Principal risks and uncertainties

RESPONSIBLE RISK MANAGEMENT

RISK MANAGEMENT

Temenos Risk management policy is aligned with ISO: 31000 Risk management – Principles and guidelines. It defines the methodology, roles and responsibilities, reporting and monitoring for key risks. Temenos' operational management is responsible for managing day-to-day risks. Periodical risk assessments are performed within business units and summarized results reported to management along with mitigation plans where appropriate. The Audit Committee oversees the program and reviews key risks of the Group.

We have implemented a robust internal control and risk management system for financial reporting that goes beyond statutory requirements. All relevant risks are identified, formally assessed and documented. For each risk we have implemented specific controls and mitigation plans. Their effectiveness is regularly evaluated through a self-assessment process which is independently tested by internal and external auditors.

The following sections outline the risks that we have identified and track. They represent an aggregated view.

ECONOMIC, POLITICAL AND SOCIAL ENVIRONMENT

Temenos derives all of its licensing, SaaS, maintenance and services revenues from banks and other financial institutions. The banking industry is sensitive to changes in global economic conditions, financial markets and is highly susceptible to unforeseen external events, such as political instability, terrorist attacks, recession, inflation or other adverse occurrences that may result in a significant decline in the use and/or profitability of financial services. Any event that results in decreased consumer or corporate use of financial services, or cost-cutting measures by financial services companies, may negatively affect the level of demand for Temenos products and services.

In recent years, there have been substantial changes in the banking industry, including continuing consolidation among market participants, the introduction of wide ranging regulatory changes and extensive technological innovation. These changes have inter alia resulted in increased IT spending by banks and driven market participants to replace legacy systems, leading to increased demand for Temenos' solutions. If the pace of change were to decrease, demand for Temenos' products and services may decrease, which could have a material adverse effect on Temenos' business, financial condition and results.

Temenos' global presence, comprehensive product offering and market leadership help to mitigate this risk.

LAW AND LITIGATION

Temenos operates in various legal jurisdictions and as such is subject to various legal and regulatory requirements. Temenos may have legal proceedings or litigious actions brought against it. The outcome of these proceedings or actions are intrinsically uncertain and the actual outcomes could differ from the assessments made by management in prior periods, resulting in increases in provisions for litigation in the accounts of Temenos. Adverse outcomes to legal proceedings or litigious actions could result in the award of significant damages or injunctive measures that could hinder Temenos' ability to conduct business and could have a material adverse effect on its reputation, business, financial position, profit, and cash flows.

Litigation of intellectual property infringement claims may increase as a result of Temenos acquiring companies which rely on third-party code including open source code, Temenos expanding into new areas of the banking industry resulting in greater overlap in the functional scope of products, and increasing assertion of intellectual property infringement claims by non-practicing entities that do not design, manufacture, or distribute products.

Although Temenos has implemented controls and believes that its products do not infringe upon the intellectual property rights of others, and that Temenos has all the rights necessary to utilize the intellectual property employed in its business, Temenos is still subject to the risk of claims alleging infringement of third-party intellectual property rights, including in respect of intellectual property that has been developed by third parties and acquired by Temenos in business or asset purchase transactions. Responding to such claims, regardless of whether they are with or without merit and negotiations or litigation relating to such claims could require Temenos to spend significant sums in litigation costs, payment of damages and expend significant management resources.

Temenos legal teams are aligned to business operations and are involved early in any decisions which may incur legal implications. The legal team reviews and provides guidance on complex client contracts to ensure contractual agreements align to local commerce laws and regulations. Whenever possible, Temenos tries to contractually limit its liabilities. This is covered further in Foreign Operations.

More broadly, the risk of potential breach of legislative or regulatory requirements through general operations, such as breach of listing requirements or group level legal requirements are managed through group level controls, compliance policies and procedures.

Policy compliance requirements are periodically assessed through Risk Management processes and reviewed by Internal Audit to provide comfort over adequacy of policies, processes and compliance.

