
Internal Audit & Risk Charter

Introduction

This document contains the Internal Audit & Risk Functional Charter for Marks & Spencer plc (M&S) and defines the purpose, authority, responsibilities and position of the Internal Audit & Risk (IA&R) function.

Role

IA&R provides an independent assurance function which supports the Audit & Risk Committee (A&RC) in the discharge of its responsibility to ensure that there is:

- an adequate and effective system of internal controls and risk management;
- timely follow up of control deficiencies; and
- appropriate safeguarding of assets, activities and interests of the Group.

IA&R works with the business to help achieve its strategic objectives, through improving the overall control environment, and assisting in identifying emerging risks requiring mitigation.

From a risk perspective, IA&R's role is to establish the risk management framework, related policies, procedures and guidance, provide risk oversight across the Group and report on the risk profile to senior management and the Board.

Remit and Types of Services

The remit of the function incorporates all activities of the Group and considers all types of risk, including operational, financial, fraud, compliance, strategic, ethical, social, governance and brand risk.

The scope of the function encompasses, but is not limited to, objective examinations of evidence to provide independent assurance and advisory services to the A&RC and management on the adequacy and effectiveness of governance, risk management, and control processes for the Group.

The nature and scope of advisory services may be agreed with the party requesting the service, provided the internal audit function does not assume management responsibility.

The function also supports M&S in fulfilling its corporate governance requirements to provide a confidential reporting mechanism for colleagues and the investigation of matters raised.

The function may carry out special investigations, including investigations into suspected or actual frauds, as requested by the A&RC or management.

Professionalism

Members of the function must exhibit the highest level of professional objectivity in gathering, evaluating and communicating information about the activity or process being examined. In performing their duties, the team must always exercise due professional care.

The IA&R function will adhere to the standards set by the Institute of Internal Auditors (including the Definition of Internal Auditing, the Code of Practice, the Code of Ethics and the International Professional Practices Framework) and to the Group's relevant policies and procedures, including the Code of Conduct and Behaviours.

Functional standards and ways of working are set out in the M&S Internal Audit Methodology and Guidance manual and the Group Risk Management Policy and Guidelines (which are subject to periodic review and update).

Authority and Access

IA&R derives its authority from the Board through the A&RC. The A&RC grants IA&R the mandate to provide the A&RC, Board and senior management with objective assurance, advice and insight. IA&R is authorised full, free and unrestricted access to all the Group's records, physical properties, and personnel pertinent to carrying out any engagement. Authority for access is vested in the Head of Internal Audit & Risk (HIAR) who is responsible for making sure this authority is exercised responsibly.

All colleagues are requested to assist IA&R in fulfilling its roles and responsibilities. IA&R will also have free and unrestricted access to the Board. In return, IA&R will operate with strict accountability for confidentiality and safeguarding records and information.

In addition, the HIAR:

- should be informed promptly by management of any significant potential or actual control failures (including 'whistleblower' related incidents or those identified by external third parties);
- should be invited to attend any committee meeting relevant to the function's responsibilities; and
- should be informed promptly by management of any major corporate activity that may have a material impact on the risk and control environment of the Group.

Internal Audit & Risk Charter (cont.)

Independence and Objectivity

The independence of IA&R from day-to-day line management responsibility is fundamental to its ability to deliver objective coverage of all parts of the Group. IA&R must have an impartial, unbiased attitude and avoid any conflict of interest.

IA&R will remain free from interference by any element in the organisation, including matters of audit selection, scope, procedures, frequency, timing or report content to permit maintenance of a necessary independent and objective mental attitude; if necessary, the HIAR must disclose any such interference and its related implications to the Audit Committee.

Members of the function will have no direct operational responsibility or authority over any of the activities audited and will not implement internal controls, develop procedures, install systems, prepare records, or engage in any other activity that may impair their judgment or compromise their independence.

Should a colleague transfer from the business into IA&R, safeguards will be formally established to ensure any audits of the areas, department or activities associated with their previous role are not impacted by a conflict of interest and IA&R's impartiality/independence is not affected.

While the HIAR has responsibility for overseeing the facilitation of risk management and reporting processes across the Group, the individual is not responsible for setting risk appetite, identifying and prioritising risks, or taking decisions on risk mitigation, acceptance or management.

IA&R colleagues with real or perceived conflicts of interest must inform the HIAR as soon as these issues become apparent so appropriate safeguards can be put in place. The HIAR will confirm to the A&RC, at least annually, the organisational independence of the internal audit activity.

The remuneration of the HIAR and the team will be subject to periodic review by the A&RC Chair and the Remuneration Committee.

Once the tenure of the HIAR exceeds 7 years, the A&RC will formally consider the HIAR's continued independence and objectivity on an annual basis.

Reporting Lines

To maintain organisational independence, the HIAR will report functionally to the A&RC and administratively (i.e. day to day operations) to the Chief Financial Officer. The HIAR will have unrestricted access to the A&RC Chair. The A&RC will approve all decisions regarding the appointment or removal of the HIAR.

