Internal Audit & Risk Functional Charter – approved at Sept '23 AC

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 Committee 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 improve the overall control environment and to assist in identifying emerging risks requiring mitigation.

Remit

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 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 Audit Committee 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 Standards for the Professional Practice of Internal Auditing) 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 & 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 Audit Committee. 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.

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.

Internal Audit & Risk Functional Charter (cont.)

Independence and Objectivity (cont.)

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 Audit Committee, 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 Audit Committee Chair and the Remuneration Committee.

Reporting Lines

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

Corporate Responsibilities

Management

- Identifying, understanding and managing risks effectively;
- 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;
- 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

- Setting and delivering a functional strategy to support continuous functional improvement;
- Developing a risk based, flexible and commercially focused annual audit plan, considering the input of senior management and review of the audit universe, for review and approval by the Audit Committee. The plan will incorporate both existing business processes and systems and those under development (programme assurance);
- Executing the audit plan utilising a risk based audit methodology and reporting findings to the Audit Committee, CEO, CFO and other relevant senior management;
- Reporting annually on any thematic issues identified and actions being taken by management to mitigate risks associated with these issues;
- Developing data analytics to help identify potential control weaknesses and anomalies;
- Maintaining the M&S Internal Audit Methodology & Guidance manual and Group Risk Management Policy and Guidelines;
- Establishing an effective quality assurance and improvement programme to ensure the function's judgements and observations are adequately supported and evidenced;
- Ensuring the 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 through the effective and timely completion of agreed actions;

Internal Audit & Risk Functional Charter (cont.)

Corporate Responsibilities (cont.)

Head of Internal Audit and Risk (cont.)

- Working closely with the CFO, and maintaining effective relationships across the business, to promote good governance, risk management and controls across the business;
- Overseeing the facilitation of risk management and reporting processes across the Group;
- Working with a cross-functional team to oversee the Group's fraud risk framework and facilitation of fraud risk management and reporting processes;
- Collaborate with relevant teams across the business on the Audit & Assurance Policy development, implementation, and associated reporting;
- Overseeing the confidential reporting process, ensuring contacts are investigated through the most appropriate channels, including IA&R as required, and coordinating reports to the Audit Committee on significant whistleblower claims, theft and fraud investigated within the Group;
- Quarterly reporting of gifts and hospitality;
- Providing proactive advice to the business on risk management and controls, within the boundaries of the function's independence, to support the continuous improvement of the control environment;
- Maintaining a professional audit staff that, together with external resources utilised, has sufficient knowledge, skills and experience to carry out the audit plan;
- Maintaining effective relationships with other control and assurance functions (including control and compliance functions within the Group and the external auditors) to minimise duplication of effort and share learnings and best practice; and
- Liaising with the Audit Committee, internal audit and control functions of Joint Ventures to obtain assurance that risks are sufficiently mitigated (where possible).

Audit Committee

- Audit Committee responsibilities, in terms of evaluating the effectiveness of, and supporting, the IA&R function, are outlined in the Audit Committee Terms of Reference.

Reporting and Monitoring

The HIAR will report periodically to the Audit Committee 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 Audit Committee 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.

In addition, the objectives of the HIAR and the team will be reviewed and approved by the Audit Committee Chair.

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 Audit Committee. In addition, the Audit Committee will formally consider functional performance on a periodic basis and at least once every three years.

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

Approval

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