# S&P Global Ratings' Internal Control Structure

## Overview

S&P Global Ratings manages and mitigates regulatory, compliance, and operational risk related to the determination and dissemination of Credit Ratings, Ancillary Services and Other Services through an internal control structure. Regulatory risk includes the failure to effectively respond to a change in laws and regulations that may impact the business of S&P Global Ratings. Compliance risk includes exposure to legal and financial risk for failure to follow laws and regulations and internal policies and procedures. Operational risk includes risk resulting from failed procedures and/or systems. In addition, S&P Global Ratings also manages other risks such as strategic and reputational risk, which may result or increase from regulatory, compliance or operational risk.

S&P Global Ratings has a balanced approach to risk management. Risk is mitigated to an acceptable level within established organizational risk appetites and tolerances while supporting the achievement of operational and strategic goals.

In addition, the internal control structure at S&P Global Ratings ensures that S&P Global Ratings complies with laws and regulations that govern credit rating agencies, including establishing, maintaining, enforcing and documenting an effective internal control structure that governs the implementation of and adherence to policies, procedures, and methodologies for determining Credit Ratings. The internal control structure is intended to provide S&P Global Ratings' executive management and its applicable boards of directors ("Boards"), with reasonable assurance that S&P Global Ratings and its Employees are in compliance with laws, regulatory requirements, and internal policies and procedures.

The internal control structure at S&P Global Ratings also covers operational resilience and works to ensure that S&P Global Ratings maintains critical operations through a disruption, and prevents, adapts and responds to, recovers and learns from operational disruptions.

The S&P Global Ratings internal control structure, which is aligned to the Committee of Sponsoring Organizations of the Treadway Commission ("COSO") published framework for internal control, consists of an internal control framework and control functions. The control functions are separate from the activities they are assigned to monitor, audit or control.

S&P Global Ratings operationalizes the internal control structure through three lines of defense. The first line of defense, composed of S&P Global Ratings' primary business and operations functions, owns and manages risks including the effectiveness of the internal control structure. The second line of defense, primarily provided by S&P Global Ratings' risk and compliance functions, provides oversight and challenge to the first line of defense to ensure compliance with laws and regulations, internal policies or prescribed best practices and facilitates and monitors the implementation of effective risk management practices. S&P Global Ratings also leverages control functions of S&P Global Inc. ("SPGI"), including the information security and corporate risk functions. The third line of defense, composed of the internal audit function of SPGI and independent from S&P Global Ratings, provides independent assurance on the effectiveness of governance, risk management, and internal control.

## S&P Global Ratings' Internal Control Structure

Management of S&P Global Ratings conducts periodic assessment of the effectiveness of the internal control structure and is accountable for addressing issues in the internal control structure that are identified as a result of these assessments. As part of the periodic assessment process, management develops and implements action plans describing how and when issues that constitute deficiencies in the internal control structure will be addressed and provides periodic updates on the progress of remediation efforts.

As required by certain laws and regulations, S&P Global Ratings submits an annual report to applicable regulators containing management's assessment of the effectiveness of the internal control structure governing the implementation of and adherence to policies, procedures, and methodologies for determining Credit Ratings.

Oversight of risk and internal control at S&P Global Ratings is provided through formalized governance mechanisms that include the Boards, the Global Executive Risk Committee, the Global Risk and Compliance Committee and the Controls Working Group. The Boards oversee the establishment, maintenance, and enforcement of policies, procedures and methodologies for determining Credit Ratings and managing and disclosing potential conflicts of interest and monitor the effectiveness of the internal control structure. The Global Executive Risk Committee provides management oversight of the identification, measurement, monitoring, mitigation, and reporting of risks across S&P Global Ratings and promotes a strong culture of risk management, compliance and control. The Global Risk and Compliance Committee reports and advises executive management on risk, compliance, regulatory and control-related matters across all regions in which S&P Global Ratings operates. The Controls Working Group provides oversight of the internal control structure including making the final determination of deficiencies in the internal control structure.

