


Ref	Requirement		
	HEADER		
	ICAEW Technical Accreditation Scheme Expense Management Software Evaluation		
	SAP Concur		
	Product Focus: Expense Management module <i>SAP Concur has multiple products, however this review is only assessing the functionality within the SAP Concur Expense Product.</i>		
			
	Jun-25		
	© ICAEW. Technical Accreditation Questionnaire		
	CONTENTS		
1	Introduction and Prologue		
2	Issues identified and evaluation conclusion		
	-- GLOBAL REQUIREMENTS:		
3	Access and Security		
4	Data processing and reporting		
5	Usability		
6	SaaS hosting		
7	Expense management		

Ref	Requirement		
1.	INTRODUCTION AND PROLOGUE		
Introduction			
1.01	The suitability of software for each particular user will always be dependent upon that user's individual requirements. These requirements should therefore always be fully considered before software is acquired. The quality of the software developers or suppliers should also be considered at the onset.		
1.02	<p>Fundamentally, good software should:</p> <ol style="list-style-type: none"> 1. Be capable of supporting the functions for which it was designed. 2. Provide facilities to ensure the completeness, accuracy, confidentiality and continued integrity of these functions. 3. Be effectively supported and maintained. <p>It is also desirable that good software should:</p> <ol style="list-style-type: none"> 5. Be easy to learn, understand and operate. 5. Make best practical use of available resources. 6. Accommodate limited changes to reflect specific user requirements. <p>It is essential, when software is implemented, for appropriate support and training to be available.</p>		
Approach to Evaluation			
1.03	The objective is to evaluate a product against a set of criteria developed by the ICAEW to ensure that the software meets the requirements of Good Accounting Software, as laid down in the summary.		
1.04	In order to effectively evaluate the software, a product specialist from the vendor completed the detailed questionnaire and provided it to the ICAEW to examine. The ICAEW's Scheme Technical Manager then reviewed the operation of the various aspects of the software assisted by a member of the vendor's technical staff and checked the answers to confirm their validity. The questions were individually reviewed and commented on and the majority of assessments were confirmed.		
1.05	The Technical Manager discussed the assessment with a member of the vendor's staff in order to clarify any points requiring further information. In the event of disagreement between the supplier and the Technical Manager, the Technical Manager's decision was taken as final and the response changed accordingly.		
1.06	The latest version of the software was used throughout the evaluation.		
1.07	When the evaluation had been completed, a draft copy was sent to the ICAEW Scheme Manager for review before completion of the final report.		
Prologue: vendor's introduction to their product and company:		<i>NB: This text has been provided directly by the software vendor and does not form part of the ICAEW's & RSM's evaluation</i>	
1.08	General Overview:	<p>SAP Concur is a leading global provider of integrated travel, expense, and invoice management solutions. SAP Concur offers cloud-based solutions designed to streamline corporate travel and expense management processes.</p> <ul style="list-style-type: none"> •Headquarters: Bellevue, Washington, USA •Founded: 1993 (as Concur Technologies, later acquired by SAP in 2014) •Global Presence: Operate in more than 150 countries •Product Suite: SAP Concur offers solutions for travel booking, expense reporting, and invoice management. Product Focus for this review is SAP Concur Expense. 	
1.09	Supplier background:	See above	
1.10	Product background and suitability for the user:	<p>SAP Concur provides cloud-based solutions for travel, expense, and invoice management, helping businesses streamline and automate their administrative processes. The platform helps organizations manage and track employee travel bookings, expenses, and invoices in a way that is efficient, compliant, and cost-effective.</p> <p>A summary of Concur Expense (expense management), which is the product at the focus of this accreditation, is below:</p> <p>Expense Reporting: Employees can easily create and submit expense reports by capturing receipts through their mobile devices or automatically importing transactions from credit cards.</p> <p>Policy Enforcement: Ensures that expenses comply with company policies by flagging non-compliant submissions and automating approval workflows.</p> <p>Automation: Reduces manual work by automatically categorizing expenses, matching receipts to transactions, and eliminating errors.</p> <p>Here's a breakdown of the other SAP Concur modules, which have not been included as part of this accreditation:</p> <p>Travel Management (Concur Travel):</p> <p>Booking Travel: Allows employees to book travel (flights, hotels, car rentals) while adhering to company policies and preferred suppliers.</p> <p>Travel Policy Compliance: Ensures that bookings are made within the company's travel guidelines (e.g., budget limits, preferred vendors).</p> <p>Global Travel Support: Supports multiple currencies, languages, and international travel needs.</p>	

Ref	Requirement		
1.10 cont.		<p>Invoice Management (Concur Invoice): Automated Invoice Processing: Manages the entire lifecycle of invoices, from receipt and approval to payment. Invoice Approval Workflows: Automates approval workflows and ensures that invoices are matched with purchase orders or contracts. Supplier Management: Ensures proper management and tracking of supplier invoices for accurate and timely payments.</p> <p>Across all three modules, the Concur product also provides: Analytics & Reporting: Insights and Analytics: Provides detailed reporting and analytics to help organizations understand travel and expense spending patterns, optimize budgets, and improve cost control. Customizable Reports: Offers customizable reporting options for finance teams to track and analyze spending by department, employee, project, or location.</p> <p>Mobile Access: Mobile App: Employees can book travel, capture receipts, and submit expense reports on the go, which makes the process more efficient and user-friendly.</p> <p>Integration with ERP & Accounting Systems: Seamless Integration: SAP Concur integrates with other enterprise software, including SAP ERP systems, for a smooth flow of financial data across the organization.</p>	
1.10 cont.		<p>Benefits of SAP Concur: Time Savings: Automates time-consuming tasks like travel booking, expense reporting, and invoice approvals, freeing up employees for higher-value activities. Improved Compliance: Helps businesses enforce travel and expense policies, ensuring that employees follow the rules and reducing the risk of fraud. Cost Control: Provides visibility into spending trends, helping businesses reduce costs and optimize budgets. User Experience: A user-friendly interface for employees, which simplifies processes and reduces the administrative burden on finance teams. SAP Concur offers an integrated platform that simplifies and automates the management of travel, expenses, and invoices, allowing businesses to reduce administrative work, ensure compliance, and gain greater control over costs.</p>	
1.11	Add-on modules:	Invoice, Travel, Audit, Budget, Request, User Support Desk, Service Administration, Premium Administration, Consultative Intelligence	
1.12	Typical implementation [size]:	All - from small businesses to global businesses- across all industries.	
1.13	Vertical applications:	SAP Concur is used across all verticals/ industries.	
1.14	Server platform and database:	<p>Our cloud platform is based on a high-availability architecture with no single point of failure that is hosted on our owned hardware or in Amazon Web Services (AWS). The production hardware is co-located in several global Tier 3+/Tier 4 data center facilities. For details on specific data center platforms, see below:</p> <ul style="list-style-type: none"> • AWS https://aws.amazon.com/compliance/data-center/data-centers/ 	
1.15	Client specification required:	Web browser and/or smartphone	
1.16	Partner network:	<p>SAP Concur has a large number of partners from integration and implementation partners, to partners that integrate into the Concur platform :</p> <p>https://www.concur.co.uk/app-centre/</p>	

