Risk management

- Risk management and control 30
- How we address risk management 32
- How we monitor effectiveness 34
- How we provide independent assurance 35
- Principal risks 36
“Risk management is part of our culture across the Company. We accept the risks we can manage and where this gives us a competitive advantage. We seek to mitigate or avoid other risks. Ensuring we have an efficient risk management system in place is key to developing our business and achieving our objectives.”

Philippe Vallée
Chief Executive Officer

Trusted to manage our risks

Security is our business – so risk management is a necessary and intrinsic part of the way we work. Our customers trust us to make it integral to our service and our culture. It is part of our responsibility to them, as well as to investors, employees and other stakeholders.

We review our principal risks regularly, because we work in a dynamic environment where new risks may arise or previously identified risks may have a different impact. Effectively managing risks is the responsibility of all employees. Managers are accountable for allocating required resources to successfully manage the risks they own.

The Board needs reasonable assurance that our risk management and reporting systems remain sound. So we have a range of policies and processes involving both internal and independent controls: Internal Audit, external certification bodies and external auditors. These are designed to strike the right balance between cost and effectiveness. Together, they aim to help us achieve our business objectives while cutting to an acceptable minimum the risk of operational failures, misstatements, inaccuracies and errors, fraud and non-compliance with laws and regulations.

What we focused on during the year

We strive for a simple and practical approach while constantly improving our risk management process and the quality of information it produces. Our key focus areas during the year were:

• Further improved the Company’s level of preparation for crisis management. Maturity assessment performed on all the plans submitted by our crisis management leaders.

• Expanded risk assessment on key activities with a focus on our Platforms & Services businesses.

• Fraud risk assessment performed.

• Concentrated support provided to Manufacturing and Information Solutions and Services (ISS) in terms of Business Continuity management.

What we plan to do in the future

• Support our key suppliers to improve their business continuity responses.

• Continue to enhance our business continuity planning with a focus on our IT recovery.

• Ongoing development of our holistic control view through synergies, exchanges and reviews between Risk management, Internal control, Internal Audit, Quality and Corporate Strategy teams.
How we share our risk management responsibilities

Who is responsible for what

The Board
– Approves strategic objectives and validates our risk appetite.
– Reviews the Group’s key risks and mitigating measures.
– Reviews the Company’s risk management and internal control systems.
– Assesses these systems’ effectiveness through its Audit committee.

Senior Management
– Is responsible for the “tone at the top”.
– Oversees design and sustainable implementation of Enterprise Risk Management (ERM) and internal control systems.
– Defines and allocates risk appetite.
– Makes decisions when substantial risk is at stake.
– Evaluates the adequacy of risk mitigation plans.

Business management
First line of defense
– Identifies, takes and manages risks in their areas of responsibility.
– Maintains day-to-day internal control.

Support functions
Second line of defense
– Define internal control policies and provide guidance in their areas.
– Develop risk management culture and awareness of internal controls.
– Establish discipline and act as guardrails.

Corporate risk management
Second line of defense
– Develops and promotes ERM framework to help managers identify, assess, manage, monitor and report risks.
– Facilitates reviews of the design and implementation of internal controls.

Internal audit
Third line of defense
– Provides independent assurance of the effectiveness of the Group’s risk management and internal control frameworks and activities.

Five key risk management processes

1. Budgeting, planning and reporting
2. Risk assessment and mitigation
3. Crisis and business continuity management
4. Fraud risk management
5. Transfer to insurance

See page 32
See page 32
See page 33
See page 33
See page 33

Foundations

Our processes are underpinned and informed by:

Strategy and objectives
Culture and values
Internal control
Sustainability
How we address risk management

Five key risk management processes

Our principal risks and mitigating actions are explained on pages 36-38. We have five dedicated processes for managing these and other risks:

1. Budgeting, planning and reporting
2. Risk assessment and mitigation
3. Crisis and business continuity management
4. Fraud risk management
5. Transfer to insurance

1. Budgeting, planning and reporting
To support informed and timely decision-making, we maintain strategic planning and detailed annual budgeting and forecasting processes with complementary reporting systems.

Our 2014-2017 Development Plan, prepared in line with Group objectives and strategy, covers the whole Group. The planning process includes analysis of our own business and its competition across all our activities, assessing strengths, weaknesses, opportunities and threats.

