## Principal risks and uncertainties

### Risk Management overview

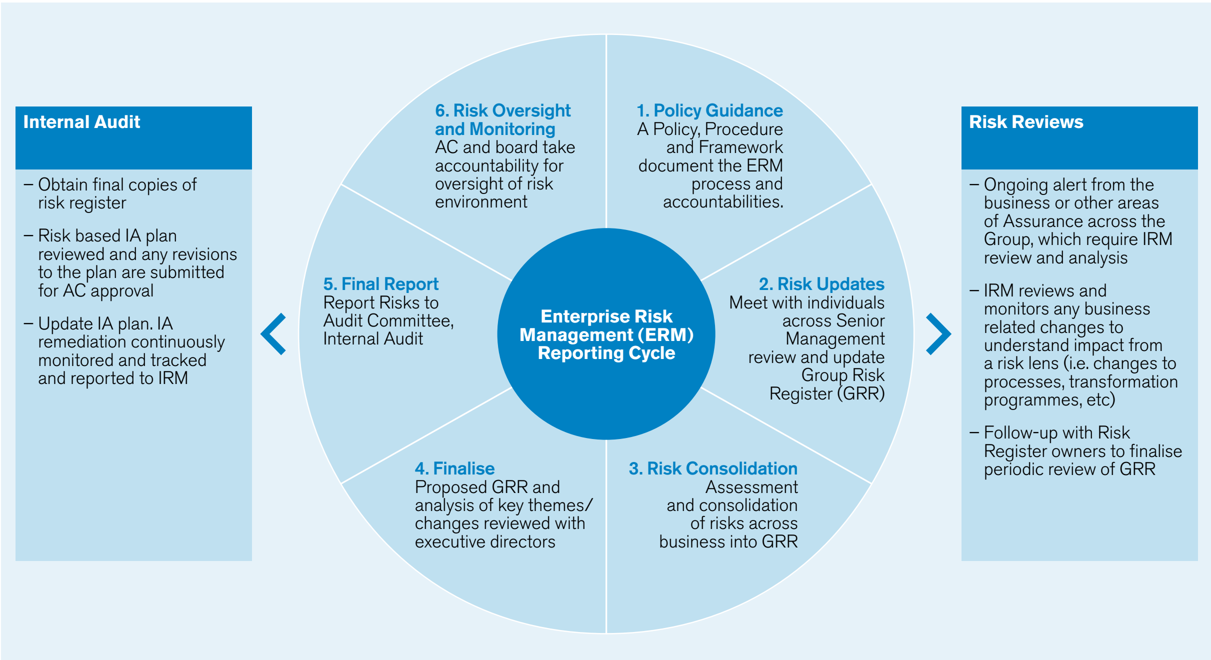
Our business model, future performance, solvency, liquidity and reputation are exposed to a variety of risks and uncertainties. The board's role is to determine the principal risks the Group is willing to take to achieve its long-term strategic objectives and enhance the sustainability of value creation. Underpinning the operation of, and central to, the risk management process is the culture of the Group, led by the board, of openness, transparency, debate, trust and accountability. On behalf of the board, the Audit Committee reviews and challenges the effectiveness and robustness of the risk management process.

### Risk Management process

The board manages risk in accordance with the enterprise Risk Management Framework ("RMF") under the Group's Risk Management Policy and Procedure. The RMF is aligned to the business objectives and strategy (see page 14). A key component of the RMF for the board is that, whilst the RMF enables an assessment of risk, it is also practical and proportionate. This ensures that the RMF is able to be embedded into the day-to-day business processes across the Group, to drive risk awareness and risk culture. The board continues to build upon the RMF to respond to any future change in the Group's risk profile. During the period, the board continued to assess the gross and net risks against the defined risk appetite statements of the Group and to further align the risks to the Group's strategy. The risk appetite statements set out the board's risk-taking approach to ensure a balanced view between risk aversion, opportunity and gains, against a background of maintaining reputation, financial stability and compliance.

