Trust. Every day
Keeping corporate networks private in the US

Red Hat is the world’s leading provider of open-source software solutions. But its virtual private network (VPN) needs to be completely private, since its 7,000 employees use it to access sensitive company information – even remotely. To protect this access more strongly, Red Hat selected our Protiva token technology in 2014 to provide multi-factor authentication. And in keeping with its open-standard ethos, our interoperable solution promises easy integration with its present and future IT systems.
Risk management and control

**Trusted to manage our risks**

A distinctive feature of our Company is that security, and hence risk management, is an intrinsic part of our entire business. As some potential risks to our activities could impact our operational security, reputation, integrity and continuity, we see effective risk management as part of our responsibility to customers, as well as to investors, employees and other stakeholders. Our customers trust us to make it integral to our service and our culture.

In common with most organizations worldwide, we are affected by a number of risk factors, not all within our control. Some, such as macroeconomic factors, are likely to affect the performance of businesses generally; others are specific to our operations. We have put in place processes to identify and address our key risks. These include, for instance, ‘technology shift’ because of fast technology changes and ‘foreign exchange’ because we operate in many different countries worldwide.

We review our principal risks regularly. As the Company operates in a dynamic environment, there may be circumstances in which previously unidentified risks arise or the impact of identified risks is greater than expected.

To provide reasonable assurance to the Board as to the integrity of Gemalto's reporting and effectiveness of its systems of risk management, we have implemented a range of policies and processes with both internal and independent controls. The latter comprise Internal Audit, external certification bodies and external auditors. Together, these aim to support the achievement of our business objectives while reducing to acceptable levels the risks of operational failures, misstatements, inaccuracies and errors, fraud and non-compliance with laws and regulations in a way which balances the cost and effectiveness of the controls.

**The foundations of our approach**

- Our overall *strategy and objectives* set the parameters within which we identify and manage risk. They are described on pages 06-13.

- Our *culture and values* shape the manner in which risk management policies and internal control procedures are implemented. They form part of our wider approach to *sustainability*.

- Our *control environment* is governed by charters, as well as operational and financial policies and procedures, that set risk management and control standards for the Group’s worldwide operations. They are published on our intranet and updated as required.

To promote effective implementation we organize regular training and awareness sessions throughout the Company on topics such as security, internal control, ethics, anti-fraud, authority limits, contract management, crisis management, governance, trade compliance and competition rules.

**What we focused on during the year**

We continue to drive improvements to our risk management process and the quality of risk information generation, while at the same time maintaining a simple and practical approach. During the year we focused on a number of key areas, and in particular on:

- Enhancing the business continuity framework and organization.

- Performing several new risk assessments on key businesses highlighted in the 2014-2017 Development Plan.

**What we plan to do in the future**

We will continue to evolve and build on our existing risk management framework, enhancing risk management culture across the business in line with best practices. Our next set of priorities includes:

- Completing our Enterprise Risk Assessment on Platforms & Services businesses.

- Deploying our Business Continuity Framework on strategic sites and organizations.

- Streamlining our Internal Control framework.

“We see effective risk management as part of our responsibility to customers, as well as to investors, employees and other stakeholders. Our customers trust us to make it integral to our service and our culture.”

OLIVIER PIOU
CHIEF EXECUTIVE OFFICER
How we share our risk management responsibilities

We regard risk prevention and management as part of our culture; a responsibility that is shared by management throughout the organization. We have made sure that Gemalto is set up in such a way as to optimize our ability to manage risks.

The Board
- Approves strategic objectives and validates our risk appetite.
- Reviews the Company’s risk management and internal control systems.
- Assesses these systems’ effectiveness through its Audit committee.

Senior Management
- Oversees suitable design and sustainable implementation of Enterprise Risk Management (ERM) and internal control systems across the Company.
- Defines and allocates risk appetite within the Group.

BUSINESS AND OPERATIONS MANAGEMENT
- Identifies and manages risks for its scope of responsibility.
- Maintains effective internal control day-to-day.