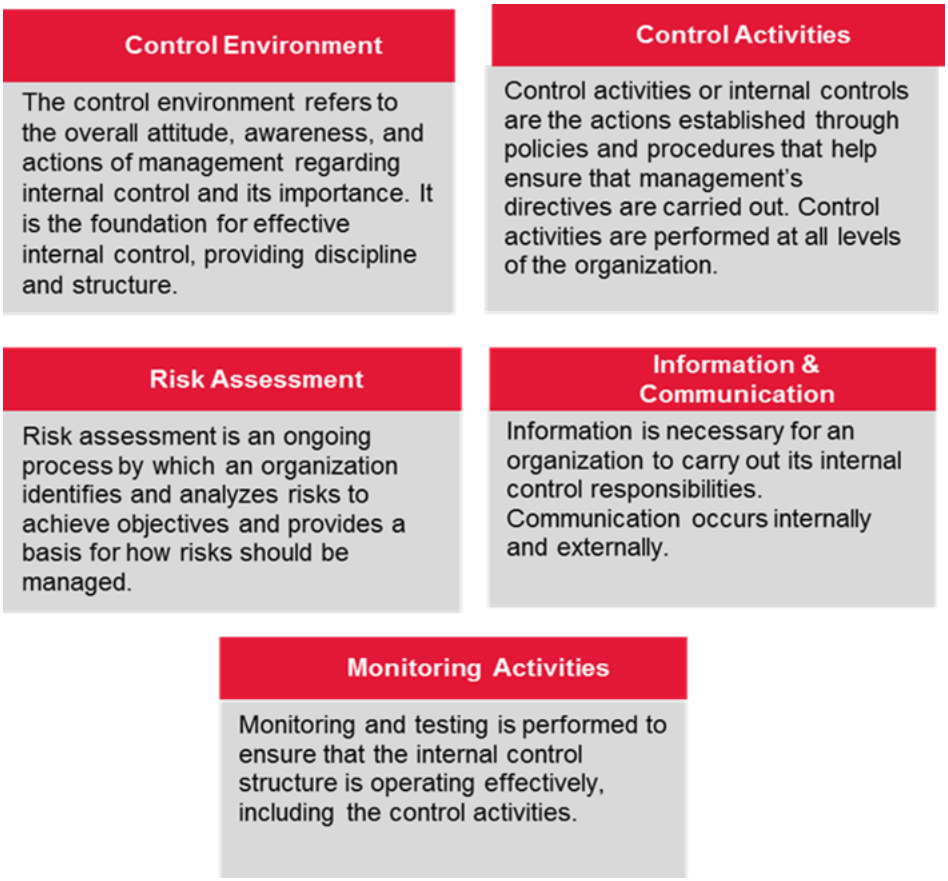
S&P Global Ratings, as a division of SPGI, escalates risk matters in accordance with the requirements of SPGI's risk management framework to allow for effective management and oversight of risk at the enterprise level. S&P Global Ratings' risk management processes are aligned with the requirements of SPGI's risk management framework.

### Description of the Internal Control Framework

S&P Global Ratings internal control framework consists of five interrelated components as defined below. This framework is used to manage risks that S&P Global Ratings faces, including Regulatory and Compliance Risk, Methodology and Analytical Process Risk, Third Party Risk, and Technology and Cybersecurity Risk. Every individual in the organization has a role in effecting internal control. Roles vary in responsibility and level of involvement, as defined in the S&P Global Ratings Risk Management Policy.

The internal control framework is operationalized across the division through common risk and internal control processes that are supported by specific risk and control assessments as necessary. Within the internal control framework, S&P Global Ratings has adopted specific principles aligned by component to ensure that adequate and effective internal control is in place to mitigate risk and that these controls

are applied consistently throughout the division. Periodically an evaluation of whether these principles are present and functioning is performed.




The following key processes are in place within S&P Global Ratings in support of the internal control framework:

- Monitoring risk appetite statements and tolerances
- Top Risk Assessment
- Regional risk discussions and quarterly global risk review
- Annual Management Assessment related to determining credit ratings
- Specific risk and control assessments (e.g. Vendor and Affiliate, Data Quality, IT Applications, Cybersecurity)
- Risk-based control testing
- Quarterly issue review to determine if a deficiency in the internal control structure exists
- Quarterly risk and internal control reporting to the Global Risk and Compliance Committee, Global Executive Risk Committee and the Boards
- Periodic regulatory reporting on risk and internal control
- Maintenance of a process, risk and control inventory.