The Group maintains a risk based annual internal audit plan (see pages 85 to 87 for the report on internal controls). During the period, the Group underwent a significant transformational change with the acquisition of the HPE Software business on 1 September 2017 and announced the sale of the SUSE business on 2 July 2018 as set out on page 12. As the risks assessed under the RMF changed during the period, the annual internal audit plan was flexed to ensure appropriate levels of assurance. The Group risk register is reviewed with internal audit during the development of the annual internal audit plan, and subsequently at each update of the Group risk register throughout the period, to ensure alignment of the internal audit plan to the Group's risk profile. To underpin the robustness of the operation of the RMF, as part of the risk based internal audit process, the internal auditors assess the gross and net risk ranking assigned by the risk owners.

The RMF is also subject to an annual review by an external specialist and shared with the internal audit team. A key area of focus for improving the RMF in the forthcoming year is to continue to embed the RMF across the Group. The enterprise risk management reporting cycle and alignment with internal audit and the wider business is as follows:



Risks are identified, assessed and recorded by the Micro Focus and SUSE Product Portfolios and the Group functions. Each business area director and Group function head is responsible for the identification, assessment and management of risk in their area. Each risk is owned by an individual in that area. The process includes the use of risk registers and one to one interviews with business area directors, Group function heads and board members. Risks are assessed on a gross and net basis against a consistent set of criteria defined by the board. The criteria measures the likelihood of occurrence against the potential impact to the Group including financial results, strategic plans, operations and reputation. Each risk is allocated a risk appetite category and a risk tolerance; changes in the risk profile are tracked at each reporting point during the period. The assessment includes current and emerging risks. Principal risks are categorised into four distinct areas, both externally and internally driven, which include financial, infrastructure, marketplace, and reputational risks. Existing controls and improvement actions are recorded on the risk register for each risk, together with internal audit reviews.

The RMF sets out a continuous cycle of review, reporting and improvement over the period. Following one to one interviews with the business area directors and Group function heads, the individual risk registers are consolidated to form the Group risk profile. The Group risk profile is reported to the executive directors for monitoring, review and challenge. A report is made to every Audit Committee meeting during the period for review, to challenge the effectiveness of the RMF and then approval by the board. As part of the RMF an annual review of risk is also undertaken, this is aligned with the annual review of internal audit. These annual reviews focus on areas for improvement in the process, as well as the key emerging areas of risk for the Group in the year ahead. The board and the Audit Committee also received detailed risk assessments as part of reports on material projects across the Group.

In the period, we continued to work to improve the way we manage risk and, embed risk methodology into the business at management level. Metrics over risks (i.e. trend analysis) are performed periodically. We reviewed and improved our Fraud Risk Management policy and procedures including a revised anti-fraud policy as part of our integrated Code of Conduct across the Group.

### Changes in the period

The risk movement reflects the key activities and challenges across the period. In particular the transformational HPE Software business acquisition and integration, and the preparation for the divestment of the SUSE business. The board is mindful of the interdependencies and speed of some risks. As set out on pages 18 to 19 the HPE Software business integration is significantly complex. In the period, there has been an improvement in integration related risks, with detailed action plans being executed to improve the quality of delivery, speed of decision-making and accountability. The divestment of SUSE also represents a complex process. The governance framework for management of these programmes includes full time dedicated programme management offices that work together to mitigate key areas of principal risks. Details of the complexity and challenges, in particular in relation to IT systems, of the integration and divestment are set out in the Chief Executive's Strategic review on page 20.

Although there continues to be significant uncertainty with Brexit implications, our cross-functional Brexit Working Group continued to monitor developments, as far as possible, for impacts to our business. Areas under review for possible impacts include people, tax, treasury, regulatory and commercial matters. The readiness work and analysis aims to provide confidence to our people, suppliers and customers of our Brexit readiness.