BUSINESS SUPPORT FUNCTIONS
- Defines internal control systems in their scope of expertise ensuring their continuous appropriateness to the Company’s risks.
- Develops risk management culture and awareness of those internal control systems.

RISK PREVENTION AND MANAGEMENT AND INTERNAL CONTROL DEPARTMENT
- Develops and promotes the ERM framework to support management in the identification, assessment, management, monitoring and reporting of risks.
- Facilitates consistent and periodic reviews of the design and implementation of internal control systems.

INTERNAL AUDIT
- Provides independent assurance of the effectiveness of risk management and internal control frameworks and activities in the Group.

BUSINESS AND OPERATIONS MANAGEMENT
1. Budgeting, planning and reporting
   See page 38
2. Risk assessment and mitigation
   See page 38
3. Crisis and business continuity management
   See page 39
4. Fraud risk management
   See page 39
5. Transfer to insurance
   See page 40

FOUNDATIONS
Our processes are underpinned and informed by:
- STRATEGY AND OBJECTIVES
- CULTURE AND VALUES
- INTERNAL CONTROL
- SUSTAINABILITY

Gemalto Annual Report 2014
Once validated, operating results which have been consolidated by the Corporate Accounting department, reviewed by the Group Treasurer, Group Tax Director and Group Controller, are presented to the CFO and COO for review. The Group Controller, CFO and COO then present them jointly to the CEO. The Group Treasurer prepares a monthly report which includes a review of the financial results for the period, the efficiency of the balance sheet and cash flow hedges, the client receivables position and the Group’s cash and debt positions.

Drawing on the review of the operating results and the treasury report, the Group Controller and CFO prepare the operating dashboard and accompanying CEO and CFO letter. These are reviewed by the CEO before being circulated to the Board and Senior Management. The dashboard and accompanying letter cover the activity by segment, the updated operating income statement forecast for the current quarter, and the cash, debt and working capital positions. A review of the activity is presented by the CEO, COO and CFO at each Board meeting.

In the last days of each quarter the Head of Consolidation holds pre-close reviews with each segment and region. Combined with the monthly result calls, these allow prompt identification and communication of any transaction or event which could significantly impact the Group’s results or financial condition.

2. Risk assessment and mitigation

Our risk management process involves:

- Mapping and anticipating the main identifiable risks, with regular updates;
- Prioritizing them against the Group’s strategy and risk appetite;
- Allocating risk ownership;
- Developing and implementing mitigation plans that are proportionate to the risks involved, including transfer to insurance market;
- Communicating key control objectives to operational managers;
- Regularly checking the effectiveness of the process.

Identifying and assessing our major risks enables us to focus on those that matter and to align our action plans and resources accordingly. Risk assessment is carried out at all management levels as shown in the chart below, and is supported by the use of an ERM software tool.

- **Group level:** major new investments, like major assets, acquisitions and developments, are analyzed from a risk perspective, and reviewed with the segments. Following the publication of each new multi-year development plan, new enterprise-wide risk assessments (ERA) are conducted either at Group level or per segment.

- **Business level:** risk assessments are performed on major bids and contracts as well as on new activities.
3. Crisis management and business continuity

Since we cannot identify all the risks we may face, our crisis management processes and business continuity responses are there to improve our resilience to unforeseen events.

This proactive approach enabled us to respond effectively to issues when they arose, minimizing their impact on our stakeholders and reputation.

Our crisis management framework encompasses basic escalation and communication rules, guidelines for anticipation and action, and clear roles and responsibilities.

Over 120 crisis management leaders are in place worldwide, trained through simulation exercises.

In 2014, we continued to update and refine our crisis management framework and improved the preparation level of the Company.

In particular, all Crisis Management Leaders were asked to formally submit their updated Crisis Management Plans to the Corporate Risk Management team.