Ref	Requirement		
2.	ISSUES AND CONCLUSION		
Highlighted issues			
2.01	Please note that no significant limitations in relation to the product were identified, however it is important that any business contemplating the purchase of software reviews the functionality described by the vendor, in addition to the reviewer comments.		
*			
Evaluation conclusion			
2.02	For the specific use-cases in support of assisting accountancy firms to make effective use of <u>expense management</u> software, for which the product is designed, the solution appears to meet this criteria. It continues to be actively developed and enhanced. Members should be aware of the limitations of the solution as above, and fully understand the role that it can play in helping manage their compliance needs. * NOTE THAT THE QUESTIONNAIRE RELATES TO THE SOFTWARE PRODUCT AND NOT ANY SUPPLEMENTARY SERVICES PROVIDED BY THE SUPPLIER TO THE ACCOUNTANCY FIRM USING THAT PRODUCT *		
Disclaimers			
2.03	Any organisation considering the purchase of this software should consider their requirements in the light of proposals from the software supplier or its dealers and potential suppliers of other similarly specified products. Whilst the contents of this document are presented in good faith, neither ICAEW, nor the ICAEW's Technical Manager (RSM UK Consulting LLP or any party nominated by the ICAEW to perform this role on the ICAEW's behalf) will accept liability for actions taken as a result of comments made herein. The decision to purchase software resides entirely with the organisation.		

Ref	Requirement	Response	Reviewer Comments
3.	ACCESS AND SECURITY		
Access control			
3.01	What security features are included to control access to the application?	<p>We utilize a lifecycle-driven access management process for controlling and managing personnel access to systems. Because access management is a key activity in the security of information systems, our access management processes are heavily audited by various internal and external audit organizations including:</p> <ul style="list-style-type: none"> • SAP Concur internal business audit • SAP Concur internal IT audit • Sarbanes Oxley auditors • SOC 1 / SOC2 auditors • ISO27001 auditors • PCI auditors • FISMA auditors (Only applicable to US Government organizations) <p>We maintain strict separation of duties. Information Services personnel are provided access to client systems based on job description and role, with the minimum level of privileges required to perform their specific job function. Roles are separate in such a way that a specific employee will not have access to multiple security layers. Only specific Information Services employees have access to hosted systems. Separate authentication is required. Access privileges are reviewed and audited quarterly.</p> <p>Access Review Process</p> <p>We perform three types of quarterly access review processes, to ensure that only authorized personnel have access to SAP Concur systems.</p> <ul style="list-style-type: none"> • Termination review. This is a detailed check to ensure that all terminated actions have been carried out. • User re-certification. This is a detailed check to ensure that every person with access to a system is still required to have their access. • Dormant account review. This is a detailed check to check for user accounts that have not been used in the prior 90-180 days. Such unused accounts are subject to restriction or removal. 	Noted
3.01 cont.		The customer handles access control via the user provisioning and the roles defined within our solution. We provide a role based system. The role of the logged in user determines what functionality is available to the user, along with what screens, links, and modules the employee can access. The configuration of the system determines whether different user groups can access different sets of forms and fields.	
3.02	Can access to functions be managed via a permissions matrix so users can only see (in menus and other links) and access those areas they are authorised to access?	<p>The customer handles access control via the user provisioning and the roles defined within our solution. We provide a role based system. The role of the logged in user determines what functionality is available to the user, along with what screens, links, and modules the employee can access. The configuration of the system determines whether different user groups can access different sets of forms and fields.</p> <p>For our employees:</p> <p>We maintain strict separation of duties. Information Services personnel are provided access to client systems based on job description and role, with the minimum level of privileges required to perform their specific job function. Roles are separate in such a way that a specific employee will not have access to multiple security layers. Only specific Information Services employees have access to hosted systems. Separate authentication is required. Access privileges are reviewed and audited quarterly.</p>	Noted - users can have multiple roles however SAP Concur explained that this would never enable users to bypass approvers for expenses. They have a number of controls in place including segregation of duties to avoid this risk.
3.03	Is this access to the application managed by:- - Individual user profiles? - User groups or job roles?	see above	Noted
3.04	Can a report be produced detailing all current users, their	Yes, through either our Intelligence or Consultative Intelligence reporting (additional	Noted
3.05	If menus can be tailored does the system limit the display of menu options to those for which permission has been granted for each user?	Yes.	Noted
3.06	Does security allow for access to be limited to: - Read only? - Read/write? - Read/amend/delete?	Yes, Concur supports flexible role-based access control. These are configured via permission groups and roles.	Noted
3.07	If data can be accessed by separate reporting facilities, such as ODBC or an external report writer, is the user access security control applied?	Yes — if a user accesses data through supported reporting tools like Cognos, their access is restricted according to their SAP Concur security profile.	Noted
3.08	Does the system security integrate with Microsoft's Active Directory or other tools that provide a single sign-on?	<p>SAP Concur supports SAML 2.0-based Single Sign-On (SSO), enabling clients to:</p> <ul style="list-style-type: none"> • Manage user authentication through their own Identity Provider (IdP). • Control access to SAP Concur solutions with enhanced security through multifactor authentication (MFA). • Customers can configure SSO through the SAP Concur administration console. 	Noted
3.09	Does the system provide multi-factor authentication (MFA)?	Yes, see above	Noted
Passwords and access logs			