We have included a separate principal risk relating to cyber security. Cyber threats pose a risk to our entire industry. Work continues to further strengthen our resilience in this area and to further develop our cyber defence capabilities.

We have included a narrative relating to risks around internal controls over financial reporting. As part of its disclosure obligations in the United States the Group is required to furnish an annual report by its management on its internal controls over financial reporting and include an attestation report issued by its independent registered public accounting firm pursuant to Section 404 of the Sarbanes-Oxley Act of 2002 (SOX). The first report will be required to be produced as of 31 October 2019.

Please also refer to the section on internal controls within the corporate governance report on pages 72 to 79.

### Principal Risks and Uncertainties

In common with all businesses, the Group could be affected by risks and uncertainties that may have a material adverse effect on its business operations and achieving its strategic objectives including its business model, future performance, solvency, liquidity and/or reputation. These risks could cause actual results to differ materially from forecasts or historic results. Accepting that risk is an inherent part of doing business, the board is mindful of the interdependencies of some risks. Where possible, the Group seeks to mitigate risks through its RMF, internal controls and insurance, but this can only provide reasonable assurance and not absolute assurance against material losses. In particular, insurance policies may not fully cover all of the consequences of any event, including damage to persons or property, business interruptions, failure of counterparties to conform to the terms of an agreement or other liabilities.

The following are the principal risks and uncertainties, potential impacts and mitigations that are relevant to the Group as a provider of software products and associated services at this time. They do not comprise all of the risks associated with the Group and are not set out in priority order. Additional risks not presently known to management, or currently deemed to be less material, may also have an adverse effect on the Group.

The net risk movement from the prior period for each principal risk has been assessed and presented as follows:

No change    Increased net risk exposure    Reduced net risk exposure

## Products

Risk Trend    Link to: Business Model: **Make software**    Risk Category: **Marketplace**

### Principal Risk Description

To remain successful the Group must ensure that its products continue to meet the requirements of customers and must be effectively balanced between growth and legacy products. Investment in research and innovation in product development is essential to meet customer and partner requirements in order to maximise revenues and corporate performance. The Group has a large number of products, at differing stages of their life-cycle. The extent of investment in each product set needs to be managed and prioritised considering the expected future prospects, to ensure an effective balance between growth and legacy products. The Group's business and reputation may be harmed by errors or defects in its products.

### Potential impact

If products do not meet the requirements of customers, they will seek alternative solutions, resulting in the loss of new revenue opportunities and the cancellation of existing contracts. Insufficient focus on key research and development projects may damage the long-term growth prospects of the Group.

### Mitigation

When considering investment priorities, both organic and inorganic, the Group evaluates its options against a set of characteristics mapped to each stage of the product life-cycle enabling the categorisation of its product portfolio into the following: new models, growth drivers, optimise and core (further details are set out on page 23 (Business Model section)).

As set out on page 24 (Business Model section) the Group continues to align resources and develop propositions across four main focus areas: Enterprise DevOps; Hybrid IT Management; Security, Risk & Governance; and Predictive Analytics and to improve the interaction between Product Management, Product Development, Sales and Marketing. The Micro Focus product portfolio consists of five product groups with over 300 product lines, as set out on page 28 (Portfolio Review), which are uniquely positioned to help customers maximise existing software investments and embrace innovation. The Group has improved alignment and applied robust application of the four-box model across the Enlarged Group, as set out on page 23 (Business Model section). The product portfolio is focused on delivering "customer centric innovation" that delivers tangible business impact for customers in all stages of the software life-cycle.

## Go-To-Market ("GTM") Models

Risk Trend

Link to Business Model: **Sell software**

Risk Category: **Marketplace**

### Principal Risk Description

For the Group to succeed in meeting revenue and growth targets it requires successful GTM models across the full product portfolio, with effective strategies and plans to exploit channel opportunities and focus the sales force on all types of customer categories. In addition, effective GTM models may be more successful if accompanied by compelling Micro Focus brand awareness programmes. The Group is dependent upon the effectiveness of its sales force and distribution channels to maintain and grow licence, maintenance and consultancy sales.