We have also developed business continuity responses to avoid or minimize disruption to customers and our business in the event of a crisis. These measures include greater standardization of production tools and processes for greater flexibility between sites; multi-sourcing strategies so that we are not dependent on a single supplier; and the creation of redundancy in our infrastructure so that support is available in the event of a problem.

We reinforce this by storing certain types of key information in back-up sites, so enabling our operations to continue uninterrupted even in the face of difficulties. In 2014, we also continued to reinforce our business continuity framework with improved tools, templates and educational support across the Company. Continued governance and oversight of business continuity development is provided by our Business Continuity Leadership team.

4. Fraud risk management

The anti-fraud framework aims at preventing, detecting, deterring, reporting and responding to fraudulent activities. The Gemalto Anti-fraud commission oversees this framework. It comprises the Group General Counsel; the EVP Human Resources; the Chief Information Officer; the Internal Audit Director; the Security Director; and the Compliance Officer. Its objectives encompass continuous fraud risk assessment, anti-fraud policy and procedures, and action in response to actual or suspected frauds.

In 2014, around 430 key personnel received training in anti-fraud or anti-bribery and over 1,000 people were trained in Ethics, Bribery Law, CFRUS and Trade Compliance topics. In addition, newsletters including these topics were sent to around 1,800 employees.

The anti-fraud policy requires all managers to inform the Anti-fraud commission of any suspicion of fraud. Employees can also use the whistle-blowing line to raise any financial irregularities to a confidential advisor.
Managers are primarily responsible for investigating and responding to any suspected fraud cases in their own department. Following a fraud, he or she must make appropriate corrective changes to systems, controls, education and procedures to prevent re-occurrence of a similar fraud. The Anti-fraud commission monitors the effectiveness of such actions.

The main investigated fraud cases are reported periodically to the CEO, the CFO, the external auditor and the Audit committee.

5. Transfer to insurance
The Group policy on insurance coverage focuses on optimizing and securing the policies we contract. The aim is to protect the Company against exceptionally large or numerous claims, at a cost that does not impair Group competitiveness. The Group neither owns nor operates any captive insurance. Our global insurance programs involve only high-quality and financially sound insurers and combine master policies and local insurance policies where countries require this.

The negotiation and coordination of these programs is 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. Gemalto reviews its insurance coverage strategies periodically, taking into account changes in its risk profile (such as acquisitions, claims, loss events and other activities) and insurance market trends.

Our insurance programs encompass property damage, business interruption, public, product and professional liability, and Directors’ and officers’ exposures.

How we monitor effectiveness

1. Risk management
The Risk, Internal Control and Trade Compliance department reporting both to the General Counsel and the CFO has a global view of risks since its responsibilities encompass several key processes from ERAs to transfer to insurance including internal control, crisis management and business continuity. This transversal view is a strong asset in the understanding of the risk and the Company’s capabilities to manage it.

It facilitates the development of a pragmatic overall risk management approach.

2. Internal control
Gemalto has established a strong framework of internal control across all of its business areas and functions. This framework is based upon a clear statement of ethical business principles, established procedures and training of the key personnel who are responsible for implementing and overseeing it.

Our internal control system was implemented according to a risk based approach, taking the COSO model as the reference. Updated yearly, it will continue to evolve in line with the new recommendations of the COSO 2013 and according to needs induced by the Company’s development.

While it cannot provide absolute assurance and while keeping a reasonable balance between cost and assurance, it nevertheless aims at ensuring that the realization of objectives (including sustainability goals) is monitored, financial reporting is reliable and applicable laws and regulations are complied with.

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

Our Internal Control team develops awareness on internal control matters in the Company and uses yearly risk-based self-assessment campaigns to ensure that the proper level of internal control is maintained and regularly enhanced.