IP PROTECTION

Temenos relies upon a combination of copyright, trademark and trade secrecy laws, trade secrets, confidentiality procedures, contractual provisions and license arrangements to establish and protect its proprietary rights and Temenos' ability to do so effectively is crucial to its success. Temenos enters into agreements with its employees, Partners, distributors and clients that seek to limit the distribution of and otherwise protect its proprietary information. However, Temenos cannot give full assurances that the steps taken will be adequate to prevent misappropriation of its proprietary information as all of the protection measures afford only limited protection. Temenos' proprietary rights could be challenged, invalidated, held unenforceable or otherwise affected. Certain proprietary technology may be vulnerable to disclosure or misappropriation by employees, Partners or other third parties and third parties might reverse-engineer or otherwise obtain and use technology and information that Temenos regards as proprietary. Accordingly Temenos might not be able to protect its proprietary rights against unauthorized third-party copying or utilization, which may undermine Temenos' market position and deprive it of revenues.

Temenos may not be able to detect unauthorized use of its intellectual property, or take appropriate steps to enforce Temenos' intellectual property rights. Temenos' products are used globally and are therefore subject to varying laws governing the protection of software and intellectual property in each of these jurisdictions. Temenos cannot guarantee that its software and intellectual property will be afforded the same level of protection in each jurisdiction, as some jurisdictions may offer no effective means to enforce Temenos' rights to its proprietary information, which could result in competitors offering products that incorporate features equivalent to Temenos' most technologically advanced features, which could have a material adverse effect on Temenos' business, results of operations and financial condition.

Principal risks and uncertainties continued

IP PROTECTION CONTINUED

Any legal action that Temenos may bring to enforce its proprietary rights could involve enforcement against a Partner or other third party, which may have a material adverse effect on its ability, and its clients' ability, to use that Partner's or other third parties' products. Moreover, litigation, which could involve significant financial and management resources, may be necessary to enforce Temenos' proprietary rights. Any material infringement of Temenos' proprietary technology could have an adverse effect on its reputation, business, financial position, profit and cash flows. Our Partner contracts are designed in a manner which provides clarity and understanding of both parties with regard to the protection and safeguarding of their IP.

UNDETECTED DEFECTS OR SECURITY VULNERABILITIES

Temenos' products and offerings may contain defects or security vulnerabilities that Temenos has not been able to detect and that could adversely affect the performance of the products and negatively impact Temenos' relationship with its clients.. It is not always possible to identify and rectify all errors or defects during a product or services developmental phase, and more commonly Temenos has discovered minor software defects in certain new versions and enhancements of its products after they have been introduced. The detection and subsequent correction of any errors or defects can be expensive and time consuming, and it is not always possible to meet the expectations of clients regarding the timeliness and the quality of the defect resolution process. In a worst case scenario, it might not be possible to wholly rectify certain defects or entirely meet client expectations. In such circumstances it is possible that clients may pursue claims for refunds, damages, attempt to terminate existing arrangements, request replacement software or seek other concessions.

A defect or error in any newly developed software of Temenos could result in adverse client reactions and negative publicity, as Temenos' clients and potential clients are highly sensitive to defects in the software they use. Any negative publicity could hinder the successful marketing of the new software, reducing demand for the software. A defect or error in new versions or enhancements of Temenos' existing products could result in the loss of orders or a delay in the receipt of orders and could result in reduced revenues, delays in market acceptance, diversion of development resources, product liability claims or increased service and warranty costs, any of which may have a material adverse effect on Temenos' business, results of operations and financial condition. Any claim brought against Temenos in connection with defective software, regardless of its merits, could entail substantial expense and require a significant amount of time and attention by management personnel.

We continually enhance our quality program as part of the Software Development Life Cycle. We have centralized our product security group and practices. Extensive testing is carried out to identify and resolve any issues which may adversely affect the functionality, security and other performance of our products and offerings.

KEY PERSONNEL

Temenos operates in an industry in which there is intense competition for experienced and highly qualified individuals. The success of Temenos is partly dependent on its ability to identify, attract, develop, motivate and retain highly skilled and qualified management and other personnel, particularly those with expertise in the banking software industry. If Temenos fails to recruit and retain the numbers and types of employees that it requires, its business, operating results and financial condition may be adversely affected.