### Potential impact

Poor design and/or execution of GTM plans may limit the success of the Group by targeting the wrong customers through the wrong channels and using the wrong product offerings.

### Mitigation

As set out on page 19 of the Chief Executive's Strategic Review, there has been good progress in the development of the Group's customer and partner proposition. Across the five product categories that the Group reports against, the Group has great depth of capability and experience to help its customers address some of the most complex challenges they face. To best enable the Group's customers to exploit this breadth and depth it is aligning resources and developing compelling propositions across four focus areas – Enterprise DevOps; Hybrid IT Management; Security, Risk & Governance; and Predictive Analytics.

Sales execution has received considerable attention and improvement measures have focused on the consistent execution of simpler, more effective sales processes, better alignment and accountability within the sales management teams through the removal of unnecessary global structures and management layers, organisational changes to align marketing and product teams much more tightly and investments made to build a consistent approach to enablement globally. We have strengthened the team through the appointment of Jon Hunter as Chief Revenue Officer.

## Competition

Risk Trend

Link to Business Model: **Sell software**

Risk Category: **Marketplace**

### Principal Risk Description

Comprehensive information about the markets in which Micro Focus and SUSE operate is required for the Group to assess competitive risks effectively and to perform successfully. The Group operates in a number of competitive markets and success in those markets depends on a variety of factors.

### Potential impact

Failure to understand the competitive landscape adequately and thereby identify where competitive threats exist may damage the successful sales of the Group's products. If the Group is not be able to compete effectively against its competitors, it is likely to lose market share which may result in decreased sales and weaker financial performance.

### Mitigation

Group product plans contain an analysis of competitive threats and subscriptions to industry analyst firms are leveraged to better understand market dynamics and competitor strategies. In addition, customer contact programmes are analysed for competitive intelligence. Micro Focus and SUSE continue to monitor and review intelligence on market threats to focus on offering best in class service to customers.

## Employees and Culture

Risk Trend

Link to Business Model: **Make, Sell, Support software**

Risk Category: **Infrastructure**

### Principal Risk Description

The retention and recruitment of highly skilled and motivated employees, at all levels of the Group, is critical to the success and future growth of the Group in all countries in which it operates. Employees require clear business objectives, and a well-communicated vision and values, for the Group to achieve alignment and a common sense of corporate purpose among the workforce.

### Potential impact

Failure to retain and develop skill sets, particularly in sales, IT and research and development may hinder the Group's sales and development plans. Weak organisational alignment and inadequate incentivisation may lead to poor performance and instability. It could also have an adverse impact on the realisation of strategic plans.

### Mitigation

Successful cultural alignment across the Group is intrinsic to the way we do business and is a key focus for the Group. Leading by example from the top is a key driver. The Group has policies in place to help ensure that it is able to attract and retain employees of a high calibre with the required skills. These policies include training, career development and long-term financial incentives. The Group also has in place a performance management and appraisal system. Succession plans have been developed and are in place for key leadership positions within the Company. During the period a new Chief Human Resources Officer was appointed. In the period the Group also took significant action to develop its management capability both internally, by training and promotions, and through external hires.

## Tax

Risk Trend

Link to Business Model: **Support software**

Risk Category: **Financial**

### Principal Risk Description

The tax treatment of the Group's operations is subject to the risk of challenge by tax authorities in all territories in which it operates. Cross-border transactions may be challenged under tax rules and initiatives targeting multinationals' tax arrangements, including the OECD's Base Erosion and Profit Shifting project and EU state aid rules. As a result of the HPE Software business acquisition, the Group may be required under the tax matters agreement entered into with HPE (the "TMA") to indemnify HPE, if actions undertaken by the Group affect the tax treatment of the separation of HPE Software business from HPE.