Ethical practices and employee confidence

In the 2014 internal PeopleQuest survey (see page 33) employees confirmed their confidence in the Company’s ethical practices and performance. They said that Gemalto and its Management:

- are committed to ethical practices 91%
- set a good example 90%
- provide adequate information about ethical practices 87%
The production and control of financial information is structured to be consistent with our segments. To ensure the quality and completeness of the financial data produced and reported, we have set up a process for the production and management review of operating results, identified the main risks which significantly impact the financial statements, and implemented preventive and corrective controls to mitigate those risks.

To improve internal control, we run an annual self-assessment campaign. Facilitated by a dedicated software solution, it mostly addresses financial risks, IT/IS risks, resilience capabilities and some legal and governance matters (e.g. ethics, sustainability). For a number of our most critical processes and entities, the self-evaluations of the controls are tested by internal auditors. This process helps us to define plans for remedying identified deficiencies and to follow up the progress of those plans year-on-year, with a special focus on newly acquired companies.

An annual report on financial internal controls and internal audit activity is prepared by the Internal Audit Director, reviewed and agreed with the CFO, and then with the CEO. It is presented to the Audit committee as part of the review process of the annual accounts.

3. Financial control
Internal Audit and Corporate Risk Management, together with Financial controllers, are responsible for identifying the risks which significantly impact the financial statements, and implement preventive and corrective control to mitigate those risks. They are also responsible for assuring Senior Management that the controls over the Group’s earnings and operating performance remain adequate. They participate in drawing up the budget and quarterly business reviews; and they oversee the monthly financial results of segments, regions and the Group as a whole. 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 on effectiveness
A number of bodies provide reasonable assurance on the design and effectiveness of the risk management processes and compliance with the relevant standards, policies and norms.

1. Internal audit
To assess and test our internal risk management and control systems we have a dedicated and certified Internal Audit department operating under a charter approved by the Audit committee (updated in 2012). Its work conforms to the International Standards for the Professional Practice of Internal Auditing as published by the Institute of Internal Auditors (IIA). Consisting of eight auditors with diverse backgrounds based in Amsterdam, it has direct and unlimited access to Group operations, documents and employees. The Internal Audit Director reports directly to the CFO and has an independent line of communication with the Audit committee Chairman and with the CEO, as well as regular private sessions with the Audit committee.

In December 2013, the committee approved a new three-year plan covering the period 2014-2016. It drew on the findings of the ERA, the yearly financial risk mapping, discussions with management and regular audits of major sites.

For each audit, a formal report is issued and circulated. This includes recommendations for corrective actions with an implementation plan and the comments of the auditees. Implementation of accepted corrective actions is followed up systematically and documented in a formal report. The Internal Audit department performs follow-up reviews of acquisitions at the request of Senior Management, the Audit committee or the Strategy and M&A committee.

The Internal Audit Director prepares a monthly report – including a summary of his department’s activity, key internal control issues and their status – for the Chairman of the Audit committee and the CFO. An annual report on internal audit and internal control is also submitted to the CEO and the Audit committee. Audit missions include ethics and fraud reviews.

In December 2013, the Institut Français de l’Audit et du Contrôle Internes (IFACI), the French representative of the Institute of Internal Auditors (IIA renewed the professional certification of Gemalto’s internal audit team, processes and activities.

2. External certifications
Because of the nature of our activities, we maintain a number of certifications, some of which (including EMV, GSM SAS, ISO 9001, ISO/TS 16949, ISO 14001, OHSAS 18001 and ISO 27001) are necessary for the conduct of our business. These vary from site to site and by business type, according to local regulations and customer requirements. The effectiveness of our Quality and Health, Safety and Environment (HSE) management systems is constantly challenged by external and internal audits. Both look for continuous improvement through identification of sensitive areas and deployment of best practices.

3. External auditor
The independent external auditor is granted unrestricted access to Gemalto sites and documentation. The external auditor communicates regularly with the Internal Audit department and with the Audit committee, being invited to all the Audit committee meetings and to private sessions.

The Audit committee assesses the work of the external auditor at least once a year. The external auditor provides an independent opinion on the financial results of the Group, and its report is available on page 119.