Corporate Responsibilities

Management

- Identifying, understanding and managing risks effectively, in line with Group Risk Appetite;
- Maintaining a sound system of internal controls over people, processes and systems and key risks facing the business and its operations, the existence of IA&R does not relieve them of this responsibility;
- Taking appropriate and timely action in response to audit findings;
- Fraud prevention and detection;
- Facilitate IA&R processes by engaging with IA&R, providing info requested on timely basis, attending opening and closing meetings and ensuring relevant colleagues are available during audit engagements;
- Facilitate work of IA&R by providing explanations for actions and unimpeded and timely access to colleagues and records; and
- Where information is of particular sensitivity, management may request that access to the information be restricted only to the HIAR.

Head of Internal Audit and Risk

The HIAR is accountable for all aspects of delivery associated with:

- group internal audit;
- risk management and reporting, including coordinating meetings and agendas for the Executive Risk Committee;
- oversight and management of the whistleblowing process;
- monitoring of reporting and compliance with business integrity matters, such as gifts & hospitality;

Internal Audit & Risk Charter (cont.)

Corporate Responsibilities (cont.)

Head of Internal Audit and Risk (cont.)

- undertaking targeted investigations for issues of significance at group level;
- working with the broader risk and assurance community across the business and
- engaging with the audit and risk teams at our joint venture operations.

Full details of the HIAR's accountabilities and responsibilities are outlined in the HIAR remit.

Audit Committee

- A&RC responsibilities, in terms of evaluating and supporting IA&R, are outlined in the A&RC Terms of Reference.
- In addition, the objectives of the HIAR, and the team, will be approved by the A&RC Chair.

Reporting and Monitoring

The HIAR will report periodically to the A&RC on:

- The annual functional budget and resource plan;
- The results of audit reviews;
- The status of management action plans to address identified control gaps;
- The status of the overall control environment within the Group based on the findings of work completed;
- Progress against the audit plan including proposed variations and additions for A&RC approval;
- The risk management process, the Group's Principal Risks and uncertainties, emerging risks and ad hoc risk updates as required;
- The fraud risk management framework, significant fraud risks, status of agreed actions, potential deficiencies and identified frauds;
- The number and nature of confidential whistleblower contacts received, and the significant whistleblower claims, theft and fraud investigated within the Group;
- Gifts and hospitality offered or accepted by business colleagues; and
- The sufficiency of function resources, in terms of both capacity and skill set.

Periodic Assessment

IA&R will be subject to a formal functional effectiveness review, supported by an external third party, at least every five years, with results reported to the A&RC. In addition, the A&RC will formally consider functional performance on a periodic basis and at least once every three years.

In between the external assessments, IA&R will maintain a quality assurance and improvement programme, including evaluation of conformance with the Standards and assessing efficiency and effectiveness to identify opportunities for improvement. The HIAR will communicate outcomes of the programme to the A&RC.

Approval

The IA&R Functional Charter will be reviewed and approved annually by the Audit Committee.

Changes to the Charter

Some circumstances may justify changes to the IA&R Functional Charter, to be discussed with the A&RC outside of the annual review cycle. Such circumstances may include but are not limited to:

- A significant acquisition or reorganisation within the Group.
- Significant changes in the HIAR, A&RC, and/or senior management.
- Significant changes to the Group's strategies, objectives, risk profile, or the environment in which the business operates.
- New laws or regulations that may affect the nature and/or scope of internal audit services.
- A significant change in the Global Internal Audit Standards or to regulatory or best practice expectations specifically for internal audit. For example, the Internal Audit Code of Practice.

Head of Internal Audit & Risk Remit

Head of Internal Audit & Risk Remit

Job title	Head of Internal Audit & Risk ('HIAR')
Business area	Finance
Report to	Audit & Risk Committee (A&RC) Chair, dotted line to the CFO
Reward level	F
Direct reports	1 (team of 16)

Key Accountabilities

The HIAR is accountable for all aspects of delivery associated with:

- group internal audit;
- risk management and reporting;
- oversight and management of the whistleblowing process;
- monitoring of reporting and compliance with business integrity matters, such as gifts & hospitality;
- undertaking targeted investigations for issues of significance at group level;
- working with the broader risk and assurance community across the business including Group Asset Protection; and
- engaging with the audit and risk teams at our joint venture operations.

The remit of the function incorporates all wholly owned activities of the Group and considers all types of risk, including operational, financial, fraud, compliance, strategic, ethical, social, governance and brand risk.

The function derives its authority from the Board through the A&RC and is authorised full, free and unrestricted access to all the Group's records, physical properties, and personnel pertinent to carrying out any engagement.