Future changes to US and non-US tax laws could adversely affect the Group. The Group will be subject to tax laws of numerous jurisdictions, and the interpretation of those laws is subject to challenge by the relevant governmental authorities.

### Potential impact

Tax liabilities in various territories in which the Group operates, particularly as a result of the HPE Software business acquisition, could be significantly higher than expected. The Group may be obliged to make indemnification payments to HPE under the TMA, which, if payable, would likely be substantial.

### Mitigation

Tax laws, regulations and interpretations are kept under on-going review by the Group and its advisors. The Group reviews its operations, including the structuring of intra-Group arrangements, on a periodic basis to ensure that all relevant laws are complied with and that risks are identified and mitigated appropriately. External professional advice is obtained ahead of material structuring activity and to support positions taken in financial statements and local tax returns where there is significant uncertainty or risk of challenge. During the period, a governance framework and process has been developed to remind relevant employees of the requirements and guiding principles to comply with the obligations under the TMA.

## Business Strategy and Change Management

Risk Trend

Link to Business Model: **Make, Sell, Support software**

Risk Category: **Marketplace**

### Principal Risk Description

The Group is engaged in a number of major change projects including acquisitions and divestments to shape and grow the business by strengthening the portfolio of products and capabilities and IT projects to standardise systems and processes. The successful integration of businesses will build a solid base for further expansion. These projects expose the Group to significant transformation risks. The Group's strategy may involve the making of further acquisitions to protect or enhance its competitive position and failure to identify, manage, complete and integrate acquisitions, divestitures and other significant transactions successfully could have a material adverse effect on the Group's business.

The integration of the HPE Software business and the divestment of SUSE are both complex transactions with a range of integration and separation risks. The integration of the HPE Software business with the existing businesses carried on by the Group may be more time consuming and costly than anticipated. Successful execution of the SUSE divestment may be compromised by adding a new level of complexity to an existing heightened operation environment across the Group and be a distraction to deliver business plans.

### Potential impact

Failure to analyse, execute and co-ordinate the various integration, divestment and transformation programmes successfully may result in the disruption of the on-going business without delivering the anticipated strategic and operational benefits of such transactions. In addition, this may affect the ability to execute strategic plans for growth.

### Mitigation

As set out on page 15. The Group has an established acquisition strategy and focus on efficient execution in the mature infrastructure software market. The delivery and execution of the HPE Software business integration and the SUSE divestment is controlled and mitigated by respective dedicated full-time programme offices. During the period there have been enhancements made to programme governance. The operating plan is focused on delivering targeted, relevant business outcomes and the simplification of business operations to improve empowerment, speed and accountability of decision-making and drive a heightened sense of urgency across all aspects of execution. Programme risks and interdependencies are managed carefully including the utilisation of detailed deep dives, cross functional integration/divestment walk the walls sessions, a cadence of weekly and daily cross functional calls and risk assessments to ensure that execution of the various projects are successfully aligned to minimise any disruption to business as usual. The integration and harmonisation will continue as a key area of principal risk in the forthcoming year.

## Intellectual Property ("IP")

Risk Trend

Link to Business Model: **Make software**

Risk Category: **Marketplace**

### Principal Risk Description

The Group is dependent upon its intellectual property, and its rights to such intellectual property may be challenged or infringed by others or otherwise prove insufficient to protect its business. Some of the Group's SUSE products utilise Open Source technology, which is dependent upon third party developers. The Group's products and services depend in part on intellectual property and technology licenced from third parties, and third-party claims of intellectual property infringement against the Group may disrupt its ability to sell its products and services.

### Potential impact

Failure could adversely affect the ability of the Group to compete in the market place and affect the Group's revenue and reputation.

### Mitigation

There are procedures in place across the Group to ensure the appropriate protection and use of the Group's brands and IP and these are monitored by the IP Panel and Legal team. During the period, the IP Panel and Group IP procedures were updated and extended across the Enlarged Group.

