

RISK MANAGEMENT

Tungsten Corporation plc is proud to operate the world's largest compliant e-invoicing network and to be the trusted partner to hundreds of thousands of global enterprises.

Principal risks and uncertainties

Tungsten Corporation plc is proud to operate the world's largest compliant e-invoicing network and to be the trusted partner to hundreds of thousands of global enterprises. Our customers expect us to proactively manage and predict the risks and uncertainties that are inherent in business.

Risk management at Tungsten Corporation plc starts at the Board, but is delivered throughout the Group.

The Audit & Risk Committee continually monitors and promotes the highest standards of integrity, financial reporting, risk management and internal control.

The Executive Directors and the senior management team oversee the management of the business utilising a wide range of controls, including financial, operational and compliance oversight, together with risk management. They ensure that the risk management strategy is implemented throughout the business.

Tungsten Corporation plc has dedicated compliance and cyber security teams. Amongst other things, these teams are accountable for the maintenance of the appropriate controls and processes to sustain Tungsten Corporation plc's certification under both ISO 27001 (information security management) and ISAE 3402 (controls at a service organisation).

The Security Committee is chaired by the Chief Financial Officer and includes other members of the senior management team as well as key personnel from the business who are responsible for delivery.

All significant sales opportunities are subject to technical and contractual review by senior members of our legal, financial, commercial and technology teams. There are strict internal controls applied to the development of our systems, products and services. In order to assist with the management of risks, the Group continues to recruit individuals who are expert in our markets, technology and support disciplines. The Group has a delegation of authorities that clearly sets out the approval required for key activities, including those restricted to the Board and the Executive Directors.

The disclosure of the key risks and uncertainties in the table below reflects the approach of the Company to also look for the opportunities presented when addressing such risks. This is not an exhaustive list of all the risks faced by the Company.

Tungsten Network considers these risks in accordance with the governance procedures set out on page 31.

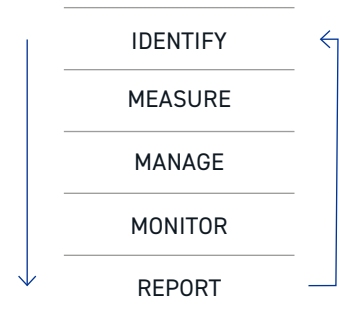
| Risk | Impact |
|--|---|
| Strategic | |
| Direction of change | |
| The Company is stable and is demonstrating progress in executing its business strategy. | |
| The business model fails to meet its strategic objectives. | <ul style="list-style-type: none"> Failure to achieve targets for revenue, profit and earnings Damage to reputation |
| Tungsten Network works with some of the world's biggest companies. There is a risk that Tungsten Network may fail to win and/or retain contracts on satisfactory terms and conditions with the existing as well as new targeted customers and markets. | <ul style="list-style-type: none"> Failure to meet our growth plans Failure to achieve targets for revenue, profit and earnings |
| Failure to invest in enhancements to the infrastructure and operating systems leading to loss of advantage over our competitors and failure to meet the expectation of our customers. | <ul style="list-style-type: none"> Failure to meet our growth plans Failure to achieve targets for revenue, profit and earnings Products and services become unavailable Damage to reputation |

| |
|----------------------|
| Strategic report |
| Governance |
| Financial statements |

RISK MANAGEMENT FRAMEWORK

Tungsten Network’s customers and other stakeholders expect the highest standards of risk management. To facilitate this and evidence assurance, the risks from the risk register are discussed, debated and challenged, firstly by the Executive Committee and then by the Audit Committee before the principal risks are presented to the Board.

The disclosure of the key risks and uncertainties in the table below reflects the approach of the Company to also look for the opportunities presented when addressing significant risks. This is not an exhaustive list of all the risks faced by the Company. Tungsten Network considers these risks in accordance with the governance procedures set out on page 31.



Key risks and their likelihood

| Low | Stable | High |
|---|--|---|
| <p>3 1 2</p> <ol style="list-style-type: none"> 1. Anti-fraud, bribery and corruption 2. Concentration on major customers 3. Failure of critical vendors | <p>5 10 4 6 7 8 9</p> <ol style="list-style-type: none"> 4. Compliance with local tax, legal and regulatory regimes 5. Political, including the impact of the UK leaving the EU 6. Commercial failure of products 7. Complexity of operational processes 8. Change to business execution 9. Retention of key personnel 10. Availability of sufficient liquidity to meet growth expectations | <p>11 12 13</p> <ol style="list-style-type: none"> 11. Data protection and cyber security including GDPR 12. IT system enhancements 13. Change to business execution |

Mitigation

- The strategy is regularly reviewed and challenged by the Executive Committee and Board
 - The strategy forms the basis of the annual business planning process
 - Performance targets are aligned to strategy
 - Strategy is regularly and effectively communicated to all staff
-
- Active management in place to spread revenues across all customers. No one customer accounts for significant revenue or concentration of revenue
 - Structured contracts approval process with clearly defined selection criteria to ensure contracts are taken on or renewed only where Tungsten Network can provide a good service and manage any risks involved
 - Continual review and development of the client relationship management structure and function to improve services to the existing customer base
 - A process is in place to continuously listen and respond to customers to enhance their experience of using Tungsten Network’s products and services
-
- The governance frameworks are key to ensuring successful implementation of all aspects of the planned enhancements and changes
 - Detailed approval and planning process prior to project commencement
 - The Executive Committee and Board review and challenge the status/progress of key change programmes and projects
 - Experts in infrastructure projects and change programmes have been hired to achieve successful implementation
 - Post-implementation reviews are undertaken once a project is completed so that lessons can be learned

RISK MANAGEMENT CONT.