Incentive and recognition programs are utilized to align staff efforts to organizational objectives. Staff receive various training to ensure they have the necessary skills to perform their duties. We have launched various CSR initiatives to demonstrate our commitment to employees. Career and succession planning are carried out annually to provide for continuity of operations

FOREIGN OPERATIONS

Temenos systems are currently installed at more than 3,000 live sites in 150 countries and it has sales and support offices in over 40 countries. Temenos' future revenue growth depends on the continued successful expansion of its development, sales, marketing, support and service organizations, through direct or indirect channels, in the various countries around the world where its current and potential clients are located, including in many developing countries. Such expansion will require the opening of new offices, hiring new personnel and managing operations in widely disparate locations with different economies, legal systems, languages and cultures, and will require significant management attention and financial resources. Temenos' operations are also affected by other factors inherent in international business activities, such as:

- Differing or even conflicting laws and regulation of risk and compliance in the banking sector
- Difficulties in staffing including works councils, labor unions and immigration laws and foreign operations
- The complexity of managing competing and overlapping tax regimes
- Differing import and export licensing requirements;
- Operational difficulties in countries with a high corruption perception index
- Protectionist trade policies such as tariffs;
- Limited protection for intellectual property rights in some countries
- Difficulties enforcing intellectual property and contractual rights in certain jurisdictions
- Differing data protection and privacy laws
- Political and economic instability, outbreaks of hostilities, terrorism, mass immigration, international embargoes, sanctions and boycotts.

The risks associated with the factors stated above will intensify as Temenos expands further into new countries and markets through organic growth or acquisitions. Additionally laws and regulations and governments' approaches to their enforcement, as well as Temenos' products and services, are continuing to change and evolve. Compliance with the laws and regulations in the various jurisdictions may involve significant management time, costs and require costly changes to products and/or business practices.

Risks related to foreign operations are regularly assessed and mitigated as needed. Specific policies and procedures are in place to ensure compliance with export control and sanctions, anti-bribery and corruption, anti-money laundering, data protection and privacy and other legislation.

Foreign exchange and/or interest rate fluctuations

Temenos' financial statements are expressed in US dollars and Temenos generates the majority of its revenues in US dollars. However, a significant portion of its operating expenses are incurred in currencies other than the US dollar, particularly in Euros, Swiss francs, Rupees and Pounds Sterling.

Furthermore, Temenos is exposed to the fluctuation in exchange rates of each of these currencies. Temenos makes efforts to mitigate its foreign exchange risk by aligning its revenue streams to currencies that match its cost base and hedges most of the residual exposure. However, such hedging may not be sufficient protection against significant fluctuations in the exchange rate of the US dollar to other currencies, in particular those currencies in which Temenos incurs operating expenses, generates revenues or holds assets. Such fluctuations may impose additional costs on Temenos and have a material adverse effect on Temenos' financial condition and results of operations, and on the comparability of its results between financial periods.

Temenos uses a combination of various techniques to protect against currency and rates fluctuations.

COMPLIANCE WITH THE TERMS OF TEMENOS CREDIT FACILITIES

Temenos has credit facilities in place with a syndicate of banks. The facilities contain financial and negative covenants, undertakings and event of default provisions. Moreover, the facilities contain cross-default provisions such that a default under another debt instrument, such as bonds, could result in a default under the credit facilities and acceleration of the debt thereunder.

The inability of Temenos to draw under the credit facilities to satisfy its financing requirements, could have an adverse effect on Temenos' growth. Compliance with the terms is monitored on monthly basis.

Principal risks and uncertainties continued

MANAGING CLIENT RELATIONSHIP

Temenos enters into long term relationships with its clients. The contractual arrangements supporting these relationships are often varied and diverse to reflect the nature of the requirements of the client factoring in specific legal and cultural requirements of the client's operating environment as well as the multiple stages of the relationship.

Temenos has increased its focus on assessing client satisfaction and is proactively seeking and responding to client feedback.

Improved mechanisms for tracking and oversight of contract clauses are utilized by the global contract team to provide additional comfort over the effective management of client contractual arrangements.

Temenos aims to build long term strategic relationships with clients in order to maximize the value provided to both parties. Through strong relationships, Temenos is able to further develop products according to industry needs and requirements.

STRATEGIC PARTNERSHIPS

Temenos delivers its products to clients directly and indirectly through distributors and through strategic alliances with IT service providers. Temenos' strategic Partners sell to clients and provide implementation services through a contract with the client, rather than with Temenos. These relationships with IT service providers and strategic Partners help to drive co-innovation of Temenos' products, profitably expand Temenos' routes-to-market to enhance market coverage and provide high quality services in connection with Temenos' product offerings. Any failure to maintain and expand these relationships could adversely affect Temenos' products and services which, in turn, would have an adverse effect on Temenos' ability to compete successfully with its competitors and therefore negatively affect the results of operations and financial condition.