## Legal and Regulatory Compliance

Risk Trend

Link to Business Model: **Support software**

Risk Category: **Reputational**

### Principal Risk Description

The Group operates across a number of jurisdictions and two regulated exchanges. Compliance with national and regional laws and regulations is essential to successful business operations. The Group may be involved in legal and other proceedings from time to time, and as a result may face damage to its reputation or legal liability. The Group has entered into various acquisitions and a disposal over recent years and may be subject to, or have the benefit of, certain residual representations, warranties, indemnities, covenants or other liabilities, obligations or rights. The Group has a variety of customer contracts in a variety of sectors, including Government clients.

### Potential impact

Failure to comply could result in civil or criminal sanctions (i.e. personal liability for directors), as well as possible claims, legal proceedings, fines, loss of revenue and reputational damage.

### Mitigation

The Group has in place policies and procedures to mitigate these risks. The Group's legal and regulatory team, enhanced by specialist external advisors as required, monitor and review compliance. There is a Compliance Committee, which reports into the board. All staff are subject to mandatory compliance training. The Group is committed to ensuring ongoing compliance with anti-bribery and corruption, data protection and market abuse and insider dealing laws. A new, integrated Code of Conduct was rolled out in August 2018, with supporting training materials distributed to all employees during October 2018. Significant work was undertaken during the period to ensure compliance with the General Data Protection Regulation ("GDPR"). This included the approval of four new data protection policies by the board, GDPR Awareness training being circulated to all employees, and regular communications to employees is on-going regarding the importance of compliance with the requirements. Data protection compliance is subject to on-going monitoring by our privacy team. The compliance environment is also strengthened by the implementation of SOX controls, as set out on page 41.

## Macro Economic Environment and Brexit

Risk Trend

Link to Business Model: **Sell, Support software**

Risk Category: **Marketplace**

### Principal Risk Description

The Group's businesses may be subject to inherent risks arising from the general and sector specific economic and political conditions in one or more of the markets in which the Group operates. This is heightened by the fact the Group sells and distributes its software products globally. Exposure to political developments in the United Kingdom, including the terms and manner of the UK's withdrawal from the EU, could have an adverse effect on the Group.

### Potential impact

Adverse economic conditions could affect sales, and other external economic or political matters, such as price controls, could affect the business and revenues.

### Mitigation

The spread of jurisdictions allows the Group to be flexible to adapt to changing localised risk to a certain extent. The Group has business continuity plans and crisis management procedures in place in the event of political events or natural disasters.

The Group has a cross functional Brexit Working Group with processes in place to assess, respond, monitor and track the impact of Brexit on our businesses, and associated risks, as matters progress and how the business can seek to mitigate these risks. Areas under review for possible impacts include people, tax, treasury, regulatory and commercial matters.

## IT Systems and Information

Risk Trend

Link to Business Model: **Support software** Risk Category: **Infrastructure**

### Principal Risk Description

The Group's operations, as with most businesses, are dependent on maintaining and protecting the integrity and security of the IT systems and management of information. Integration of HPE Software business with the existing businesses, including the respective IT systems, may be more time consuming and costly than anticipated, given the amount of change management that is involved. The Group continues to operate on two IT architectures with the attendant complexity to business operations and the control environment.

### Potential impact

Disruption to the IT systems could adversely affect business and Group operations in a variety of ways, which may result in an adverse impact on business operations, revenues, customer relations, supplier relations, and reputational damage. Dependency on IT providers could have an adverse impact on revenue and compliance in the event that they cannot resume business operations.

### Mitigation

The Group continues to focus its efforts on the stabilisation of the HPE Software business infrastructure. Progress has been made with the system now being stable and able to support the business. To maintain the required control environment the Group relies upon automated, semi-automated and manual controls together with a combination of preventative and detective controls. A Vendor Management process is in place to allow for better involvement and engagement with third party IT providers. In relation to the SUSE divestment a dedicated IT Program Director is in place to lead the SUSE IT separation and execution, working under the Divestment Programme Management office.