Ref	Requirement	Response	Reviewer Comments
3.10	Is access to the software controlled by password?	<p>We have implemented several changeable settings for authentication passwords in our applications to allow customers to define their own password policy when SAP Concur authentication is used.</p> <p>These settings include:</p> <ul style="list-style-type: none"> • Minimum Length: Default 8 characters • Maximum Length: Default 60 characters (support is available for unlimited) • Require Mixed Case: Default is "off". If "on," a password must contain at least one upper-case letter and one lower-case letter. • Require Number: Default is "off". If "on," a password must have at least one numeric character (0-9) • Require Non-Alphabetic: Default is "off". If "on," a password must have at least one character which is a number or special symbol • Expire Password on User Creation: Default is "off". If "on," users are created with expired passwords and thus will be prompted to change password on first login • Expire Passwords after N days: Default is "off". If "on," passwords expire N days after they are set. N may range from 0 (allowing all prior passwords) to 99 • Number Generations Before Reuse: Default = 1. If larger than 1, a user cannot use the same password until (# generations - 1) other passwords have been used. 	Noted
3.11	Does each user have a separate log on (user id)?	Yes, each user has an unique user and login IDs.	Noted
3.12	If there is no password facility please state how confidentiality and accessibility control is maintained within the software?	Even in cases where SAP Concur does not manage passwords directly (such as with SSO), confidentiality and accessibility are maintained through strong authentication mechanisms, strict role-based access controls, encryption, and system auditability.	Noted
3.13	Are passwords masked for any user logging in?	Yes	Noted
3.14	Is password complexity available and enforced?	Yes, see above question 3.10	Noted
3.15	How many previous passwords are retained / the password history?	see question 3.10	Noted
3.16	Are passwords encrypted?	Yes, passwords are hashed via SHA-256	Noted
3.17	<p>Are users automatically logged off after a pre-set idle time?</p> <p>- Can the time period be changed?</p> <p>- Can any information be viewed without being logged in, including after logging off, if so what information?</p>	SAP Concur enforces automatic logoff after inactivity, with configurable timeouts. No confidential data is accessible without a valid, active login session.	Noted
Deletion of transactions			
3.18	Is it possible to delete a transaction?	Transactions in Concur can be deleted if they are unsubmitted, but once processed or approved, they cannot be removed — only adjusted or voided. All actions are logged for audit integrity.	Noted - not material as users should be able to delete line items if they have not submitted their expense claims to the approver.
3.19	If so, then how are deletions controlled by the system?	see above	Noted
3.20	Are deleted transactions retained in the audit trail (see below) and denoted as such?	see above	Noted
Audit trails			
3.21	Does the system have an audit trail (log) which records all changes to transactions in the system?	<p>A "Read-Only" change log is available to track all configuration changes made by system administrators.</p> <p>See 3.18 for further information on transaction audit trails.</p>	Noted
3.22	Does this log also record any system error messages and/or any security violations?	<p>SAP Concur uses a centralized Security Information and Event Management (SIEM) system to:</p> <ul style="list-style-type: none"> • Collect and monitor logs from all systems. • Generate real-time alerts for suspicious or malicious activity. • Proactively monitor system behaviour for vulnerabilities and security threats using industry-recognized sources like CERT alerts <p>Events requiring attention generate alerts that notify appropriate personnel for immediate review and resolution. This process is audited by ISO 27001. Alerts are reviewed by appropriate personnel as soon as possible.</p>	Noted - only Concur has access to SIEM data
3.23	Is it possible to turn off or delete the audit trail?	No. Logs are read only.	Noted
3.24	Does the software allocate a system generated sequential unique reference number to each transaction in the audit log, date and time stamp it and record the user id?	Yes, logs are reviewed daily. User names, date and time, type of action, original state and new state of the item changed, are all available within Audit trails.	Noted
3.25	Are all master file changes recorded in the audit trail?	Yes, see above	Noted
Compliance			
3.26	Does the system operate in a way that is compliant with data protection legislation including GDPR? How does the system facilitate this?	<p>We adhere to international privacy laws and have controls in place for the General Data Protection Requirements (GDPR) of the European Union.</p> <p>GDPR compliance is achieved through the following measures:</p> <ul style="list-style-type: none"> • Datacenters in various regions around the world allow customers to choose where their data is processed. • Through implementation of robust security measures in terms of accountability and technology, maintaining records of processing activities, privacy by design checks, and new privacy rights within product cycles and privacy impact assessments. • By enforcing global adherence to guidelines and training through the British Standard BS 10012 (Personal Information Management), the Data Protection Management system (DPMS) that manages requirements of data protection in a structured way. • Adhering to SAP's unified approach for all cloud solutions with the Data Processing Agreement (DPA) which incorporates the Standard Contractual Clauses (SCC), but goes beyond SCC in providing data protection assurances to customers. <p>The functionality implemented in SAP Concur products to comply with GDPR:</p> <ul style="list-style-type: none"> • Transparency of data usage • Consent management mechanisms (if applicable) • Data Retention of customer data upon policy requirement • Simplified deletion of personal data • Restriction of Processing (Role-based access to personal data) • Read access logging to sensitive types of personal data • Change logging of personal data • Information notices 	Noted

Ref	Requirement	Response	Reviewer Comments
3.27	Describe your use of sub-processors if any?	<p>SAP Concur ensures transparency in the management and disclosure of sub-processors by providing customers with access to an up-to-date list of sub-processors through a self-service portal. This list includes descriptions of the activities performed by each sub-processor to help customers understand how their data is managed.</p> <p>To ensure compliance and timely communication, customers have the option to subscribe to notifications regarding changes to the sub-processor list.</p> <p>A sub-processor is an affiliate or third party that process data on behalf of our solution. Sub-processors act as a contractual party of the service agreement and process data in line with applicable data protection laws.</p> <p>In accordance with the Data Processing Agreement (DPA), any modifications or additions to sub-processors are communicated to customers, allowing them to stay informed and take any necessary actions as part of their own compliance processes. This approach reflects SAP Concur's commitment to data protection and transparency.</p>	Noted
Backup and recovery			
3.28	Is there a clear indication in the software or manuals as to how the data is backed-up and recovered?	<p>SAP Concur does not provide customer-facing documentation detailing data backup and recovery processes. However, we can confirm that:</p> <p>SAP Concur is ISO 22301 certified, ensuring that we have robust business continuity and disaster recovery measures in place.</p> <p>All data is regularly backed up and stored in geographically redundant data centers.</p> <p>Backup and recovery processes are tested routinely in line with our compliance requirements.</p> <p>Formal documentation (e.g., detailed procedures) is not shared externally, but the certification and controls are independently audited as part of our compliance framework.</p>	Noted
3.29	How often are backups taken and to what point can restores be done?	Full data backups weekly with incremental backups taken between full backups. There is no contractual agreement about RTO and RPO. However, as an internal goal and for our ISO22301, we have the target of achieving an RPO of 1h and an RTO of 12h.	Noted
3.30	How does the software facilitate recovery procedures in the event of software failure? (E.g. roll back to the last completed transaction).	<p>We are compliant and registered to ISO 27001, which requires the production, maintenance, and testing of a Disaster Recovery Plan (DRP). The current DRP is a formal recovery procedure for recovering the entire application in the alternate data center. Data is replicated to a warm site in near real-time for disaster recovery purposes.</p> <p>Our solutions been built with a high availability architecture to ensure that in the event of a failure, service performance continues to meet client expectations. This means that every tier of the architecture has either multiple servers in a cluster, or multiple network or SAN paths so that there is no single point of failure, all key components are implemented in parallel.</p> <p>The SAP Concur cloud deployment in AWS leverages the strength of their “availability zones” to provide three geographically close data centers, ensuring high availability and durability of customer data. In addition, traditional data recovery would be maintained through near-synchronous replication with an additional AWS region in a geographically disparate location. This replication should improve the ability to withstand outages and catastrophic events.</p>	Noted
3.31	If software failure occurs part way through a batch or transaction, will the operator have to re-input the batch or only the transaction being input at the time of the failure?	SAP Concur is a cloud-based solution, so there is no concept of local batch processing in the traditional sense. All data is stored centrally, and users typically interact with the system in real time. If an issue occurs, the platform will retain all completed and saved work up to the point of disruption.	Noted
3.32	What features are available within the software to help track down processing problems?	Concur Open provides real-time information on service availability and known outages. There is also real-time recovery and backup capability meaning that when minor fixes are required there is no needed downtime which would impact the end users.	Noted