## Description of Control Functions

The following organizational functions support S&P Global Ratings' internal control structure and are further described below:

- In-Business Control
- Compliance and Risk Department
- SPGI Global Risk and Corporate Compliance
- SPGI Information Security
- SPGI Internal Audit

### In-Business Control

In-Business Control ("IBC") is a group within the first line of defense that assists the Analytical practices, Operations, Data, and Technology functions in performing risk and internal control activities to mitigate risk in S&P Global Ratings. IBC ensures that controls are embedded into processes and solutions to ensure quality and adherence to regulation and internal policies and confirms that controls are designed and operating effectively through monitoring and testing. IBC works with management to identify, assess, and monitor risk in their departments by considering key risk indicators and other information, such as incidents and issues that are self-identified or identified by independent reviews. IBC ensures that issues are escalated and management's responses to risk and control issues are appropriate and mitigating actions are completed on a timely basis.

IBC works closely with the Risk and Internal Control Function within the Compliance and Risk Department to provide risk reporting to senior management and the Boards; and to enhance risk processes and the internal control structure.

IBC reports to the Global Head of Analytical Business Operations and Controls and has the following responsibilities:

- Practice Area/Department aligned In-Business Control Officers – partner with other first line departments and colleagues to implement the internal control structure; assist in day-to-day risk and internal control activities including design and implementation of control activities; perform risk and control assessments and ensure remediation of control issues.
- IBC Operations - manage key risk-related processes that span across the Ratings organization including error forums, application access management and business continuity management.
- Vendor & Affiliate Management – assess and monitor third party risk including affiliates.
- IBC Reporting/Analytics & Risk/Control Standards – develop standards for conducting risk/control assessment and build reporting capabilities to support the needs of IBC teams and first line stakeholders.

**Compliance and Risk Department**

The Compliance and Risk Department is headed by the Global Chief Risk and Compliance Officer ("GRCO"), who reports to the S&P Global Ratings President. The Compliance and Risk Department is responsible for monitoring and reporting on the compliance of S&P Global Ratings and its employees with its regulatory obligations. The Compliance and Risk Department is also responsible for ensuring that the internal control structure is operationalized across the division.

Risks and issues are identified through timely monitoring and assessment activities performed by several functions. The GRCO manages the Compliance function, the Risk and Internal Control function, and the Analytic Quality and Validation function. These second line functions support adherence to global and local regulatory requirements as well as to S&P Global Ratings' policies and procedures. The second line functions report periodically and ad hoc to various stakeholders including the Boards, the Global Executive Risk Committee, the Global Risk and Compliance Committee and the SPGI Executive Risk Management Committee.

Compliance Function Structure and Responsibilities

The Compliance function's structure and approach are grounded in three pillars:

- Advisory: Day-to-day advice, policy violation investigations and discipline, advising on and overseeing policy changes, development and implementation of formal and ad hoc training, conducted by Covering Compliance Officers and the Global Matrix Group.
- Regulatory: Maintaining and managing regulatory relationships and interactions, exam management and coordination, regulatory filings, regulatory remediation oversight, and regulatory reporting, conducted by the Covering Compliance teams, Exam Management team and Regulatory Coordination team.
- Monitoring: Periodic and dynamic compliance examinations, continuous and periodic monitoring, surveillance, conflicts controls, and metrics reporting, conducted by the Control, Monitoring and Examinations team.

To achieve its mission, the Compliance function is organized into the following functions:

- Covering Compliance
- Control, Monitoring and Examinations
- Global Regulatory Coordination
- Global Matrix Group

The primary responsibilities of each function are as follows:

Covering Compliance

Covering Compliance Officers promote adherence to policies and procedures by supporting the direction and implementation of policies and procedures, reviewing and monitoring adherence to policies and procedures, and administering discipline for policy violations. Covering

Compliance Officers also support surveillance and monitoring activities carried out by other parts of Compliance, participate in Compliance examinations and investigations as requested, and collaborate with other S&P Global business functions on risk management, Credit Rating quality and internal controls.