There is an on-going programme of simplification being delivered, with a parallel project approved by the board and now underway to build the future, simplified systems architecture for the Group (as set out in the Chief Executive's Strategic Review set out on page 20). The IT control environment is also being improved as part of the implementation of controls to meet Sarbanes-Oxley Act 2002 (SOX) compliance, as set out on page 41.

## Cyber Security (previously part of IT systems and information)

Risk Trend:

Link to Business Model: **Support software** Risk Category: **Infrastructure**

### Principal Risk Description

Risk of hacking or other cybersecurity threat leading to data loss and/or disruptions to business. The IT environments of both the Group and its customers may be subject to hacking or other cybersecurity threats, which may harm customer relationships, financial performance and the market perception of the effectiveness of the Group's products.

### Potential impact

Data loss, which could harm client and customer relationships, compliance and/or perception of the effectiveness of the Group's products.

### Mitigation

The Group works continually to counter the risk posed by the current and emerging cyber security threat landscape. The cyber team manages the security of our data, technology and training programme to protect the performance and availability of the Group IT systems. Group-wide cyber readiness policies and processes are in place. Cyber security testing in critical areas of the business is on-going, Group-specific vulnerabilities are reviewed and continuously managed.

## Treasury

Risk Trend

Link to Business Model: **Support software** Risk Category: **Financial**

### Principal Risk Description

The Group operates across a number of jurisdictions and so is exposed to currency fluctuations. The risk of foreign exchange fluctuations may be increased as a result of Brexit.

The Group targets a Net Debt to Adjusted EBITDA ratio of 2.7 times and may require additional debt funding in order to execute its acquisition strategy. The Group is exposed to interest rate risk related to its variable rate indebtedness, which could cause its indebtedness service obligations to increase significantly.

The Group's operational and financial flexibility may be restricted by its level of indebtedness and covenants and financing costs could increase or financing could cease to be available in the long term. The Group may incur materially significant costs if it breaches its covenants under its banking arrangements.

### Potential impact

The relative values of currencies can fluctuate and may have a significant impact on business results.

Insufficient access to funding could limit the Group's ability to achieve its desired capital structure or to complete acquisitions.

An increase in interest rates could have a significant impact on business results.

### Mitigation

The Group's operations are diversified across a number of currencies, with limited exposure to £ Sterling. Key currency exposures are detailed on page 144. Changes in foreign exchange rates are monitored, exposures regularly reviewed and actions taken to reduce exposures where necessary. The Group provides extensive constant currency reporting to enable investors to better understand the underlying business performance.

The Group has significant committed facilities in place, the earliest of which matures in November 2021 and sufficient headroom to meet its operational requirements. The Group seeks to maintain strong relationships with its key banking partners and lenders and to proactively monitor the loan markets. The Group also has strong engagement with the providers of equity capital, which represents an alternative source of capital. Currency change fluctuations as a result of Brexit are being monitored by the Brexit Working Group.

The Group holds interest rate swaps to hedge against the cash flow risk in the LIBOR rate charged on $2,250.0m of the debt issued by a Group subsidiary company, Seattle Spinco, Inc. from 19 October 2017 to 30 September 2022. Under the terms of the interest rate swaps, the Group pays a fixed rate of 1.94% and receives one month USD LIBOR.

Monitoring policies and procedures are in place to reduce the risk of any covenant breaches under the Group's banking arrangements. At 31 October 2018, $nil of the Revolving Facility was drawn. As a covenant test is only applicable when the Revolving Facility is drawn down by 35% or more, and $nil of Revolving Facility was drawn at 31 October 2018, no covenant test is applicable.