Ref	Requirement	Response	Reviewer Comments
4.	DATA PROCESSING AND REPORTING		
Input and validation of transactions			
4.01	Is data input controlled by self-explanatory menu options?	Yes, SAP Concur provides self-explanatory menu options to control data input. The interface is designed to be user-friendly, with clear and intuitive menus that guide users through the data entry process. This helps ensure that data is entered accurately and efficiently, reducing the likelihood of errors.	Confirmed
4.02	Are these menus user/role-specific?	Yes	Noted
4.03	Can the creation or amendment of standing data (e.g. customer account details) be undertaken using menu options or dialogue boxes as opposed to requiring system configuration?	Yes, SAP Concur allows the creation and amendment of standing data, such as customer account details, using menu options and dialogue boxes. This user-friendly approach eliminates the need for complex system configuration, making it easier for users to manage data directly through the interface.	Noted
4.04	Does the software provide input validation checks such as: - [account] code validation? - reasonableness limits? - validity checks?	N/A - see tab 7 for details on checks and hard vs soft stops configured within the system	N/A
4.05	What control features are within the software to ensure completeness and accuracy of data input?	Input data validation is verified in the Risk Assessment, Threat Modelling, Static Analysis, Dynamic Analysis, and final security review. Refer to 'security activities in software development' section of the SAP Secure SDLC document for more information: https://www.sap.com/about/trust-center/security.html?pdf-asset=a248a699-627c-0010-82c7-eda71af511fa	Noted
4.06	How does the software ensure uniqueness of the input transactions? (i.e. to avoid duplicate transactions)	Each expense line items has a unique ID and we have flags to identify potential duplicate expenses.	Noted
4.07	Is data input by users validated by scripts or routines in the browser, or other client software, before transmission to the server?	At the application layer, business rules and validation checks are in place to detect and prevent duplicate transaction submissions based on key attributes such as timestamps, transaction IDs, or contextual metadata (e.g., user, vendor, or document reference). Additionally, API endpoints and ingestion mechanisms are designed to be idempotent, where applicable, to prevent duplicates in retry scenarios. At the database level, uniqueness is enforced through constraints such as primary keys, unique indexes, and integrity checks on relevant fields. In our environment using AWS RDS and Microsoft SQL Server, these constraints are implemented to guarantee transactional consistency and prevent duplicate records at the persistence layer.	Noted
4.08	Is data input by users validated by routines running on the server before data files are updated?	Expense types are mapped to general ledger codes, and Cost objects are imported from the master accounting system. This data can be checked by a Processor before it is extracted from the SAP Concur system.	Noted
4.09	Does the above validation ensure that data entered in all input boxes: - Cannot be longer than a maximum length? - Cannot contain unaccepted characters such as semi-colons etc?	Yes	Noted
4.10	Are input errors highlighted?	Yes	Noted
4.11	If Yes are they: - Rejected and error report generated on-screen? - Rejected and error reports generated? - Accepted and posted to a temporary account/area?	Warnings, such as missing information or policy checks can be flagged to the claimant to correct. This can be by amending the information or adding comments, depending on the client requirements.	Noted
4.12	Are responses to erroneous data input clear so that they do not lead to inappropriate actions?	Yes	Noted
4.13	Does the software have an automatic facility to correct/reverse/delete transactions?	SAP Concur does not provide an automated facility to correct/reverse/ delete transactions; this would need to be a manual check.	Noted
4.14	If yes, are these logged in the audit trail?	Yes, all changes are logged.	Noted
4.15	Are all data entries or file insertions and updates controlled to ensure that should part of a data entry fail the whole transaction fails?	Yes. These files are processed in a batch fashion, and thresholds for failure (number of allowable error records) are configurable	Noted
4.16	Are messages provided to users clearly explaining whether the data entry or file upload has been processed successfully or not?	Yes	Noted
Import and export of data			
4.17	Can files/attachments be uploaded and stored against any transaction?	Yes, users can upload receipt images.	Noted
4.18	Is there an additional charge made for storage of uploaded files? - If yes, please indicate the cost.	No, there is no additional charge.	Noted
4.19	Can data be imported into the system from multiple types of files, e.g. XLS, text, CSV?	Yes, SAP Concur supports the import of data from multiple file types, including XLS, text, CSV, and PDF for receipts. This flexibility allows users to easily integrate data from various sources into the system.	Noted

Ref	Requirement	Response	Reviewer Comments
4.20	Explain how the system validates imports into the system and what happens to any import which fails?	<p>We process and monitor batch jobs in an automated fashion, with alerts generated for any data output issues that may arise. Issues are resolved prior to encrypting and placing the file on the SFTP site for customer pick up. There is also a header record that summarizes the number of lines and total amount of the extract. This ensures that files are complete and data is accurate.</p> <p>After a transfer, the administrator will be informed by email once data submitted to us has been integrated. This notification will indicate whether the import was successful, successful with errors or failed. The administrator can then access further details from the administration portal explaining why errors occurred and where.</p> <p>As part of the file transfer process, files transferred via SFTP must first be encrypted using PGP. In the event of the files being corrupted during the transfer process, the files will fail the PGP integrity test and not decrypt. By using this method we ensure that both the confidentiality and the integrity of the files uploaded are preserved and ensures files corrupted after they were encrypted will not be imported.</p> <p>The SAE is downloaded by customer systems from the SFTP server. It is also PGP encrypted and part of the integration process will involve decrypting the file and re-downloading or requesting a new file in the event of a corrupted file. Prior to import, the integrity of the file should be checked and basic formatting checks should be performed.</p>	Noted
4.21	Are imported /interfaced transactions detailed in the audit trail? <i>[See also 3.27]</i>	All transactions are logged in the audit trail for transparency and accountability.	Noted
4.22	Can data be exported from all areas of the system to multiple formats e.g. XLS, CSV, PDF, text; if so specify which formats are supported?	<p>Data is available via CSV format file exchanges via Concur SFTP server and in XML / JSON via optional web services (RESTful APIs).</p> <p>RESTful APIs use HTTPS. The payload is encrypted in transit but the data itself on the secure channel is not encrypted. Please refer to developer.concur.com for more information.</p> <p>Data can also be exported from Intelligence reporting in, XLS, PDF and CSV formats. These files can be distributed via email or via SAP Concur solutions SFTP server.</p>	Noted
Data processing			
4.23	Does the software ensure that menu options or programs are executed in the correct sequence (e.g. outstanding transactions are processed before month end is run)?	<p>Yes, SAP Concur ensures that menu options and programs are executed in the correct sequence to maintain data integrity and operational efficiency. Here are some key features that support this:</p> <p>Workflow Automation: SAP Concur automates workflows to ensure that tasks are completed in the correct order. For example, outstanding transactions are processed before month-end procedures.</p> <p>Approval Processes: The system includes approval workflows that ensure critical steps are reviewed and authorized before proceeding.</p> <p>Batch Processing: SAP Concur uses batch processing for tasks like expense report approvals and payments, ensuring that these are completed in the correct sequence.</p> <p>Audit Rules: Configurable audit rules help enforce the correct sequence of operations by flagging any deviations.</p> <p>These features collectively help ensure that operations within SAP Concur are executed in the proper order, preventing errors and maintaining data accuracy.</p>	Noted
4.24	Does the software provide automatic recalculation, where appropriate, of data input? (e.g. VAT)	Yes, this is possible. SAP Concur can be configured to calculate VAT. We have a large number of pre-built templates and can also build custom templates where needed.	Confirmed
4.25	Is a month/period-end routine required to be undertaken?	Yes, typically customer will extract data on a regular schedule, such as at month end.	Noted
4.26	Is it possible to delete accounts if the balance is Nil but transactions have been recorded against the code?	In SAP Concur, it is generally not possible to delete accounts if transactions have been recorded against the code, even if the balance is nil. Instead, accounts can be deactivated to prevent further use while retaining the transaction history. This approach ensures that all historical data remains intact for auditing and reporting purposes.	Noted
4.27	What is the size and format of reference numbers and descriptions within:- - Ledgers? - Stock? - Currencies?	N/A	N/A
4.28	How does the software guard against/warn about duplicate account numbers on set up?	If a duplicate account number is detected, the system generates an error message to alert the user. This message typically provides details about the duplication and prompts the user to enter a unique account number.	Noted
4.29	How does the software enable the traceability [from, to and through the accounting records] of any source document or interfaced transaction?	A full audit trail of an expense submission is available, as are any configuration changes.	Noted
4.30	What drill down/around functionality is available within the software?	Drill down functionality is available within our reporting solution.	Noted
4.31	If the software uses a lot of standing information which changes frequently or regularly, does the software allow for such changes to be effected through the use of parameters or tables?	Yes there are options to import various data e.g. Employee data, cost centre data. We also handled the updating of localised rates e.g. Mileage and Tax rates.	Noted
Report writer			
4.32	Does the system have an in-built report generator or is a third-party solution used (if so please specify)?	Yes, it is inbuilt using Cognos.	Noted
4.33	Is the report writer based on a standard SQL-type approach and is it flexible and easy to use?	The reporting tool is based on IBM Cognos.	Noted
4.34	Can the report generator operate over the financial and operational aspects of the system, e.g. combining service metrics with financial information?	No, data is based on transactional data.	Noted
4.35	Is a comprehensive data dictionary provided to aid field selection?	Yes any fields that are in SAP Concur as a system, can be reported on.	Noted
4.36	Does the system provide a library of reports and templates which can be amended, saved and re-run?	Yes, SAP Concur provides a pre-built catalogue of reports.	Noted