Covering Compliance consists of three regional teams: Americas, EMEA and India, and Asia Pacific. The Chief Compliance Officer ("CCO") or Designated Compliance Officer ("DCO") for each region leads each regional covering compliance group, and oversees the Covering Compliance functions, regulatory exam management, regulatory reporting oversight and routine policy violation examinations within the relevant region. Where applicable, a DCO or CCO may leverage Compliance resources across regions.

The Chief Compliance Officer for EMEA and India ("CCO EMEA") is based in Dublin and reports to the GRCO. The CCO EMEA manages a team of fourteen Covering Compliance Officers. With reference to Israel, compliance matters are primarily handled by the EU/MEA Regional Covering Compliance Manager, who is also acting as Designated Compliance Officer for S&P Maalot and is based in Milan. The Regional Covering Compliance Manager reports to the CCO EMEA. The EMEA Compliance Officers receive additional global Compliance support.

Control, Monitoring and Examinations Group

The Control, Monitoring and Examinations Group ("CME") has responsibility for controls designed to prevent or detect failures of compliance with regulations, policies and operating procedures globally.

The examination function conducts and reports on compliance examinations and periodic thematic monitoring reviews. In doing so, CME evaluates adherence to written compliance policies and procedures, compliance with regulatory requirements, and the adequacy and effectiveness of compliance controls. In addition, compliance examinations may be undertaken as special process and operational reviews. CME issues reports in relation to these examinations and monitoring and tracks the status and completion of management action plans that address findings. A monitoring team working with the examination team conducts periodic recurrent testing of the operation of specific operating procedures and controls. Results of recurrent monitoring tests are reported to Covering Compliance to determine if remedial actions or additional controls should be undertaken.

The Global Control Room in CME administers a set of preventive and detective controls established to protect the integrity of the analytical process, manage conflicts of interest and prevent misuse of material non-public information. To help S&P Global Ratings prevent commercial conflicts from tainting the integrity of the analytical process, the Control Room chaperones certain communications between employees in Analytical and Commercial Roles. Chaperoning ensures that such communications proceed in compliance with requirements set forth in applicable policies. The team's role in controls for protection of information includes

advising on information access controls, maintaining insider lists and responding to regulatory requests for information on S&P Global Ratings' employees' access to non-public information.

The Digital Communications Surveillance team in CME conducts a risk-based review of digital communications as a detective control for compliance policy violations and as a support to front-line supervisors. The surveillance is performed through a software application that identifies communications for review according to parameters that are set and dynamically updated by the Digital Communications Surveillance team.

Global Regulatory Coordination

The Global Regulatory Coordination team ensures coordination and consistency across regions and facilitates remediation activities stemming from findings and recommendations from regulatory agencies. The team validates completion of regulatory remediation efforts and reports regulatory updates to senior management. The Global Regulatory Coordination team is also responsible for regulatory reporting. The team delivers reports to regulators and manages required regulatory disclosures on S&P Global Ratings' public website while ensuring that regulatory registration and reporting are accurate, complete and timely.

Global Matrix Group

The Global Matrix Group maintains and oversees the change process for the chapters of the S&P Global Ratings policy manual and SPGI policies as applicable to S&P Global Ratings, develops, tracks and coordinates compliance training, coordinates and oversees global compliance-related reports and presentations, and gathers data periodically on certain global compliance department activities, such as complaints, reviews and disciplinary actions.

Risk and Internal Control Function Structure and Responsibilities

The Risk and Internal Control Function is a second line of defense function that provides advice, oversight, coordination and reporting in support of S&P Global Ratings' internal control structure. This function is responsible for the development and implementation of the risk management framework. It also ensures that risks are identified, assessed, managed and properly reported by the relevant departments/functions within S&P Global Ratings.

The Risk and Internal Control Function works closely with In-Business Control to ensure that each department has defined and documented appropriate internal controls in policies, procedures and standard work within their respective departments. The Risk and Internal Control Function ensures that each department appropriately identifies, assesses and monitors risk, including evaluation of the effectiveness of their internal controls through monitoring and testing. Activities to mitigate risk, including the remediation of internal control deficiencies, are monitored by the Risk and Internal Control Function to ensure appropriate actions are taken on a timely basis.