Operating and financial results and forecast are reviewed monthly. Operating results and forecast are reviewed first by our CEO and Group Controller and the Executive Vice-President and/or Controller of each segment and geographic area. They are then consolidated for review by the Corporate Treasurer, Group Tax Director and the CFO.

Our business review process covers all operational entities and corporate departments at least quarterly. The budget process begins in September and delivers an annual Group budget for the following year. This is approved by the Board in December. Whenever justified by changes in activity, current quarter and current year forecasts are reviewed and consolidated into updated forecasts for the Group.

The Group Treasurer prepares a monthly review of financial results, the efficiency of the balance sheet and cash flow hedges, client receivables, and Group cash and debt.

Drawing on the review of the operating results and the treasury report, the Group Controller and CFO prepare an operating dashboard and report for review by the CEO and circulation to the Board quarterly. A review of activity is also presented by the CEO and the CFO at each Board meeting.

In addition to the monthly result calls, the Head of Consolidation holds quarterly reviews with each segment and region to help identify any transaction or event which could significantly impact the Group’s results or financial condition.

2. Risk assessment and mitigation
Our risk management process has six key elements:

- Map and anticipate main identifiable risks and regularly update assessments
- Prioritize them against Group strategy and risk appetite
- Allocate risk ownership
- Develop and implement policies and mitigation plans, including transfer to insurance
- Communicate key control objectives to operational managers
- Provide training and support, regularly check the effectiveness of the process
Integrated in the Company’s processes, our approach is based on the principles of responsibility, ownership, performance-oriented and continuous improvement. Key risks are assigned to risk owners responsible for developing action plans. Reporting on progress on the mitigation plans is done every six months by each manager sponsor of a risk assessment to the ERA* Steering Committee chaired by the CEO.

Risk assessment is carried out at all management levels as shown in the chart below, and is supported by an ERM software tool also used to manage our internal control self-assessment questionnaires.

*Enterprise Risk Assessment.

3. Crisis and business continuity management

We cannot identify all the risks we may face. So we have crisis management processes and business continuity responses designed to improve our resilience to unforeseen events – such as a supply chain disruption, employee repatriation, or network intrusion attempts – and minimize their impact on our stakeholders and reputation.

Our Crisis Management Framework was first rolled out in 2010. It encompasses basic escalation and communication rules, guidelines for anticipation and action, and clear roles and responsibilities. Close to 140 Crisis Management Leaders are in place worldwide and trained through simulation exercises.

In 2016, we continued to update and refine our crisis management framework and improved the Company’s preparation level. In particular, the Corporate Risk Management department assessed the maturity of all the crisis management plans submitted by the crisis management leaders, and provided guidelines on the improvement areas.

4. Fraud risk management

We have built an anti-fraud framework to prevent, detect, deter, report and respond to fraudulent activities. This is overseen by the Gemalto Anti-Fraud Commission comprising the Group General Counsel, EVP Human Resources, Chief Information Officer, Internal Audit Director, Security Director and Compliance Officer.

All managers must report any suspicion of fraud to the Commission, and our whistle-blowing hotline enables employees to raise suspected irregularities with a confidential advisor. In the event of a fraud, managers must make appropriate changes to systems, controls, education and procedures to prevent recurrence, and the commission monitors the effectiveness of such actions.

In 2016, we performed a fraud risk assessment and trained some 267 key people in anti-fraud, anti-bribery, anti-trust and ethics. In addition, some 1585 employees were trained in CFIUS and trade compliance topics. We also sent out internal newsletters on Internal Control and trade compliance.

5. Transfer to insurance

Our global insurance programs cover property damage, business interruption, public, product and professional liability, and Directors’ and Officers’ exposures. They aim to protect the Company against exceptionally large or numerous claims, at a cost that does not impair Group competitiveness. We neither own nor operate any captive insurance: we use only high-quality and financially sound insurers, combining master policies with local insurance policies and officers’ exposures. They aim to protect the Company against exceptionally large or numerous claims, at a cost that does not impair Group competitiveness. We neither own nor operate any captive insurance: we use only high-quality and financially sound insurers, combining master policies with local insurance policies.