CLOUD AND SAAS SOLUTIONS

Cloud and SaaS technology is inherently complex and relatively new to the banking and financial market sector. Accordingly, Temenos may be subject to changing regulatory requirements, evolving client attitudes and technical complexities in developing a new business offering and support services. Temenos may fail to achieve desired operating profit results in this new market due to regulatory changes, inability to develop a competitive product or which appeals to its clients.

By providing cloud technology to clients, Temenos will hold client data. Hardware or data center failures, product defects or system errors could result in data loss or corruption, or cause the information held to be incomplete or contain inaccuracies. The availability of Temenos' application suite could be interrupted by a number of factors, such as the failure of a key supplier, its network or software systems due to human or other error and security breaches.

Although Temenos employs strict security, data protection and privacy measures there is a risk that such measures could be breached as a result of third party action, employee error and malfeasance, or otherwise, and if as a result unauthorized access is obtained to client data, which may include personally identifiable information about users, Temenos could suffer significant reputational damage and be exposed to liabilities.

Temenos is constantly enhancing its cloud and SaaS offering and security. In addition, Temenos holds SSAE 18 SOC 1 and 2, ISO 9001 and ISO 27001 certifications to provide a greater degree of assurance to clients.

SOFTWARE IMPLEMENTATION PROJECT MANAGEMENT

The implementation of Temenos' software and integration of various product components is a complex process requiring skilled and experienced personnel. The implementation of Temenos' software is often performed in part or wholly by service delivery Partners as well as committed resources of the client. The complex nature of the solutions makes it necessary to provide training and education on the operation of the product.

The reliance on third party capabilities, and the complex nature of product customization and installation requirements mean that there is a high potential for unforeseen events to occur delaying the progress of implementations.

Temenos focuses heavily on training the staff and Partners responsible for implementation of software to ensure a strong mix of qualified project managers and technical product expertise. Temenos ensures the adequacy of skills through requiring certification of staff and Partners in Temenos Implementation Methodology and products. Launch of Temenos Learning Community (TLC) shows our further commitment to this area.

Implementation teams are also trained to identify and effectively manage any unforeseen events and a suite of risk management tools are used to monitor and track potential issues which may adversely impact the successful installation of software. Project governance boards are held monthly to oversee the delivery of the implementation against milestones.

Temenos Implementation Methodology is periodically reviewed and updated in order to maintain high standards for Temenos staff and Partners. Identified initial project risks receive an increased level of review and analysis in order to more effectively mitigate and monitor them throughout the life of the implementation project.

MERGERS AND ACQUISITIONS

Temenos pursues a strategy of making targeted acquisitions. The risks associated with such a strategy include the availability of suitable candidates and successful integration. Risk of failure to assimilate operations and personnel, may materialize. The process of integrating an acquired company or business may create unforeseen operating difficulties and expenditures.

Further consolidation in Temenos' industry may decrease the number of potential desirable acquisition targets. Failure to acquire, integrate and derive the desired value of any businesses or assets in the future could materially adversely affect Temenos' business, results of operations and financial condition.

In addition, acquired businesses might not perform as anticipated, resulting in charges for the impairment of goodwill and other intangible assets on Temenos' statement of financial position.

Detailed integration planning is utilized to ensure a smooth transition of product offerings and services. Legal, commercial and personnel matters are also considered prior to integration in order to limit exposure to unexpected losses or damage.

SECURITY, BUSINESS CONTINUITY AND RESILIENCY

As a software technology vendor and SaaS provider, we face various cyber and other security threats, including:

- Attempts to gain unauthorized access to sensitive information and data
- Threats to the safe and secure operation of our software solutions and services
- Threats to the safety of our Directors, officers and employees
- Threats to the security of our facilities and infrastructure
- Threats from terrorist acts or other acts of aggression.

Our clients and Partners (including subcontractors) face similar threats.

Although we utilize various procedures and controls to monitor and mitigate the risk of these threats, there cannot be full assurance that these procedures and controls will be sufficient. These threats could lead to losses of sensitive information or capabilities, harm to personnel, infrastructure or products, and/or damage to our reputation as well as our Partners' ability to perform on our contracts.

Cyber threats are evolving and include, but are not limited to:

- Attempts to gain unauthorized access to data, information or intellectual property
- Disruption to or denial of service
- Other malicious or criminal activities.