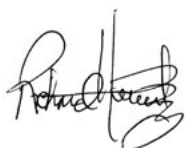
| Risk | Impact |
|--|---|
| Technological & Operational | |
| Direction of change | |
| There are several multi-year projects to upgrade the underlying systems and infrastructure as well as improve operational processes. The majority have been completed, however, these changes can be significant and critical to the success of the business. Therefore, the overall level of technological and operational risk facing Tungsten Network remains high. | |
| Tungsten Network has a highly developed and complex operational and IT infrastructure, which is constantly developed and upgraded. A major incident as a result of an internal or external event could impact the ability of the Company to provide products and services to its customers. | <ul style="list-style-type: none"> • Products and services become unavailable • Customer claims for losses. Loss of customers • Damage to reputation • Failure to meet our growth plans |
| The Tungsten Network has a highly developed and complex IT infrastructure. There is a risk of information security breach including cyber-attacks leading to loss of confidentiality, integrity or availability of data. | <ul style="list-style-type: none"> • Products and services become unavailable • Customer claims for losses. Loss of customers • Damage to reputation • Failure to meet our growth plans |
| Tungsten Network is constantly developing and upgrading many aspects of its technology software and hardware. As a result, there is a risk of failure or inefficiencies in its operations, systems and infrastructure. | <ul style="list-style-type: none"> • Products and services become unavailable • Customer claims for losses. Loss of customers • Damage to reputation • Failure to meet our growth plans • Additional costs if projects not delivered on time or within budget or if additional work required |
| Tungsten Network processed 17.7 million transactions and over 5 million purchase orders in FY18 and holds a significant volume of customer data. There is a risk of a data breach. | <ul style="list-style-type: none"> • Uninsured loss claims from customers • Loss of customers • Damage to reputation • Financial penalties |
| Tungsten Network uses market-leading external IT vendors to support its businesses including software upgrades. There is a risk of failure/closure of a vendor which could impact the ability of the Company to provide products and services to its customers. | <ul style="list-style-type: none"> • Products and services become unavailable • Customer claims for losses. Loss of customers • Damage to reputation • Failure to meet our growth plans |

Mitigation

- The strategy is regularly reviewed and challenged by the Executive Committee and Board
 - The strategy forms the basis of the annual business planning process
 - Performance targets are aligned to strategy
 - Strategy is regularly and effectively communicated to all staff
 - Documented up-to-date disaster recovery and business continuity plans which are regularly tested. Use of multiple hosting centres
 - IT recovery plans include website resilience and penetration tests
 - Ongoing, real-time technology defence mechanisms in place
 - Continuous monitoring of IT systems availability
 - Governance frameworks in place to ensure appropriate management of the risks and mitigants
 - New employees with the appropriate skills have been recruited and, where required, third party experts are used to review and validate both the planning and execution of programmes of work
-
- Mitigating cyber-attacks is of paramount importance to the Company to ensure customer confidence in the security and availability of our products and services
 - Well-defined IT security procedures in place
 - Documented up-to-date disaster recovery and business continuity plans, which are regularly tested. Use of multiple hosting centres
 - Comprehensive review of procedures and controls as part of the annual International Standards for Assurance Engagements (ISAE) 3402 Assurance Reports on Controls at a Service Organisation
 - Comprehensive review of procedures and controls as part of the annual independent ISO 27001 certification, the international standard describing best practice for an Information Security Management System
 - Training and employee awareness programmes in place
-
- Processes in place to improve operational performance
 - Documented up-to-date disaster recovery and business continuity plans which are regularly tested. Use of multiple hosting centres
 - IT recovery plans include website resilience and penetration tests
 - New employees with the appropriate skills have been recruited and, where required, third party experts are used to review and validate both the planning and execution of programmes of work
 - Continuous monitoring of IT systems availability
 - Continuing to enhance our technological and operational capabilities through investment in high quality staff and IT functionality
 - Oversight of satisfactory completion of improvements and enhancements by Executive Committee
-
- Processes in place to ensure adherence to data protection and security awareness policies
 - Training and employee awareness programmes in place
 - No issues raised under the independent review of procedures and controls as part of the annual ISAE 3402 Reports
-
- Prior to appointment, key vendors are subject to due diligence check and assessed for financial viability
 - The relationship with and financial position of key vendors are reviewed on a regular basis
 - Key vendors required to have ISO 27001 certification. Only leading vendors are engaged

RISK MANAGEMENT CONT.