**Risks related to Internal Controls over Financial Reporting**

As part of its disclosure and reporting obligations in the United States, the Group will be required to furnish an annual report by its management on its internal control over financial reporting and include an attestation report issued by its independent registered public accounting firm pursuant to Section 404 of the Sarbanes-Oxley Act of 2002 ("SOX"). The first report will be required to be produced as of 31 October 2019.

The Group is in the process of implementing a programme of SOX compliant internal controls under its SOX Implementation Programme (SIP) together with a specialist team from its outsourced Internal Audit Partner, PwC. Governance for the SIP includes a cross functional SOX Steering Group (SSG) chaired by the Group's Chief Financial Officer reporting to the Audit Committee. As part of the SIP a new Disclosure Committee, chaired by the Chief Financial Officer, has been set up to assist the Chief Executive Officer and Chief Financial Officer in fulfilling their responsibilities in connection with the accuracy of financial reporting. The SIP is being implemented across the Group during a period of significant change across the organisation. As part of the governance the SSG monitors potential adverse impacts of organisational change to the SIP. During the period, as part of the SIP, end to end process mapping and walkthroughs were carried out of the Group's main processes, Hire to Retire, Quote to Cash, Procurement to Pay and Record to Report, leading to the development of documented controls for each process. Each process and its associated controls are owned by a Global Process Owner. In the period, the Group has also reviewed its entity level controls and commenced implementation of a SOX training plan across relevant parts of the Group. A key work stream of the SIP relates to the adequacy of IT General Controls (ITGCs). The challenges with the IT systems, including controls acquired with the HPE Software business, are set out on page 20. As a consequence, each business will remain on its legacy IT systems, necessitating business process controls and ITGCs across both systems. The work undertaken under the SIP to date has identified a number of areas for improvement in the Group's ITGCs, which now forms part of the SIP. Work in this area is continuing under an IT SOX Compliance Group chaired by the Chief Information Officer reporting to the main SSG. As part of this work, an IT strategy has been developed and is being implemented across the network in both the Group's owned IT systems and those operated by its external cloud partner.

As a requirement for the Group's listing in the United States, its internal controls over financial reporting were for the first time subject to review under the US Public Company Accounting Oversight Board (PCAOB) auditing standards in connection with the audit of Micro Focus' annual consolidated financial statements for the three years ended 30 April 2017. As a result of the work undertaken, certain weaknesses in the Group's internal control over financial reporting were identified, which under PCAOB standards were considered to be material weaknesses. Under the PCAOB standards a material weakness is a deficiency, or a combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the Group's annual or interim consolidated financial statements will not be prevented or detected on a timely basis. The material weaknesses related to the fact that the Group did not have sufficient formally documented and implemented processes and review procedures, nor did it have sufficient formality and evidence of controls over key reports and spreadsheets. Whilst the Group has made significant progress towards remediating the material weaknesses in the heritage Micro Focus systems and processes, the significant challenges with the IT systems acquired with the HPE Software business means that these material weaknesses and other control deficiencies are also relevant for this area of the organisation. The remediation activity includes system upgrades and formal documentation of control and review procedures.

The Group continues its work under the SIP to remediate the material weaknesses and other control deficiencies, and any other matters, which arise during its progress towards SOX compliance. To maintain the required control environment the Group relies upon automated, semi-automated and manual controls together with a combination of preventative and detective controls. The material weaknesses, control deficiencies and other matters may not be able to be remedied by 31 October 2019, and there is a risk that other deficiencies for the purposes of SOX may be identified. Failure to correct the material weaknesses or our failure to discover and address any other material weakness or control deficiencies could result in inaccuracies in our financial statements and impair our ability to comply with applicable financial reporting requirements and related regulatory filings on a timely basis. It could also result in an adverse reaction in the financial markets due to a loss of confidence in the reliability of the Group's financial statements and could have a material adverse effect on the Group's business, financial condition, results of operation and prospects.