Across this range of activities, the key responsibilities are:

Cross-functional

- Setting and delivering a functional strategy to support ongoing delivery and a programme of continuous improvement across all areas of responsibility;
- Working closely with the CFO to promote an effective governance, risk management and controls culture across the business;
- Providing monthly updates, and, where needed, ad hoc reports, on functional activities, progress and emerging issues to the CEO and Executive Committee;
- Providing proactive support and advice to the business on all matters linked to risk, control and assurance, mindful of the need to maintain the function's independence.
- Working effectively as part of a cross-business team to support business compliance with the UK Corporate Governance Code, including forthcoming provision 29 requirements;
- Maintaining effective relationships with other control and assurance functions to minimise duplication of effort and share learnings and best practice;
- Maintaining a professional, capable team, supported by a co-source model, that has sufficient knowledge, skills and experience to carry out all required tasks;
- Ensuring compliance with the business' people & performance management processes;
- Functional budget setting and cost management;
- Managing and reporting on functional independence and other requirements to comply with the IIA standards; and
- Engaging effectively with the group's external audit provider.

Internal audit

- Maintaining the M&S Internal Audit Methodology & Guidance manual;
- Developing a risk based, flexible and commercially focused annual audit plan, considering the business risk profile, input of senior management, alignment with the audit universe, and incorporation of external perspectives for review and approval by the A&RC;

Head of Internal Audit & Risk Remit (cont.)

Internal audit (cont.)

- Monitoring the plan's continued relevance and making recommendations on proposed additions, deletions and deferrals;
- Executing the audit plan, adhering to the defined audit methodology and reporting findings to the A&RC, CEO, CFO and other relevant senior management;
- Tracking and follow up of management actions to address identified control gaps, and bringing to management's attention instances where risks are not sufficiently mitigated;
- Developing data analytics to help identify potential control weaknesses and anomalies as an integrated part of the core audit delivery and as standalone pieces of work;
- Quarterly reporting of gifts & hospitality across the business and monitoring of periodic supplier submissions;
- Reporting annually on thematic audit/control issues identified;
- Establishing an effective quality assurance and improvement programme to ensure the function's judgements and observations are adequately supported and evidenced;
- Managing all aspects of the co-source service provider's activities; and
- Reporting periodically to the A&RC on:
 - The annual functional budget and resource plan;
 - Progress against the audit plan including proposed changes for A&RC approval;
 - The results of all completed audit reviews;
 - The status of management action plans to address identified control gaps;
 - The status of the overall control environment within the Group based on the findings of work completed as part of the audit plan and other corporate activities;
 - Significant control or integrity related issues, including fraud, whistleblowing and other irregularities that are identified; and
 - Functional performance.

Risk management

- Maintaining the M&S Group Risk Management Policy and Guidelines;
- Maintaining a set of risk appetite statements for Board approval, including coordinating and reporting of key risk indicators linked to these;
- Coordinating risk reporting activities across the business and monitoring the quality, completeness, validity and severity of reported risk information;
- Maintaining the business' risk reporting repository;
- Conducting risk analysis at Group level, including undertaking risk consolidation, calibration, aggregation and trend analysis;
- Tracking and follow up of management identified actions to improve risk management, and bringing to management's attention instances where risks are not sufficiently mitigated;
- Supporting and challenging the business and functional teams on periodic reporting to the A&RC on their management of risk, control, compliance and assurance matters;
- Coordinating meetings and agendas for the Executive Risk Committee, including managing updates on specific actions arising from discussions;
- Producing group-wide risk reporting for the Executive Directors, the Executive Committee, Executive Risk Committee, A&RC and Board;
- Drafting all external disclosures on risk management for A&RC approval; and
- Reporting periodically to the A&RC on:
 - Updates to the risk management policy;
 - The annual risk appetite refresh;
 - Half year and full year compliance with the risk management policy and business outputs;
 - Business performance on implementing risk mitigation actions;
 - The proposed external disclosures for interim and year end reporting; and
 - Compliance reports setting out key indicators of business performance.

Head of Internal Audit & Risk Remit (cont.)

Whistleblowing

- Overseeing the business whistleblowing process, ensuring contacts are investigated through the most appropriate channels, including IA&R as required;
- Reporting to the Executive Committee and A&RC on significant whistleblower claims and their resolution;
- Managing all aspects of the external confidential reporting service provider's activities; and
- Reporting periodically to the A&RC on the number and nature of confidential whistleblower contacts received, significant whistleblower claims, trend analysis, resolution of matters raised and maintenance of the support process.

Fraud risk management

- Working with a cross-functional team to oversee the Group's fraud risk framework and facilitation of fraud risk management; and
- Reporting periodically to the A&RC on:
 - The fraud risk management framework;
 - Significant fraud risks;
 - Status of agreed actions;
 - Potential deficiencies; and
 - Any material/significant identified frauds.

Joint Ventures ('JVs')

- Liaising with risk, internal audit and controls teams at our JVs;
- Attendance at JV audit committee meetings;
- Monitoring outputs of risk, control and assurance activity at JVs;

Joint Ventures (cont.)

- Completion of agreed audit reviews to support both the local audit teams and as part of the M&S plan delivery; and
- Reporting the outcome of the above activities to the A&RC.