These threats could lead to disruptions in mission critical systems, unauthorized release of confidential, personal or otherwise protected information (ours or that of our employees, clients or Partners), and corruption of data, networks or systems. In addition, we could be impacted by cyber threats or other disruptions or vulnerabilities found in products we use or in our Partners' or clients' systems that are used in connection with our business. These events, if not prevented or effectively mitigated, could damage our reputation, require remedial actions and lead to loss of business, regulatory actions, potential liability and other financial losses.

Principal risks and uncertainties continued

SECURITY, BUSINESS CONTINUITY AND RESILIENCY CONTINUED

We provide software products and services to various clients who also face cyber threats. Our software products and services may themselves be subject to cyber threats and/or they may not be able to detect or deter threats, or effectively to mitigate resulting losses. These losses could adversely affect our clients and our Group. The impact of these factors is difficult to predict, but one or more of them could result in the loss of information or capabilities, harm to individuals or property, damage to our reputation, loss of business, regulatory actions and potential liability, any one of which could have a material adverse effect on our financial position, results of operations and/or cash flows.

From an organizational perspective, the Security and Privacy Committee provides the Group level oversight.

In terms of business processes, security assurance is integrated into all business processes related to R&D, the supply chain, sales and marketing, delivery and technical services. In addition, Temenos reinforces the implementation of the cyber security assurance system by conducting internal audits and receiving external certification and auditing from security authorities or independent third-party agencies.

In connection with personnel management, our employees, Partners and consultants are required to comply with security policies and requirements established by Temenos and receive appropriate training so that the concept of security is deeply rooted throughout Temenos. To promote cyber security, Temenos will take appropriate action against those who violate cyber assurance policies. Employees may also incur personal legal liability for violation of relevant laws and regulations. If Temenos security measures are breached and unauthorized access is obtained to Temenos' IT systems, Temenos' business could be disrupted and Temenos may suffer financial losses as a result of the loss of confidential client information or otherwise.

Temenos' insurance coverage might not cover claims against it for loss or security breach of data or other indirect or consequential damages. If Temenos experiences interruptions in the availability of its application suite, Temenos' reputation could be harmed, which may have a material adverse effect on Temenos' business and financial condition.

As part of the periodic Risk Assessment of IT infrastructure, potential physical and security vulnerabilities are factored into the process for developing a resilient and robust IT infrastructure.

The physical security of IT infrastructure and personnel are kept secure through standardized general IT controls across Temenos in line with best practice standards.

A Business Continuity Management framework provides contingency planning for all mission critical business functions and process within the organization.

Information systems are regularly audited internally and externally to provide a reasonable assurance on effective management of these risks.

INSURANCE

Temenos has taken out a variety of insurance policies in areas where a loss would have a significant financial impact, or to ensure safety of employees while on business trips.

Across the various local legal jurisdictions in which Temenos operates, there are various legal requirements to hold certain insurance policies such as workers compensation policies and public liability for example.

Temenos' local offices manage their legally required policies with oversight and review by Temenos Head Office. Each office is reviewed and as necessary covered for property damage, business interruption and public liability risks. Information and IT infrastructure is also covered by regional and local computer policies.

Temenos Head Office also manages all global policies. The main global policies provide coverage across core business areas such as Professional Indemnity liability (covering Errors and Omissions, Cyber Liability and Data Protection), Cyber Insurance, Crime Insurance, Global Travel Insurance and Directors and Officers policy that is providing the professional coverage.

All insurance policies are reviewed periodically to ensure that Temenos, our offices and employees are adequately covered in line with the most actual and comprehensive insurance portfolio software for companies.

INTERNAL CONTROLS FAILURES

Although Temenos considers the controls and procedures it currently has in place to minimize the financial reporting, legal, disclosure and other regulatory, compliance and operational risks associated with its business to be adequate, Temenos recognizes that the efficacy of some of these controls and procedures depends significantly on employees and contractors, and on input from external parties and all of these controls and procedures need to be kept under regular review, particularly given the pace at which Temenos' business has developed and generally increasing regulatory scrutiny.

There is no guarantee that Temenos will not be targeted by those willing to commit fraud against Temenos. Such an action could come from either an internal or external source and could result in a significant adverse impact on Temenos' business, results of operations and financial condition.

Internal controls are regularly reviewed, updated and tested. Internal audit serves as a third line of defense to provide assurance on the effectiveness of risk management and internal controls system.