Ref	Requirement	Response	Reviewer Comments
4.37	Can users create their own reports? If so, what are the controls on users doing this?	<p>Yes, custom reports can be built by users with the appropriate access levels.</p> <p>There are two additional services that are extension to the reporting tool, Intelligence and Consultative Intelligence:</p> <p>Intelligence allows clients access to an enhanced report writer but still using Cognos technology (as well as other features such as report scheduling, access to pre built dashboards).</p> <p>Consultative Intelligence includes the intelligence features as well as access to a reporting services team at Concur to put through consultancy / report building requests to that team.</p> <p>Concur also provides an additional "Data delivery service" which allows clients to take the data out of Concur to report in an external reporting solution</p>	Noted - these additional services were not assessed as part of our accreditation
4.38	Can users create saved searches /filters / queries?	Yes, admin users are able to build and save queries. These can then be easily accessed and run when needed.	Noted
4.39	Can regular reports be added to user menus in the appropriate area of the system?	Most recently accessed reports are displayed to the user.	Noted
4.40	Does the system support the production of on demand (interactive) and scheduled batch reports?	Yes, both are possible. SAP Concur can also schedule and deliver reports to an individual on a regular basis.	Noted

Ref	Requirement	Response	Reviewer Comments
5.	USABILITY		
Ease of use			
5.01	Does the solution provide a multi-language user interface?	Yes, SAP Concur's UI is available in over 20 languages.	Noted
5.02	Does the system allow for customizable branding and UI (e.g. corporate colour palate, upload company logo, etc)?	Businesses can add their logo but are not able to adjust the colour palate.	Noted
5.03	Does the system have a similar look and feel and overall and consistency between screens and modules?	Yes	Noted
5.04	Is data entry easily repeated if similar to previous entry?	Yes, SAP Concur does offer the option to copy an existing expense line item if the user is claiming for something similar, for example, a toll on consecutive days.	Noted
5.05	Does the software prevent access to a record while it is being updated?	Yes	Noted
5.06	Is there locking at file or record level?	As a SAAS SAP Concur does not lock files or records in the traditional On Premise sense, but it uses built-in controls to prevent unauthorized edits and ensure users cannot overwrite each other's changes.	Noted
5.07	Does the software allow for the running of reports whilst records are being updated?	SAP Concur's reporting solution is updated overnight, so will reflect all submitted expense reports up until the previous day.	Noted
5.08	Can timestamps or user comments be added to transactions?	Yes, there is a full audit trail visible to the user, approver and processor which shows dates, times and comments.	Noted
5.09	Is there the ability to store preferences and default values on a per-user basis. e.g. department/team/user?	Yes, these fields are typically held in the employee profile and each business can choose to make these read only, editable or hidden.	Confirmed
5.10	Does the system have the ability to provide user-defined fields with associated validation of data input?	Yes, custom fields can be added by a business as needed. These can be made up of list data or free text.	Noted
5.11	Can the system provide users with reminders and notifications e.g. workflows?	Yes, SAP Concur can generate email and/or push notifications for multiple items, including credit card transaction notifications, approvals and returned expense claims.	Noted
5.12	If the system provides workflows, does it have functionality to substitute/delegate authorisations?	Yes, if an approver is out of the business, they can set a delegate to approve in their absence.	Noted
5.13	Describe the tools and features available for a power user to make configuration changes such as amending a workflow.	Admin users are able to make changes to almost all parts of the configuration, including, but not limited to, expense types, GL codes, workflow, forms/fields, custom fields, mileage rates, policy rules and user groups.	Noted
5.14	Is there the ability for users to define and configure layouts of letters and forms?	Yes. Admin users are able to configure expense forms to change what is visible, editable, read-only or hidden. This can be made on multiple screens, such as expense header, line item or allocation.	Noted
5.15	Can users save the parameters of searches?	The ability save searches is possible for Finance/ Processor users; these searches are saved as 'Queries' and then can be run when required. Approvers and Claimants cannot conducted and save searches; instead there are predefined views e.g. 'View- Active Claims'	Noted
5.16	Does the system have a "universal search" option, allowing a search to be undertaken over all modules of the system?	N/A - Expense is one module	N/A
5.17	Can the system store menu option 'favourites' on a per user basis?	Yes, a user can mark favourites for things such as attendees or allocations.	Noted
5.18	Can a user open multiple windows accessing the same or different modules of the system?	Yes, users can open multiple browser windows or tabs to access different parts of SAP Concur, including separate modules like Expense, Invoice, or Travel.	Noted
5.19	Can more than one software function be performed concurrently?	Yes, it's theoretically possible, but not applicable to SAP Concur. We don't see any use case here.	Noted
User documentation and training			
5.20	Confirm whether a user manual / instructions is provided and how this is distributed?	Support is available online through the help menu. We have a mixture of documents and videos for user support.	Confirmed
5.21	Does the user manual include: - An index or search facility? - A guide to basic functions of the software? - Pictures of screens and layouts? - Examples? - A tutorial section? - Details of any error messages and their meanings?	Yes, the help menu has search facility, basic introductions (get started), screenshots and videos available.	Noted
5.22	Is context-sensitive help available within the system?	Yes https://help.sap.com/docs/	Noted
5.23	Is the manual and/or help editable by the user (subject to the permissions matrix)?	The help menu isn't editable but businesses can add links to external documents.	Noted
5.24	Will the Software House make the detailed program documentation (e.g. file definitions for third party links) available to the user, either directly or by deposit with a third party (ESCROW)?	No – as SaaS, our customers do not have an escrow agreement with SAP Concur.	Noted
5.25	Please detail the training options available?	See 5.26	Noted
5.26	Who provides training: - Software House? - VAR?	Overview training is typically provided to the admin team as part of the implementation. End user training would typically be carried out by the client or they would use the self help guides, videos and chat.	Noted
Support and maintenance			
5.27	How is the software sold: - Direct from the software house? - Via a Value Added Reseller (VAR) or Integrator?	SAP Concur has multiple options for purchase, this can be directly from SAP Concur or by one of our reseller partners.	Noted
5.28	How is the product supported: - Direct from the software house? - Via a Value Added Reseller (VAR) or Integrator?	This would depend on how the solution is purchased and what services are in scope. Most customers would buy direct and SAP Concur would be the first line of support.	Noted
5.29	Do VARs have to go through an accreditation process?	Yes	Noted
5.30	Is the software sold based upon number of named users or a number of concurrent users?	Pricing is based on the number of expense reports submitted per month, not a user based licence model.	Noted
5.31	The supplier should detail the support cover options available, covering: - The hours provided? - Associated costs? - The global regions covered?	Yes. The hours provided- 24/7 Chat, phone and portal. - Associated costs- To be determined through scoping if applicable - The global regions covered- we offer a fully global system with support: https://assets.concur.com/tech-pubs/SAP-Concur-Training-Library/ASC-Guides/Getting_the_Most_ASC_ENG.pdf	Noted
5.32	Detail the process by which customers raise support requests and how these can be viewed/managed?	Please refer to the following guide: https://assets.concur.com/tech-pubs/SAP-Concur-Training-Library/ASC-Guides/Getting_the_Most_ASC_ENG.pdf	Noted

