9. Corporate risk management

In 2015, with the endorsement of the Board of Directors and the Executive Committee, Amadeus formally adopted the Three Lines of Defense Model – a model for integrating, coordinating and aligning all support and assurance functions within the entity, ensuring the effective management of risks across the company.

Since its adoption, the Three Lines of Defense Model has fostered effective risk management across Amadeus. In 2016 we refined the Three Lines of Defense Model through the adoption of a Combined Assurance concept. Through this Combined Assurance program, we have expanded the coordinated management of oversight control activities and the sharing of results.

First Line of Defense: executive management, management and staff

Amadeus’ commitment to integrity and transparency begins with its own staff. Amadeus employees adhere to the ethical standards set forth in the Amadeus Code of Ethics and Business Conduct and related policies. We do not see this code and our core policies purely as a “rule book,” but as a mutual agreement across the company to promote positive behaviors that will add value to our business and ensure the highest standards of integrity at all times. The areas covered in the code are as follows:

Commitment to the environment
Avoiding conflicts of interest
Protecting personal data and confidentiality
Handling relations with third parties and the media in a sensitive manner
Handling company property, equipment and installations with care

In 2017 we adopted a human rights policy affirming our respect and promotion of international human rights. We expect all our suppliers and business partners to uphold internationally recognized standards regarding working conditions and the dignified treatment of employees.
Human rights form part of Amadeus’ risk analysis. We evaluate the risks of infringing on the following rights: non-discrimination, collective bargaining, freedom of association, fair wages, no child labor or forced labor, and adequately healthy and safe working conditions. Although such risks fall very low on our risk map, we have a series of mitigating and monitoring actions to manage them, both internally and with our suppliers and business partners. Our mergers and acquisitions procedures also include due diligence on human rights–related risks. Our integration team ensures that Amadeus’ policies are effectively implemented into newly integrated companies. Furthermore, our Speak Up Policy encourages employees to report any breach of the Code of Ethics and Business Conduct, including possible resulting human rights violations. During 2018 no significant breaches to the Code of Ethics and Business Conduct were reported.

The Amadeus core policies listed on this page are supported by processes that, as with any other processes at Amadeus, undergo regular internal and external quality reviews to ensure regulatory compliance and application of best practice. We have mechanisms in place to allow the organization to seek advice on whether certain activities are considered ethical or lawful in accordance with our corporate policies. For example, the Ethics Committee acts as a vehicle to respond and give such advice as well as to report any unethical or unlawful behavior by any person.

Amadeus policies
- Compliance policies
  - Amadeus Code of Ethics and Business Conduct
  - Anti-Bribery Policy
  - Anti-Fraud Policy
  - Business Continuity Policy
  - Entertainment/Gift Policy
  - Information Classification Policy
  - Speak Up Policy

- Legal policies
  - Corporate Privacy Policy
  - ACO Privacy Manual
  - Antitrust and Competition Law – Compliance Manual
  - Internal Rules of Conduct to the Securities Market
  - Security and Privacy Handbook

- Industry affairs policies
  - Amadeus Environmental Policy
  - Charitable Contributions Policy
  - Political Contributions and Lobbying Policy
  - Social Responsibility Policy and Practice

- Human resources policies
  - Amadeus Human Rights Policy
  - Health and Safety

- Finance policies
  - Corporate Purchasing Policy

- Information security policies
  - Acceptable Use Policies

- Three Lines of Defense and Combined Assurance

  1st Line of Defense
  - Line and support management
  - Has ownership, responsibility and accountability for assessing, controlling and mitigating risks

  2nd Line of Defense
  - Human resources
  - Legal
  - Risk management
  - Data privacy
  - Compliance
  - Monitors and facilitates the implementation of effective risk management practices by the 1st line and assists risk owners in reporting risk-related information throughout the organization

  3rd Line of Defense
  - Internal audit
  - Provides assurance to the Group’s governing body and senior management on the organization’s effectiveness in assessing and managing risks and related internal control systems, including the manner in which the 1st and 2nd lines operate

GRI 102-16, 102-17, 102-30, 103-1, 103-2, 103-3 (Anti-corruption), 103-1, 103-2, 103-3 (Transparency and integrity), 103-1, 103-2, 103-3 (Risk management), 415-1, 103-1, 103-2, 103-3 (Environmental and social compliance)
Second Line of Defense: internal governance functions

Control activities are embedded in all areas of the company. Major control activities are carried out from departments such as Risk & Compliance, Security, Privacy, Legal, Finance, People & Culture and others.