The Risk and Internal Control Function facilitates the annual management assessment and attestation to the President of S&P Global Ratings for controls related to determining Credit Ratings which includes the confirmation of sufficiency of resources to support the internal control structure. The effectiveness of

the internal control structure is periodically evaluated and enhanced as needed, including risk policies and procedures, risk thresholds, control activities and reporting.

Analytic Quality and Validation Function Structure and Responsibilities

Analytic Quality and Validation ("AQV") is a second line of defense function responsible for the validation and periodic assessment of Criteria and Covered Models, the assessment of adherence to procedures and methodologies for determining Credit Ratings, and the assessment of analysis to provide assurance of its quality and defensibility. As an internal review function, AQV operates independently from the Analytical practices, Methodologies, and Commercial team.

AQV's primary responsibilities include:

- The independent ex-ante validation of proposed new or revised Criteria as well as conducting annual periodic Criteria reviews.
- The independent ex-ante validation of proposed new or revised Covered Models as well as conducting periodic Covered Model reviews.
- The independent assessment of adherence to methodologies used in determining Credit Ratings.
- Monitoring ratings quality to identify and communicate potential credit risks and opportunities that impact analytic quality and the defensibility of analysis.
- Credit risk monitoring activities, including the assessment of the quality of first line analyses and controls as well as identifying and assessing certain potential emerging risks impacting the Credit Ratings provided by S&P Global Ratings.

AQV produces reports detailing the outcome of its validation and periodic review activities to relevant stakeholders and further tracks the effectiveness and completion of management action plans that address any findings identified during AQV activities. Further, AQV may provide feedback to the Ratings organization regarding additional Analytical processes including, for example, transparency with respect to Credit Rating analysis, and published rationales for Credit Ratings.

**SPGI Global Risk & Corporate Compliance**

The mission of SPGI Global Risk & Corporate Compliance ("R&C") is to help employees make informed, risk-based, data-driven decisions across the enterprise. We provide independent, objective advice to enable mitigation of risk and compliance with policies/procedures and regulatory obligations with an emphasis on the achievement of the company's operational and strategic goals through the following teams that report to the SPGI Chief Risk & Corporate Compliance Officer:

1. Operational Risk Management ensures our risk management framework, policies/procedures and reporting support the businesses in their strategies and day-to-day activities including the following functions:
    - Enterprise Risk Management to ensure our framework and risk governance processes provide transparency and relevant oversight over the company's top risks. This function is

also responsible for oversight of the SPGI Executive Risk Management Committee and the SPGI Management Risk Committee on which S&P Global Ratings has representatives.

- Operational Resilience works with the businesses to ensure continuity of operations in the event of disruption due to incidents. The SPGI Operational Resilience Program promotes Business Continuity and IT Disaster Recovery planning and testing.
- Third Party Risk Management is responsible for assessing risks associated with vendor engagements and working with the business (i.e. S&P Global Ratings' IBCO Vendor & Affiliate Management Office) to effectively manage those risks posed by our vendors. In addition, the Third-Party Risk management team is also responsible for Client Due Diligence Response providing a formalized and consistent framework to respond to client inquiries regarding SPGI's risk and control processes while protecting confidential and internal information.

2. Cyber & Technology Risk Management establishes the SPGI enterprise-wide Technology Risk Management framework and provides independent oversight over the critically important technology and cyber risks across the enterprise. Additionally, this function manages IT and Information Security governance, policies and standards.
3. Divisional Risk Management is a second line of defense team that provides independent risk management oversight and advice to the S&P Global business divisions (for S&P Global Ratings only in cases where enterprise-wide issues impact the division).
4. Corporate Compliance provides a framework of policies, procedures, advice, training and monitoring to help ensure S&P Global complies with regulatory obligations and has established strong corporate governance as well as promotes the awareness of the importance of and adherence to ethical conduct across the organization. Corporate Compliance includes Conflicts Controls, Code of Business Ethics & Corporate Policy, Securities Disclosure, Information Governance and Privacy Compliance.
5. Global Financial Crimes Compliance provides governance, procedures, advice, training and monitoring focused on sanctions screening, anti-money laundering, and anti-corruption/anti-bribery compliance, to help ensure S&P Global compliance with regulatory requirements.
6. R&C Operations provides centralized operational support for program and project management, data and analytics, training coordination and key stakeholder reporting in support of the R&C organization.