Ref	Requirement	Response	Reviewer Comments
5.33	Please note the methods of support available: - Telephone? - Internet chat? - Remote access to customer workstation? - Other, please specify?	Yes to all methods mentioned. Other: https://assets.concur.com/tech-pubs/SAP-Concur-Training-Library/ASC-Guides/Navigate_CSP_ENG.pdf https://assets.concur.com/tech-pubs/SAP-Concur-Training-Library/ASC-Guides/Getting_the_Most_ASC_ENG.pdf	Noted
5.34	Do you offer service credits for failure to meet performance around SLA and uptime (if applicable)	Yes - see detail here https://www.sap.com/about/trust-center/agreements/cloud/cloud-services.html?sort=latest_desc&search=sla&tag=language%3Aenglish&pdf-asset=6cac64a3-887e-0010-bca6-c68f7e60039b&page=1	Noted
5.35	What is your escalation path for tickets which have not been resolved within a reasonable time?	Client Success Manager will raise an escalation against the case. This will be addressed directly with the CSM and Support leadership.	Noted
5.36	How often are general software enhancements provided?	SAP Concur produces a publicly viewable roadmap which details upcoming enhancements. These enhancements are typically delivered on a monthly release schedule.	Noted
5.37	Will they be given free of charge?	In some instances, but not all.	Noted
5.38	How are enhancements and bug fixes provided to customers?	Enhancements are rolled out on a monthly basis.	Noted
5.39	Is "hot line" support to assist with immediate problem solving available?	Yes, SAP Concur offers support for End Users and also for Admins	Noted
5.40	If so, is there an additional cost involved?	Yes	Noted
5.41	At what times will this support be available?	24/7	Noted
Integration and www facilities			
5.42	Are the different modules of the system fully integrated (i.e. no set-up effort required in order to use the various modules together)?	Yes	Noted
5.43	Are they integrated on real time basis or batch basis?	Real time for all other than the reporting solution which is an overnight schedule.	Noted
5.44	Can the software be linked to other packages e.g. word processing, graphics, financial modelling, to provide alternative display and reporting facilities?	Yes, SAP Concur offers a web service solution which allows customers to build connections to 3rd party solutions.	Noted
5.45	Can definable links to spreadsheets be created?	No, not applicable.	Noted
5.46	Does the system provide a secure document storage capability: If so, please give examples of the document types saved and what transactions these might relate to.	Yes as a cloud based system all data and receipt images are retained/stored within the service.	Noted
5.47	Can documents be scanned into a secure repository?	Receipts are uploaded directly into SAP Concur, either via the desktop, mobile app or by forwarding emails to a dedicated inbox.	Noted
5.48	Does the system provide data migration tools for transactional and master data sets (e.g. employees customers, suppliers, journals, invoices).	Data can be transferred to and from in a number of ways, either via flat file import, SFTP, web services or pre-built connector (depending on the target system). On Demand - user initiated, excel CSV Extract, Customised for ERP: The site is configured with two different editions, and complexities vary based on customer requirements. Master data for Concur Expense includes employee data, cost centres, and organizational structure, typically involving two feeds set up as scheduled recurrences. Customers can perform imports manually on demand, although automation is preferred. SFTP - scheduled extract, overnight processes, file encryption: Historically, most customers use SFTP for automation, which is bundled with implementations to provide an out-of-the-box solution. Web Services - APIs, Near Real-time, ERP Agnostic Open Standards: Web services are offered as an optional feature, enabling near real-time updates and requiring an additional subscription. They provide REST APIs across the suite, with over 70 APIs available, facilitating integrations developed by app centre partners. SAP Concur has native integrations with SAP ERP systems and pre-built integrations for systems like Netsuite, Quickbooks, Xero, and SAP ERPs. Standard interfaces and specifications are provided for APIs and imports, with documentation outlining requirements. A standard accounting extract file is provided with necessary information for the finance system, with customization options available for posting to ledgers and performing payments through the ERP system.	Noted
5.48 cont.		Partners - Specialist Integration Partners, Out of the box, ongoing support / maintenance: Key data that flows through SAP Concur partners could be everything and anything. For example trainline partner would include travel and booking information (time, date, trainline, amount etc). Key data flows/ transfers include: Card data - company card transactions can be imported into Concur to automatically appear in a users expense list Employee Data - SAP Concur supports the import of employee data from HR systems or ERP systems using both API and import files. This ensures that all relevant employee information is accurately transferred into the Concur system, facilitating seamless expense management. List Imports - Various list imports can be configured based on customer requirements. Examples include: - Client Project Data: Importing data related to client projects to ensure accurate expense allocation. - Attendees: Importing lists of personal information about attendees that are attached to expenses. - Exchange Rates: While SAP Concur manages exchange rates automatically, customers can also import their own exchange rates if preferred. Accounting Extract - The accounting extract export contains all necessary information for the finance system, including nominal ledgers behind expense types and the allocation of cost centre coding. This extract ensures that all financial data is accurately captured and ready for posting to ledgers.	