Risk management and controls

Risk & Compliance is responsible for centralizing the continuous monitoring of major risk and compliance issues within Amadeus, and also leads a transversal Combined Assurance program involving Risk & Compliance, the Group Privacy Unit and the Corporate Information Security Office. The Combined Assurance program also coordinates its activities with other functions focused on business control, including our Regional Business Oversight commissions (which are made up of senior personnel from Legal, HR, Finance and our business units) and our Internal Financial Controls unit (which oversees compliance with the Internal Control over Financial Reporting (ICFR) standard).

Risk & Compliance develops Amadeus’ Corporate Risk Map and establishes control and monitoring procedures for each of the identified risks, in conjunction with the owner responsible for each risk. The risks ascertained from this analysis, as well as monitoring measures, are reported on a regular basis to the Risk Steering Committee and the Audit Committee, as well as the Executive Committee and the Board of Directors.

We continually monitor the most significant risks that could affect Amadeus and the companies that make up Amadeus Group, as well as Amadeus’ own activities and objectives.

Amadeus’ general policy regarding risk management and monitoring focuses on:

- Achieving the company’s long-term objectives in line with its established strategic plan
- Contributing the maximum level of guarantees to shareholders and defending their interests
- Protecting the company’s earnings
- Protecting the company’s image and reputation
- Providing the maximum level of guarantees to customers and defending their interests
- Guaranteeing corporate stability and financial strength over time

The ultimate aim of the Corporate Risk Map is to provide visibility on significant risks and facilitate effective risk management. Risk analysis is a fundamental element of the company’s decision-making processes, both within the governing bodies and in the management of the business as a whole.

The Corporate Risk Map also takes into account the global risks identified each year by the World Economic Forum,\(^1\) such as economic, environmental, geopolitical, societal and technological risks.

Amadeus is concerned about near-term risks. A new edition of the Corporate Risk Map including these immediate or existing top risks was issued in 2018. But we are also focused on those other issues that have not manifested sufficiently to be managed, what is commonly known as the “known unknowns” or emerging risks. These are to us newly developing or changing risks that are difficult to identify and quantify and could have a major impact on society and the industry. The Corporate Risk Map also deals with this type of risk, examples of which are the effect of an increasingly aging population over the years on the travel sector, or the threats to our business model, especially in the context of today’s fast digital development.

The latest version of the Corporate Risk Map defines the most critical risks relating to Amadeus’ operations and objectives, among which the following are highlighted: technological risks; operational risks that could affect the efficiency of business processes and services; commercial risks that could affect

customer satisfaction; reputational risks; security and compliance risks; the macro-economic and geopolitical environment; and trends in the travel and tourism industry. Some of these risks have evolved from the previous Corporate Risk Map, while others have been newly identified.

These highlighted risks are assigned to risk owners at the highest level of the company, who are given the duty of proposing the risk response. Progress with mitigation and evolution of key risks is submitted to the Risk Steering Committee for review and consideration, together with proposed action plans, when required, to take any necessary measures or further actions.

Due to its transversal and dynamic character, the process described above identifies new risks that affect Amadeus arising from changes in the environment or the revision of objectives and strategies.

In the current business environment, which is characterized by increasing stakeholder demand for transparency, ethics and social responsibility, reputational risk management is becoming increasingly relevant. The Amadeus Reputational Risk Map is fully integrated into the overall Corporate Risk Map of the company. Therefore, assessing the reputational impact of a particular risk is embedded into our methodology. In a similar vein, cybersecurity risks are managed through a security risk framework driven by our Corporate Information Security Office, which is also integrated into the Corporate Risk Map.

In addition to managing risks, Amadeus is very focused on ensuring compliance with emerging initiatives such as the General Data Protection Regulation (GDPR) of the European Union. In 2017 we initiated a major corporate program to ensure GDPR compliance. Our activities also extend to existing control standards such as PCI-DSS (credit cards), SOC 1 (computer controls) and ISO 27001 (security).

Moreover, Amadeus, like any other organization, is exposed to potential risks that could provoke significant disruption over key internal and external IT services that we provide to customers. To ensure minimal disruption in such catastrophic events, Amadeus is implementing a Business Resilience Program (led by Risk & Compliance), designed to protect our people, assets and infrastructure, and manage any disruption to minimize the potential impact to acceptable limits.

Finally, through the training and awareness plan under coordination of the Risk & Compliance unit, we try to ensure that all employees understand and apply best practices on ethical behavior as well as security and privacy.