Negotiation and coordination of these programs are carried out centrally with the help of leading insurance brokers with integrated international networks. In this way we secure broad and consistent cover for all Gemalto activities and locations worldwide, cost optimization, and global reporting and control, while ensuring compliance with local regulatory requirements. We review our insurance strategies periodically, taking into account changes in our risk profile (such as acquisitions, claims, loss events and other activities) and insurance market trends.
How we monitor effectiveness

Ethical practices and employee confidence

In our 2016 internal PeopleQuest survey, employees confirmed their confidence in our ethical practices and performance. They said that Gemalto and its management:

91% are committed to ethical practices

91% set a good example

89% provide adequate information about ethical practices

Risk management

The Corporate Risk Management department has a global view of risks encompassing Enterprise Risk management, Internal Control, Crisis management, Business Continuity, Insurance and Trade Compliance. This broad view is a powerful asset in understanding and managing our risks, and helps us develop a pragmatic overall risk management approach. The department reports to both the General Counsel and the CFO.

Internal control

We have a strong framework of internal control across all business areas and functions, based on a clear statement of ethical business principles, established procedures, and effective training of the key personnel who implement and oversee it. It aims to check that we are meeting our objectives (including sustainability goals), reporting financial performance reliably, and complying with relevant laws and regulations.

We apply a risk-based approach. The internal control framework is updated yearly, so that it continuously evolves in line with the Company’s structure, objectives, commitments and risks.

Our internal control team develops awareness across the Company and uses yearly risk-based self-assessment campaigns to ensure that the proper level of control is maintained and enhanced. For our most critical processes and entities, these self-evaluations are tested by internal auditors. This helps us to define plans for remedying deficiencies and to monitor their implementation, with particular focus on newly acquired companies.

Our dedicated Security, Quality, Health, Safety and Environment department, with representatives throughout the Group, promotes the appropriate culture and performs regular audits.

The Audit committee regularly reviews internal control reporting and internal audit activity. An annual report to the Audit committee is prepared by the Internal Audit Director and agreed with the CFO and CEO.

Financial control

Financial controllers, with the support from Internal Audit and Corporate Risk Management, are responsible for identifying risks which significantly impact the financial statements, and for taking action to mitigate those risks. They are also responsible for ensuring that the controls over the Group’s earnings and operating performance remain adequate. They participate in the budget and quarterly business reviews, and oversee the monthly financial results of segments, regions and the Group. They also play an active role in operational and performance improvement projects, and in cost control and cost-effectiveness initiatives.
How we provide independent assurance

Internal and external bodies provide assurance on the design and effectiveness of the risk management processes and compliance with the relevant standards, policies and norms.

**Internal audit**
- Our Internal Audit department conforms to the International Standards published by the Institute of Internal Auditors (IIA). It has direct and unlimited access to Group operations, documents and employees. It reports directly to the CFO and has an independent line of communication with the Audit committee Chairman and the CEO. Internal Audit reports to the Audit committee at each meeting and holds regular private sessions with the Audit committee.
- The team reports monthly and annually to the Chairman of the Audit committee and the CFO. Audit missions include ethics and fraud reviews and follow-up reviews of acquisitions.
- The Institut Français de l’Audit et du Contrôle Internes renewed the team’s professional certification in December 2016.

**External certifications**
- We maintain a number of certifications: some, such as EMV, GSM SAS, ISO 9001, ISO/TS 16949, ISO 14001, OHSAS 18001 and ISO 27001 are necessary for the conduct of our business. The effectiveness of our Quality and Health, Safety and Environment (HSE) management systems is constantly challenged by external and internal audits seeking continuous improvement.

**External auditor**
- The independent external auditor provides an independent opinion on the financial results of the Group: its report is available on page 120. The auditor has unrestricted access to Gemalto sites and documentation, and communicates regularly with the Internal Audit department and with the Audit committee.
- The Audit committee assesses the work of the external auditor at least once a year.
Principal risks

In addition to the business risks generally faced by international businesses like Gemalto (such as country risks, M&A, foreign exchange, interest rates, liquidity...), we have outlined eight principal risks that could have an impact on the Company, and have taken measures to mitigate each one.

<table>
<thead>
<tr>
<th>Market growth</th>
<th>Competition</th>
</tr>
</thead>
<tbody>
<tr>
<td>New businesses and chosen markets do not hold their growth prospect or develop as predicted.</td>
<td>Change in the business dynamic, whereby a competitor’s product or technology may lead to loss of competitive advantage.</td>
</tr>
</tbody>
</table>

**Relevance/materiality**
- Failure to benefit as expected from business opportunities particularly in the Internet of Things, Enterprise Security and National Identity programs.
- Failure to make security a ready-to-use service that grows as fast as the markets it protects.
- Sovereignty consideration reduces potential market for global security solution providers despite increasing needs.