Ref	Requirement	Response	Reviewer Comments
5.48 cont.		Payments - Customization options within SAP Concur allow customers to select specific rows for posting to their ledgers and performing payments through their ERP system. This flexibility ensures that the payment process aligns with the organization's financial management requirements.	
5.49	What connection mechanisms does the software have and what breadth of functionality in terms of: - operations (add, update, delete)? and - what transactions/data it can access? E.g. if webservices APIs available, then can customers connect to whatever software they wish?	<p>SAP Concur offers several connection mechanisms, including Web Services APIs, and SFTP for secure file transfers.</p> <p>Operations (Add, Update, Delete): The APIs support operations such as adding, updating, and deleting data for expenses, invoices, and users, depending on the API endpoint and permissions. SFTP is typically used for secure, batch file transfers (e.g., list import, employee import, invoices, vendor information) rather than real-time operations.</p> <p>Transactions/Data Access: APIs provide access to a broad range of transactional data, including expense reports, invoices, user data, and vendor information, based on configured permissions. SFTP is used for file-based data exchanges like bulk uploads or downloads.</p>	Noted
5.50	Does the system support mobile working?	Yes, both native applications for IOS and Google play store.	Noted

Ref	Requirement	Response	Reviewer Comments
6.	<u>SaaS HOSTING</u>	This evaluation covers the system but not the method by which it is delivered and/or contracted for. Potential users need to satisfy themselves on the security and disaster recovery aspects and licensing of the online system and any data protection issues of their own and customer/supplier information, contained therein, being held on the system, as well as the return of the data when the contract expires or is terminated.	
Data centres and customer data			
6.01	Whose data centres are used and where are these located: - If hosted -- where data centre controlled by a third-party? - If SaaS -- where the software vendor will be in control?	Data location depends upon the region chosen during implementation. SAP Concur has AWS data centers in the United States (for North America) - US2, EMEA - EU2 in Germany and Ireland. We use them for IaaS (infrastructure as a Service) and PaaS (Platform as a Service). SAP Concur manages the infrastructure. https://aws.amazon.com/compliance/ https://aws.amazon.com/compliance/gdpr-center/ https://aws.amazon.com/compliance/data-center/ https://aws.amazon.com/compliance/data-center/data-centers/ We are complying with the transfer of personal data under the EU Privacy Directive by entering into Standard Contractual Clauses. Our DPA is here - https://www.sap.com/about/trust-center/agreements/cloud/cloud-services.html?search=Data%20Processing&sort=latest_desc We follow EU GDPR compliance and carry a BS 10012 certificate https://www.sap.com/about/trust-center/certification-compliance/compliance-finder.html?tag=finder-technical:trust-center/document-type/bs-10012	Noted
6.02	Does the customer get a choice of the jurisdiction in which their data resides?	Yes, see above.	Noted
6.03	What certification(s) do you or your platform operators hold relating to your data centres and your business operations?	<ul style="list-style-type: none"> • SOC 2 Type II report https://www.sap.com/about/trust-center/certification-compliance/sap-concur-soc-2-2024-h1.html • SAP Concur SOC 2 Bridge Letter Package https://www.sap.com/about/trust-center/certification-compliance/sap-concur-soc-2-isae3000-bridge-letter-latest.html • SOC 1 report https://www.sap.com/about/trust-center/certification-compliance/sap-concur-soc-1-2024-h1.html • SAP Concur SOC 1 Bridge Letter Package https://www.sap.com/about/trust-center/certification-compliance/sap-concur-soc-1-isae3402-bridge-letter-latest.html • ISO 27001 https://www.sap.com/about/trust-center/certification-compliance/compliance-finder.html?search=Concur%20ISO%2027001&sort=latest_desc&pdf-asset=42edaa99-c17e-0010-bca6-c68f7e60039b&page=1 • ISO27018 https://www.sap.com/about/trust-center/certification-compliance/compliance-finder.html?search=concur&sort=latest_desc&pdf-asset=8a82aa99-c17e-0010-bca6-c68f7e60039b&page=1 • ISO27017 https://www.sap.com/about/trust-center/certification-compliance/compliance-finder.html?search=concur&sort=latest_desc&pdf-asset=02b0aa99-c17e-0010-bca6-c68f7e60039b&page=1 • ISO22301 https://www.sap.com/about/trust-center/certification-compliance/compliance-finder.html?search=concur&sort=latest_desc&pdf-asset=4e4aab99-c17e-0010-bca6-c68f7e60039b&page=1 • SAP Concur PCI Responsibility Matrix for PCI DSS 4.0 https://www.sap.com/about/trust-center/certification-compliance/compliance-finder.html?search=concur&sort=latest_desc&pdf-asset=00cba55d-c17e-0010-bca6-c68f7e60039b&page=1 	Noted
6.04	Do you or your platform operator have an SSAE16 (System and Organization Controls) report available?	Yes, see above.	Noted
6.05	What are the physical controls over the:- - Premises? - Fileservers? - Communications equipment?	We utilize and AWS Tier III+/IV collocation data centers. AWS do not have access to client data or systems. AWS provides only physical power, internet connectivity, and physical security of the hosting facility. We undergo ISO27001 certifications which include physical security reviews. All employees, external parties, and visitors must comply with the following requirements: <ul style="list-style-type: none"> • Badges shall be displayed in plain sight between the neck and the waist while on SAP premises. • Card holders must not use their access card to allow access for others. • Tailgating is not permitted. Card holders are required to use their cards at every card reader whether or not the door/gate is already open as they approach. • Any lost or stolen card must be immediately reported to SAP Physical Security. • All visitors must be escorted by their host at all times while on SAP property and in restricted areas. • Photography, filming, or recording on SAP property is not permitted without approval/consultation with SAP Physical Security. • Movement of bulk items (equipment, boxes, crates, luggage, etc.) out of buildings requires an approved Equipment Removal Form. • Combinations, codes, or personal identification numbers (PINs) used for physical security must be changed every six months. • Personal items, bags/briefcases, cabinets, and space assigned by SAP are subject to search based on probable cause and in accordance with applicable legislation and regulations. • Weapons of any kind are prohibited on all SAP property unless such prohibition is contrary to local law. 	Noted
6.06	Is the space in this/these data centre(s) shared with any other companies?	Yes. SAP Concur is hosted on Amazon Web Services (AWS), which operates a multi-tenant cloud environment. This means that infrastructure resources are shared across multiple customers; however, strict logical separation and security controls are enforced to ensure data isolation and protection between tenants in accordance with industry best practices and compliance standards.	Noted