The Risk & Compliance Office oversees the following committees:

_ The Ethics Committee, which provides guidance on ethical behavior and compliance issues. This committee also addresses any concerns that employees may have and simultaneously assists in the implementation of the Code of Ethics and Business Conduct throughout Amadeus. We attach great importance to promoting integrity, transparency and ethical conduct in all our operations, and we are committed to applying a zero-tolerance approach regarding prohibited practices, both in our internal affairs and external operations.

_ The Risk Steering Committee, which is a decision-making body empowered by the Executive Committee to provide oversight and guidance on risk management activities and issues across Amadeus, including risk assessment and prioritization, risk mitigation strategies and crisis response.

Both the Ethics Committee and the Risk Steering Committee meet several times a year.
Third Line of Defense: Group Internal Audit

Group Internal Audit provides independent and objective assurance and consulting services designed to add value and improve Amadeus’ operations. It helps accomplish our goals by using a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management and control processes, including the potential for the occurrence of fraud and how the organization manages fraud risk.

Group Internal Audit covers all companies, businesses and processes majority-owned or controlled by Amadeus. Every year, Group Internal Audit performs a thorough background and risk assessment exercise to verify and update the established audit priorities. This exercise considers, namely but not exclusively, elements such as the Group’s strategic objectives and projects; the Corporate Risk Map; internal and external challenges and enablers identified through interviews with senior management and major control functions; business magnitudes; and audit cycles. The output leads to the formalization and approval by the Audit Committee of a yearly internal audit plan.

The legal entities included in Group Internal Audit reviews during 2018 represented more than 60% of the total Amadeus workforce. Main risks identified in the course of internal audit engagements are reported to senior management and the Audit Committee, and their status is periodically updated until resolution or acceptance by the governing bodies.

The coordination streams in place between Group Internal Audit and the main control, business and technology units ensure a continuous and optimum complement to Group Internal Audit’s independent and objective assurance activities.

Group Internal Audit is governed according to the mandatory elements of The Institute of Internal Auditors (IIA)’s International Professional Practices Framework (IPPF), including its Core Principles, its Definition of Internal Auditing, its International Standards and its Code of Ethics. Furthermore, Group Internal Audit runs a Quality Assurance and Improvement Program that combines ongoing monitoring with periodic internal and external assessments. The program includes the evaluation of Group Internal Audit’s conformance with the International Professional Practices Framework (IPPF). The program also assesses the efficiency and effectiveness of Group Internal Audit, and identifies opportunities for continuous improvement.

Amadeus Corporate Information Security Office

Amadeus continuously reviews and improves its processes to keep ahead of upcoming threats, ensuring that both people and technical controls are considered and addressed. We follow the ISO 27001 standard, including:

1. Corporate security objectives and controls set by a Corporate Information Security Office.
2. The Security Risk Map, which gives priorities for the implementation of mitigations.
3. A maturity assessment carried out by a third party to also identify security gaps, which are also monitored and followed in our Corporate Security Program.

All activities related to those sections are monitored and controlled by the Corporate Security Program (SHIELD).

From a global operations and technology perspective, Amadeus has established an independent Security Operations Center to monitor the security status of the services we provide to customers 24/7. This service also helps us understand emerging technical threats and invest in the most appropriate technology to mitigate new risks.

Since January 2017 Amadeus has become a member of the Aviation Information Sharing and Analysis Center, showing that we are constantly striving toward increasing our customers’ trust and sharing best practices.
Amadeus Corporate Information Security Office

Regional security offices
Extended security awareness and control to all Amadeus regions and subsidiaries

ISO 27001 certification
ISO 27001 level 3 certification at Amadeus corporate level

SSDLC*
Ensures the implementation of secure software development methodologies according to SSDLC standards

Security nominative framework
Policies and framework are implemented and used to assess security risks. Mitigation plan put in place

Ensures that:
- All security policies and security architecture standards are properly monitored and controlled.
- Amadeus is protected against known threats and attacks.
- Security incidents are handled with proper communication.
- Security incidents are investigated and contained.
- Artificial intelligence is used to identify vulnerabilities.
- User behavior analytics are used to provide us with actionable insights by identifying patterns of traffic caused by user behaviors, both normal and malicious.

Access control
Ensure that only authorized persons have access to confidential information on a need-to-know and need-to-handle basis

PCI-DSS** compliance
Ensure that Amadeus is PCI-DSS compliant and that we are prepared for changes in PCI-DSS compliance requirements

Security by design
Ensure that security is observed from the beginning of every new product and project

Data leak prevention
Ensure that critical information in any format does not leak out to unauthorized persons/destinations

Security awareness
Create and follow up on employee security awareness