**Potential impacts/effects**
- Negative impact on revenues, cash flows and profitability sustainability.
- Inefficient distribution of physical, personnel and financial resources.

**Mitigating actions**
- Competitive and market intelligence program.
- Formal multi-year development plan.
- Run a regular Opportunity and Portfolio financial review to gauge investment and cash allocation across our businesses.
- Focus on industries where reach is strong.
- Focus investments in growing markets.
- Target market leadership where we play.
- Design our security solutions to preserve customer ownership and control.
- Design our security solutions to facilitate enforcement of local regulatory compliances.
- Use common core technologies across segments to leverage internal synergies.
- Continuous adjustment of our geographic footprint by balancing local hiring with the right network of local partners and distributors.
- Diversification of use cases of our technologies and client bases.

For further information about financial risks (e.g. interest rate risk, liquidity risk and credit risk), see Note 4 Financial risk management, pages 81-85.
### Data protection and cyber security, data privacy regulations

Security failure in our systems or IT infrastructure, cyber attacks. Failure to comply with evolving data protection regulations.

**Relevance/materiality**
- Data protection and cyber security are core to our business, which itself is contingent on customer confidence in our ability to protect the privacy of the data they entrust to us.
- Hacking threats are growing significantly.
- Enhanced data quality and integrity lead to strategic business decisions and better customer service.
- Business development through expansion into jurisdictions with clear privacy regulations.

**Potential impacts/effects**
- Leakage and/or loss of customers’ or Gemalto confidential data resulting, for example, from cyberattacks, employee negligence or the vulnerability of our IT systems.
- Inquiries, complaints and lawsuits.
- Investigation by governmental privacy authorities.
- Replacement of products or remediation costs.
- Loss of business or market share.
- Adverse impact on reputation.
- Drop in stock prices due to negative publicity.

**Mitigating actions**
- Security and cryptography expertise, tools and systems.
- Standardized tools and policies for all devices on the Gemalto network ‘Cyber Excellence Program’ with regular training sessions.
- Awareness program and compliance action plan on Data privacy led by the Director of Global Data Privacy.
- Worldwide security organization with security officers at all important sites and regional/corporate security support.
- Security certifications by third parties (including ISO 27001, EMV, GSM, SAS, etc.).
- Corporate Security Incident Response team.
- Internal security audits (extended to IT subcontractors).
- Anti-Fraud Commission.
- Regular penetration testing on our systems and solutions, detection systems.
- Log gathering and analysis through the Security Operating Center.
- Work with national agencies.

### Product quality and service delivery

Technical requirements becoming more and more complex and demanding with high liabilities.

**Relevance/materiality**
- Development of embedded products (eSE…) will increase liabilities and replacement costs.
- Defects (visual) on Government Program products could be seen as a security breach (fake, fraud…).
- Our products support our image to the customer (brand).

**Potential impacts/effects**
- Failure to develop and deploy secure, stable or reliable technology products and solutions.
- Failure of supplier’s product embedded in a Gemalto solution.
- Major quality issue in one of our manufacturing facilities.
- Unforeseen software development problems (e.g. bugs).
- Mismanagement of after-sales service.
- Replacement of products.
- Loss of reputation.

**Mitigating actions**
- Standardized manufacturing processes.
- Quality management system and world-class enterprise organization.
- Dedicated R&D teams for Product as well as Platforms & Services.
- Bid and contract reviews with approval process based on risk assessment and according to limits of authority.
- Product and professional liability insurance.
- Customer satisfaction measured regularly with high overall customer confidence in annual survey.
- Dedicated key account management program.
- Qualification labs continuously improving qualification processes.
- Failure analysis labs.
- Corporate quality improvements programs, anti-error systems.

### Talent management

Our people and HR processes may not be adequately scalable to meet our growth and transformation ambitions.

**Relevance/materiality**
- The Group’s success and its strategic shift towards Software and Services are contingent on recruiting and retaining highly skilled personnel (senior management, R&D, engineering, sales, marketing…).
- There is intense competition for skilled employees.