Following developments in Dutch law, PwC’s mandate will come to an end at the end of 2015, and another audit firm is to be appointed. A tender was organized in 2014 with global, reputable audit firms under the supervision of the Audit committee. A mandate to appoint KPMG, the new audit firm selected, will be submitted for approval to the AGM in May 2015.
### Principal risks

#### Strategic Risks

<table>
<thead>
<tr>
<th>RISK AREA</th>
<th>MAIN MITIGATING ACTIONS</th>
</tr>
</thead>
</table>
| Economic and political environment, competition and commoditization of products (possible adverse impact on our growth and profitability) | • Formal long-range Development Plan.  
• Diversified portfolio of activities and geographic footprint (presence in 46 countries). |
| Acquisitions and/or joint ventures (inappropriate or untimely M&A strategy, poorly executed integration process) | • Dedicated team manages corporate Development Plan and M&A.  
• Formal process to manage acquisitions and integrations. |
| Technology changes, innovation, R&D (failure to manage efficiently our innovation process and R&D projects) | • Competitive and market intelligence program.  
• Diversified technology portfolio (including through M&A).  
• Strong R&D and standardization teams.  
• Focus on innovation: Gemalto filed 114 new patent applications in 2014. |

#### Legal and Compliance Risks

<table>
<thead>
<tr>
<th>RISK AREA</th>
<th>MAIN MITIGATING ACTIONS</th>
</tr>
</thead>
</table>
| Intellectual property rights risks (failure to protect Gemalto’s proprietary technology and IP rights; third-party claims for alleged infringement of their IP rights) | • Dedicated and qualified internal IP team organized by technology.  
• Internal IP department, internal inventor policies and formal Open Source software policy. |
| Business integrity and ethics (internal fraud, bribery, anti-trust violations; actions or inactions perceived by stakeholders to be inappropriate) | • Policies and procedures, Code of Ethics, whistle-blowing tool, employee survey.  
• Anti-fraud commission; Compliance Officer directly reporting to CEO.  
• Security certifications and organization. |
| Regulatory risks associated with our international operations and industry (failure to comply with regulatory changes, export controls and data protection regulations, impact of decisions from tax authorities, regulatory and other administrative bodies) | • Legal organization in regions and by activity.  
• Training on tax and other regulations.  
• Tax department with regional antennas.  
• Awareness program and compliance action plan lead by Director of Global Data Privacy. |

#### Operational Risks

<table>
<thead>
<tr>
<th>RISK AREA</th>
<th>MAIN MITIGATING ACTIONS</th>
</tr>
</thead>
</table>
| Business continuity and resilience to crisis (failure to limit impact on our operations and reputation of any internal or external critical events or situations which may materialize unexpectedly) | • Risk assessments with regular updates.  
• Crisis management framework and associated workflow training program.  
• Diversified industrial footprint.  
• Enhancement of IT technology and infrastructure resilience. |
| Sourcing and supply management (lack of supplier resilience to disaster, insolvency, non-compliance with ethical standards, inadequate management of suppliers) | • Business intelligence on suppliers.  
• Multiple sourcing strategy.  
• Safety stocks management and protection clauses in contracts. |
| Major contracts (failure on amount, duration, technology or commitments) | • Bid and contract reviews with approval process according to limits of authority.  
• Prudent revenue recognition policies for Embedded software & Products and Platforms & Services businesses. |

This table outlines what Gemalto’s management believes to be the principal risks to the Company and the actions taken to mitigate them. It is not an exhaustive list of all the risks that may affect Gemalto but aims to report the main ones that stem from our activities.1
## Operational Risks Continued

