universe and is driven by a bottom-up micro risk assessment of the firm's individual businesses.	<ul style="list-style-type: none"> <li>– Achieve annual audit plan (subject to risk-driven amendments)</li> <li>– Achieve targeted audit cycle across full audit universe</li> <li>– Results of backlog analysis</li> </ul>
Continually reflect on and adapt processes to ensure that they remain fresh and relevant, through integrated quality assurance and learning programs.	<ul style="list-style-type: none"> <li>– Existence of continuous improvement processes, including platforms for staff participation and respective PMM targets</li> <li>– Improvement of metrics</li> <li>– Feedback from Internal Quality Assurance function</li> </ul>
Conduct audit activities to obtain a variety of views of and form opinions on the control environment (e.g. within and across business units, functions, processes, and jurisdictions).	<ul style="list-style-type: none"> <li>– Number of audit reviews completed</li> <li>– Number of themed and Front-to-Back audits</li> <li>– Number of group-wide audits</li> </ul>
Produce reports (for individual audits and for governance bodies) that identify both root causes and consequences of issues and are delivered on a timely basis with clarity and impact.	<p>Qualitative measures:</p> <ul style="list-style-type: none"> <li>– Completing audits according to GIA's standards and guidance, measured by IQA</li> <li>– Quality and impact measured by internal stakeholder survey, feedback / assessment from regulators and external auditors as well as periodic external assessment</li> </ul> <p>Quantitative measures:</p> <ul style="list-style-type: none"> <li>– Issue audit reports 25 business days after completion of audit fieldwork (on average)</li> <li>– Agree actions with management that address significant issues promptly, tactical measures completed within three months</li> </ul>
Maintain effective Issue Assurance processes to evaluate the remediation of issues raised with a focus on the sustainability of remediated controls.	<p>Achieve operating effectiveness criteria:</p> <ul style="list-style-type: none"> <li>– For issues rated 3, 4 or 5, review actions and issues closed by management during the month following the month of closure (desktop review)</li> <li>– For issues rated 4 or 5, perform an in-depth review (including testing) to verify operating effectiveness and sustainability; to provide a sufficient sample period for testing, this activity should ideally be completed once 90 calendar days have elapsed from the point of closure by the issue / action owner and can also be included as part of a planned audit in the area concerned</li> <li>– Determine on a case-by-case basis whether a sustainability review will be performed within 6 to 12 months after issue closure</li> <li>– For Group Significant Operational Risk Issues (GSORIs) and Divisional Operational Significant Issues (DSORIs), provide assurance according to predefined assurance plans</li> </ul>
Apply rapid and effective processes to escalate issues that require senior management attention.	<ul style="list-style-type: none"> <li>– GIA to inform management as soon as a significant issue is identified</li> <li>– Management's response required within 10 days of being informed</li> </ul>



Aspiration / best practice	Performance criteria / measurement
<b>Technology</b>	
Leverage technology throughout all audit and administrative processes with a goal to maximize efficiency and improve audit effectiveness.	<ul style="list-style-type: none"> <li>– Systematic self-assessment (Process Board)</li> <li>– Staff survey feedback</li> <li>– Trend in efficiency measures (e.g. number of audits, PD consumption)</li> </ul>
Leverage advanced data analytics in audit lifecycle (scoping, sampling and testing), in continuous risk assessment and risk analysis.	<ul style="list-style-type: none"> <li>– Rate of advanced analytics used in audit execution, ratio of full population testing</li> <li>– Ability to identify risk trends early</li> </ul>
<b>Performance measurement / quality assurance</b>	
Define and maintain a variety of performance measurements that are regularly reviewed and acted upon.	<p>Qualitative targets:</p> <ul style="list-style-type: none"> <li>– Availability and quality of periodic MIS reports covering all KPIs, includes: <ul style="list-style-type: none"> <li>– Operate within agreed financial budgets, incl. within defined headcount targets</li> <li>– Resource allocation targets between audit, audit-related and non-audit activities</li> <li>– On average, complete audits in line with resource plans and budgets for both elapsed time and effort spent</li> </ul> </li> </ul>
Undertake regular self-review and monitor development in internal audit functions of peer organizations.	<ul style="list-style-type: none"> <li>– Have dedicated Internal Quality Assurance function</li> <li>– Perform regular peer comparison analytics (e.g. G25 comparison)</li> </ul>

## Contact information

Alan Wehrenberg  
Head of Group Internal Audit

5 Broadgate  
EC2M 2QS London  
United Kingdom

+44 20756 78048  
[alan.wehrenberg@ubs.com](mailto:alan.wehrenberg@ubs.com)

[www.ubs.com](http://www.ubs.com)