**Potential impacts/effects**
- Inability to attract, develop and retain highly qualified management and suitably skilled employees, particularly to address the markets we want to develop in.
- Loss of key resources, including in acquired companies.
- Shortage of appropriately skilled management.

**Mitigating actions**
- Comprehensive Human Resources strategy with eight pillars (diversity, mobility, promotion from within, learning, recruitment, compensation & benefits, ethics & well-being, management by objectives).
- Technical Ladder to recognize individual contributors/technical skills.
- Short-term and long-term management incentive plans.
- Succession plan for senior management positions.
- Company positioning on professional social networks.
- Yearly Employee satisfaction survey and related action plan.
- Acquisition of specific expertise accelerated through M&A.
## Principal risks continued

### Business integrity, ethics and reputation
- Internal fraud, bribery, anti-trust violations; actions or inactions perceived by stakeholders to be inappropriate.

#### Relevance/materiality
- As a listed company with a worldwide presence, the Group is subject to numerous rapidly evolving and complex laws and regulations.
- Stakeholder trust is directly tied to ethical behavior, compliance with applicable rules and regulations and internal policies and procedures.

#### Potential impacts/effects
- Loss of trust.
- Impact on our image and reputation.
- Fines and other sanctions.
- Liabilities, including Director and Officer liabilities.

#### Mitigating actions
- Risk assessments with regular updates (including fraud risks).
- Anti-fraud commission; Compliance Officer reporting directly to the CEO.
- Policies and procedures, Code of Ethics, Agents Policy, whistle-blowing tool, employee survey.
- Sustainability structure and framework in place.
- Security certifications and organization.
- Training/e-learning: security, business principles, anti-fraud, anti-trust.
- Regular internal and external audits of facilities.
- Internal audits on all suspected fraud.
- Investigation process and tools.
- Crisis management framework and associated worldwide training program.
- Code of Ethics signed by employees.
- Clear policies on “do’s and don’ts”.

### IP protection and claims
- Insufficiently protecting intellectual property (IP) rights, claims from third parties pretending that we have infringed their proprietary rights.

#### Relevance/materiality
- R&D is an important part of the activity of the Group and is dependent on proprietary technology and intellectual property rights.

#### Potential impacts/effects
- Failure to protect our proprietary technology and IP rights (inability of the Group to prevent others from commercially using our inventions, thereby increasing competition; lost opportunity to license patent rights to other enterprises which are a source of income for the Group).
- Third-party claims for alleged infringements of their patent rights (inability to use the patented invention in our products and services, damages to be paid for past infringements...).

#### Mitigating actions
- Dedicated and qualified internal IP team organized by technology.
- Internal IP department, internal inventor policies, formal Open Source software policy and other ad-hoc policies.
- Patent committee.
- Patent management database and third parties’ patents search.
- Contract reviews on IP clauses.
- Management of Open Source use within Gemalto through a dedicated process.
- In-depth analysis at the very beginning of bidding process for major deals in order to measure the Group’s likelihood of success.
- Reassessment and contract review with clear presentation of risks and approval process according to limits of authority in order to ensure decision-making at proper management level and efficient allocation of resources.
- Project-based organization of Government Programs and solutions and services contracts to manage delivery risks.
- Revenue recognition policy, contractual guidelines, business and geographical legal teams...

### Contracts
- Ineffectively managing complex national or multinational customer contracts (long-term government contracts, solution or service projects, etc.).

#### Relevance/materiality
- Potential excessive liabilities arising from contracts.
- Numerous factors including cost variation; delivery delays; changes to customer requirements, budgets, strategies, or businesses; supplier performance; our ability to negotiate back-to-back clauses for purchasing or partnership agreements affect the revenue and profitability of a contract and could lead to financial loss.

#### Potential impacts/effects
- Inability to accurately assess our selection chances within the framework of a bid process may lead to inefficient allocation of resources and additional costs.
- Inability to recover upfront/early investments in government (BOT) or solutions and services (IT infrastructure) contracts due to delays, missed milestones or country risks.
- Poor understanding and/or implementation of client expectations or needs could lead to a failed contract, resulting in reduced future revenue, profitability and cash generation.
- Contingent liabilities.

#### Mitigating actions
- Revenue recognition policy, contractual guidelines, business and geographical legal teams...