Approval of the Strategic report:



Richard Hurwitz
Chief Executive Officer

23 July 2018

| Risk | Impact |
|--|---|
| Financial | |
| Direction of change The level of financial risk facing Tungsten Network is stable as revenues have grown and losses decreased, reducing the cash requirements of the Group. | |
| Inability to finance the Group businesses. | <ul style="list-style-type: none"> • Failure to continue in business or meet liabilities • Failure to meet our growth plans |
| Tungsten Network may be subject to non-payment by its customers. | <ul style="list-style-type: none"> • Failure to meet our growth plans. Ability to invest or develop • Litigation costs |
| Exposure to foreign exchange fluctuations, resulting in a material impact on profit or cash balances. | <ul style="list-style-type: none"> • Failure to meet our growth plans • Failure to achieve targets for revenue, profits or earnings |
| People | |
| Direction of change There has been a high turnover of staff at all levels as a result of changes to the business strategy. Many new high calibre people have joined the Group, and continuous succession planning has resulted in a reduction in the level of risk. | |
| Inability to retain, develop and motivate a highly skilled and knowledgeable senior management team. | <ul style="list-style-type: none"> • Failure to implement the strategy and achieve the business' targets • Over-reliance on key senior personnel to lead the business • Loss of knowledge/skills within the senior management team |
| Inability to attract, retain, develop and motivate the best people with the appropriate capabilities to create a high quality, diverse and flexible workforce. | <ul style="list-style-type: none"> • Failure to maintain satisfactory customer service levels • Loss of knowledge/skills within the business • Over reliance on key personnel |
| Regulatory/Political/Environmental/Social | |
| Direction of change Although the markets in which we operate and their legal and political environments are constantly evolving, the overall level of regulatory/political risk facing Tungsten Network has not changed materially and remains stable. Implementation of the General Data Protection Regulation (GDPR) on 25 May 2018 has resulted in increased risk for all businesses in the area of data protection. This has previously been flagged as a high risk area, and remains so, although this as a result of the potential implications of non-compliance with the new GDPR regime rather than Tungsten's state of GDPR readiness. | |
| Tungsten Network has customers in 192 countries around the world. Our business model and our services are affected by legal, political and regulatory changes that restrict access to markets and customers. These changes include implementation of the EU General Data Protection Regulation (GDPR) in May 2018 and the UK's exit from the European Union. | <ul style="list-style-type: none"> • Financial loss as a result of restricted access to the markets • Damage to reputation. Regulatory censure • Increased compliance costs |
| Tungsten Network has a negative impact on the physical environment, social environment or communities in which it operates. | <ul style="list-style-type: none"> • Damage to environment or communities • Damage to reputation |

Mitigation

- The Directors regularly stress test the business model to ensure the Group has adequate working capital
 - Robust procedures to monitor the effective management of cash and debt including cash reports and cash forecasting
 - A cash mitigation plan exists in the event that liquidity falls below expected levels
 - The Group has secured a revolving credit facility with its Bank
-
- Ongoing project to review whole credit management processes
 - Credit monitoring process in place to address aged debtors
 - Credit analytics reporting in place
-
- Tungsten Network reports in and holds the majority of its cash balances in Pound Sterling
 - Revenues and costs for its other major currencies of US Dollar and the Euro are materially equal
 - Currency exposure is forward managed and hedging products considered where appropriate
-
- Succession planning for all members of executive management is part of the Board agenda
 - Competitive remuneration packages with oversight by the Remuneration Committee, including equity based long-term incentives
 - Strategies for senior management retention
-
- Training and development, customer relationship, leadership, social responsibility and communications programmes in place to actively engage and retain employees
 - Competitive remuneration packages with oversight by the Remuneration Committee
 - Focus on creation of a culture and values to attract and motivate our people
 - Recruitment strategy and succession planning in place including active encouragement of promotion from within
-
- Comprehensive documented policies relating to business conduct, financial crime, bribery, corruption and whistleblowing in place
 - Oversight and monitoring including reporting of any deviations and exceptions to the Executive Committee
 - Strategy to ensure that business model remains flexible and responsive to change and is regularly reviewed
 - Horizon scanning by the Executive Committee for upcoming potential changes including product/diversification strategy to reduce impact
 - An extensive programme is in place to ensure GDPR compliance. Program elements include:
 1. Engaging with external advisers to assist in assessing Tungsten Network's readiness for the GDPR
 2. Established a cross-company steering and working group, led by our Compliance and Assurance team
 3. Leveraging our current industry best practices such as ISO27001 certification and Cyber Essentials certifications, as part of readiness preparations for GDPR
 4. Acquiring the latest best-of-breed proportionate technology for data discovery and classification
 5. Training for all of our internal staff, including software development teams in secure coding and privacy through design
 6. Active program of rolling out GDPR compliant processes and policies
 7. Updating contract terms with customers and vendors to make GDPR compliant
-
- Tungsten Network's products benefit the environment through the elimination of paper
 - Tungsten Network's office footprints are assessed for their impact on the environment and 'green' options implemented where practical