### Risk Area

<table>
<thead>
<tr>
<th>Risk Area</th>
<th>Main Mitigating Actions</th>
</tr>
</thead>
</table>
| Quality of products, platforms & services (failure to develop and deploy secure, stable or reliable technology products and solutions) | - Standardized manufacturing processes.  
- Quality management system and world-class enterprise organization.  
- 30 sites with ISO 9001 certification in 2014.  
- Participation in standardization committees.                                                                 |
| Exposure to country risk (political, regulatory and trade exposure impacting our staff, footprint and receivables) | - Country risk alert monitoring and communication.  
- Travel policy, travel approval process, regional travel champions.  
- Agreements with specialized security consulting companies.  
- Specific training sessions.                                                                 |
| Data protection and cyber security (leakage and/or loss of customers’ or Gemalto’s confidential data resulting, for example, from cyber attacks, employees’ negligence or vulnerability of our information technology systems) | - Security and cryptography expertise.  
- Extensive set of security and IT policies with regular training sessions.  
- Worldwide security organization with security officers in all important sites and regional/corporate security support.  
- Corporate Security Incident Response Team.  
- Security certifications by third-parties (including ISO 27001, EMV, GSM, SAS, etc.).  
- Internal security audits (extended to IT subcontractors).  
- Anti-fraud commission.                                                                 |
| Talent management (inability to attract, develop and retain highly qualified management and suitably skilled employees.) | - Comprehensive Human Resources strategy.  
- Focus on recruitment, management by objectives, compensation and benefits.  
- Succession plan for managers (including for Senior Management).  
- Focus on diversity, ethics and community.  
- Focus on training, promotion from within and mobility.                                                                 |
| Customer retention (inability to maintain relationships with existing customers and to identify, attract and retain new customers) | - Diversified portfolio of clients.  
- Operations from worldwide locations.  
- No customer represents more than 10% of Group’s annual revenue.                                                                 |
| Foreign exchange risk (devaluation of receivables, future cash flows and other assets) | - Centralized currency risk management and reporting.  
- Treasury committee and treasury policies.  
- Manufacturing footprint providing natural hedging.  
- Hedging strategies and transaction hedging (foreign exchange forward contracts and options recorded as cash flow hedges). |
| Financial counterparty risk (inability of customers and banks to fulfill their financial obligations) | - Risk limits set for counterparties regularly reviewed.  
- Use of plain vanilla hedging instruments and low-risk money market investment.  
- Working with financial institutions of investment grade (deposits, hedging transactions).  
- Set-off provisions in financial contracts.                                                                 |
| Financial reporting risks (inability to produce timely and accurate financial statements, inaccurate assessment of tax exposures and other complex accounting issues) | - Financial policies and procedures.  
- Single financial reporting tool Company-wide.  
- Revenue recognition policies.  
- Consolidation department with dedicated specialists.  
- Regular balance sheet analysis and management reviews.                                                                 |

### Financial Risks

<table>
<thead>
<tr>
<th>Risk Area</th>
<th>Main Mitigating Actions</th>
</tr>
</thead>
</table>
| Foreign exchange risk (devaluation of receivables, future cash flows and other assets) | - Centralized currency risk management and reporting.  
- Treasury committee and treasury policies.  
- Manufacturing footprint providing natural hedging.  
- Hedging strategies and transaction hedging (foreign exchange forward contracts and options recorded as cash flow hedges). |
| Financial counterparty risk (inability of customers and banks to fulfill their financial obligations) | - Risk limits set for counterparties regularly reviewed.  
- Use of plain vanilla hedging instruments and low-risk money market investment.  
- Working with financial institutions of investment grade (deposits, hedging transactions).  
- Set-off provisions in financial contracts.                                                                 |
| Financial reporting risks (inability to produce timely and accurate financial statements, inaccurate assessment of tax exposures and other complex accounting issues) | - Financial policies and procedures.  
- Single financial reporting tool Company-wide.  
- Revenue recognition policies.  
- Consolidation department with dedicated specialists.  
- Regular balance sheet analysis and management reviews.                                                                 |

1 For further information about other financial risks that do not fall into this section (i.e. interest rate risk, liquidity risk and credit risk) and the relevant mitigating actions, see Note 4 Financial risk management pages 81-84.