R&C provides regular updates to the SPGI Audit Committee of the SPGI Board, the SPGI Executive Risk Management Committee and the SPGI Management Risk Committee.

S&P Global Ratings operationalizes the SPGI Enterprise Risk Management framework through its internal control structure. S&P Global Ratings participates in R&C activities as appropriate. S&P Global Ratings also utilizes services provided by Operational Risk Management, such as vendor risk assessment and Client Due Diligence Response support.

**SPGI Information Security**

SPGI's Information Security function, led by the SPGI Chief Information Security Officer ("CISO"), is responsible for the protection of SPGI's information and assets from threats to confidentiality, availability, and integrity by implementing, maintaining and enforcing SPGI's information security objectives, and best practices.

Furthermore, SPGI Information Security has the primary responsibility for the development, planning, coordination and communication of the SPGI Information Security Program ("IS Program") as well as its enforcement. Information security awareness for employees is included in the IS Program to enhance the security culture in the company.

The SPGI Information Security and SPGI divisions and SPGI corporate functions have joint responsibility for the deployment and maintenance of the IS Program, as applicable. The S&P Global Ratings Business Information Security Officer ("BISO"), who reports to the Ratings Chief Technology Officer, and the Ratings Business Information Security Team work with the SPGI Information Security Team to ensure that the corporate cybersecurity strategy is aligned with the division's business objectives. The BISO is primarily responsible for directing the division security strategy to ensure effective integration of the SPGI IS Program. Additionally, the BISO provides regular reporting of divisional security posture to the Global Executive Risk Committee and business and the Boards.

The CISO reports to the SPGI Chief Information Officer. The CISO provides periodic updates and advice on information security to the SPGI Audit Committee, the SPGI Executive Risk Management Committee, and the SPGI Board.

**SPGI Internal Audit**

The principal role of SPGI Internal Audit ("SPGI IA") is to provide independent and objective assurance on the control environment for the business and operations of SPGI to the SPGI Board of Directors and executive management. This role is designed to evaluate the effectiveness of governance, risk management, compliance, and analytical practices within SPGI and to support the organization in achieving its strategic objectives.

The SPGI IA function is independent of S&P Global Ratings' management and compliance and other control functions and incorporates S&P Global Ratings in its annual risk-based internal audit plan. The annual audit plan is reviewed with executive management and the Boards and presented to the SPGI Audit Committee of the SPGI Board of Directors for review and approval. Subsequent key changes to the plan are reviewed with executive management and presented to the SPGI Audit Committee for approval.

SPGI IA regularly performs compliance, regulatory, operational, information technology and financial audits on SPGI entities and subsidiaries including S&P Global Ratings. It also carries out reviews of analytical quality across S&P Global Ratings through its Analytical Assurance team. To prepare its annual

internal audit plan, SPGI IA carries out a comprehensive risk assessment process to identify significant risks, including those associated with S&P Global Ratings (including those that are regulatory in nature).

SPGI IA issues reports in relation to the audits performed and tracks the status and completion of management action plans that address the audit findings. The completion of management actions plans is validated by SPGI IA before they are closed. The results of SPGI IA reviews are reported to key stakeholders including status of management action plans and the progress against the annual approved internal audit plan.

SPGI IA also carries out quarterly continuous monitoring on SPGI divisions, including S&P Global Ratings. This activity includes stakeholder interviews and reviews of management information and business performance. The outcomes from the continuous monitoring activity are considered quarterly by the SPGI IA leadership team and informs changes to the risk assessment process and the internal audit plan.

The SPGI Chief Auditor reports to the SPGI Audit Committee of the SPGI Board of Directors on a functional basis, and administratively to the SPGI President and Chief Executive Officer. SPGI IA reports audit results including the status of audit tracking to the SPGI Audit Committee, the Boards and the Global Risk and Compliance Committee. The Chief Auditor is a member of the SPGI Executive Risk Management Committee.