Ref	Requirement	Response	Reviewer Comments
6.07	Is data for different customers/companies kept:- - On separate servers? - In different databases? - In separate database tables? - In a database with data for other customers and companies using logical security to partition customers' data?	Our solution is designed on a true SaaS platform. All clients access a single instance of the service, commonly referred to as 'multi-tenant'. Data access and visibility is logically controlled based on the identity of the logged in user. Once the user has authenticated into the service, appropriate data is stored in separate database instances within the SQL Server clustered data tier. Clients cannot access, intentionally or unintentionally, another client's data. Databases run on shared servers; however, separate databases or file folders are used where possible and appropriate. Travel records are stored in a single repository for all clients (much like the GDSs that they interact with), with the application logically separating the data Concur Premium/Professional Expense transaction records are stored in a dedicated RDBMS instance for each client (in effect their own database) Our Standard edition transactions are stored in a single shared repository, with the data segregated logically by the application Database information cannot be directly accessed. Only application servers are authorized to connect to the database.	Noted
6.08	How is it ensured that data for different customers and companies is reliably identifiable and only accessed by authorised users for each customer/company?	All clients access a single instance of the service, commonly referred to as 'multi-tenant'. Data access and visibility is logically controlled based on the identity of the logged in user. Once the user has authenticated into the service, appropriate data is stored in separate database instances within the SQL Server clustered data tier. Clients cannot access, intentionally or unintentionally, another client's data.	Noted
6.09	What controls are in place to prevent users from one customer/company accessing data from another customer/company by accident or by design?	SAP Concur prioritizes the confidentiality of sensitive customer information through a robust security framework that aligns with industry best practices and global compliance standards. Below are the key measures we implement: Encryption: <ul style="list-style-type: none"> All sensitive customer data is encrypted in transit using Transport Layer Security (TLS) and at rest using Advanced Encryption Standard (AES) with 256-bit keys. Encryption keys are managed securely, with regular rotations & strict access controls. Access Control and Authentication: <ul style="list-style-type: none"> Strict access controls ensure that only authorized personnel can access sensitive data, based on the principle of least privilege. Multi-factor authentication (MFA) is enforced for internal and customer-facing systems. Data Isolation: <ul style="list-style-type: none"> Data is logically separated by tenant, ensuring that customer information remains isolated and protected within our multi-tenant architecture. Compliance and Certifications: <ul style="list-style-type: none"> SAP Concur adheres to globally recognized security standards, including ISO 27001, SOC 2 Type II, and GDPR. These certifications demonstrate our commitment to maintaining the highest levels of security and data protection. Monitoring and Incident Response: <ul style="list-style-type: none"> Continuous monitoring of our systems ensures timely detection and response to potential security threats. A dedicated Security Operations Center (SOC) operates 24/7 to manage incidents and mitigate risks. 	Noted
6.09 cont.		Employee Training and Awareness: <ul style="list-style-type: none"> All employees undergo mandatory security training to ensure they understand their role in safeguarding customer data. Periodic assessments and awareness programs reinforce a culture of security. Data Minimization and Retention Policies: <ul style="list-style-type: none"> SAP Concur collects and retains only the data necessary for operational purposes and complies with customer-specific data retention policies. Third-Party Risk Management: <ul style="list-style-type: none"> All third-party vendors and partners undergo rigorous security evaluations to ensure they meet SAP Concur's confidentiality standards. Secure Development Practices: <ul style="list-style-type: none"> All software development follows secure coding practices, with regular code reviews, vulnerability scanning, and penetration testing to identify and mitigate risks early in the development lifecycle. Customer-Controlled Privacy Settings: <ul style="list-style-type: none"> SAP Concur provides customers with tools and settings to configure privacy and security preferences, enabling them to tailor access controls and permissions as needed. These measures collectively ensure that sensitive customer information remains confidential and secure throughout its lifecycle with SAP Concur. 	

Ref	Requirement	Response	Reviewer Comments
6.10	How is Internet communication traffic monitored to identify potential problems before they happen: - From a performance perspective? - From a security standpoint?	<p>Proactive Security & Monitoring Overview</p> <p>SAP Concur, hosted on Amazon Web Services (AWS), maintains a robust and standardized approach to logical and network security monitoring. The following key practices are in place:</p> <p>Proactive Monitoring (Logical/Network Security) SAP Concur's Security and Risk Management team actively monitors industry sources, vendor updates, and security communities for threats that may affect Concur services.</p> <p>24/7 automated monitoring is in place, supported by backup personnel to ensure continuous threat detection and incident response.</p> <p>All potential security threats are thoroughly investigated, and defined procedures exist for immediate resolution and containment of any incident.</p> <p>Host-Based Security & Alert Monitoring The team monitors vendor security updates, hacker forums, and industry threat intelligence platforms to anticipate vulnerabilities.</p> <p>Monitoring includes host-based Intrusion Detection Systems (IDS) and File Integrity Monitoring (FIM), which alert operations personnel to any unauthorized or unexpected changes on servers.</p>	Noted
6.10 cont.		<p>File Integrity Monitoring (FIM) FIM tools are deployed across all servers to detect and alert on any unauthorized changes.</p> <p>These alerts are monitored 24/7 to ensure quick investigation and response.</p> <p>Enterprise & Application Performance Monitoring A standardized monitoring methodology is implemented across all customer environments.</p> <p>Monitoring tools observe:</p> <p>Server resource usage</p> <p>Transaction response times</p> <p>Error rates and rejected requests</p> <p>Network service availability</p> <p>Performance issues are identified in real time and addressed through automated alerting.</p> <p>Global Operations Center (GOC) The GOC acts as the central triage point for all monitoring alerts, providing 24/7 oversight.</p> <p>If escalation is needed, the appropriate call staff are notified immediately.</p>	
6.10 cont.		<p>Tools & Technologies Used Industry-leading enterprise monitoring tools are used across the environment.</p> <p>These tools rely on standards like SNMP, WMI, JMX, and SAP Concur's own custom logging systems.</p> <p>All monitoring data is consolidated to a central location, allowing for rapid issue identification and event correlation.</p> <p>Security Monitoring Monitoring includes multiple redundant IDS sensors, File Integrity Monitoring, and continuous observation of:</p> <p>Internet-based, internal, and VPN network traffic</p> <p>Firewall ACL violations</p> <p>Antivirus events</p> <p>Security event logs</p>	

Ref	Requirement	Response	Reviewer Comments
6.11	What procedures are in place to prevent a break in Internet Connection (at the server, client or in between) from causing data corruption?	<p>Our network architecture ensures that sensitive client data is protected through best business practice security policies and procedures. Network security encompasses needs-based access, proper network segmentation, and Security and Risk Management oversight.</p> <ul style="list-style-type: none"> Secure Internal Administration Network: We employ a complete internal infrastructure to backup and monitor servers through secure connections. All web servers contain at least two Network Interface Cards (NICs). One NIC is connected to the production environment, and the other is connected to our Operations internal private network. The IP addresses of these servers are protected from third parties through our non-routable network. Hardened Router Configurations: Router configurations are used to correctly route packets to their proper destinations, and to restrict traffic. Access Control Lists (ACLs) on the front-end routers are used to stop common attacks that could affect the environment, including IP spoofing and limited denial-of-service attacks. Network Segmentation: Our multi-segmented network architecture prevents direct public contact or connection to our private network segment. This ensures client information is not accessible directly from the Internet. We utilize intrusion detection systems that monitor all TCP/IP incoming and outgoing traffic between network segments. Front-end Load Balancers: Access to our services is managed with redundant load balancers. The load balancers provide a variety of functions including session termination, load balancing, network address translation (NAT), and port address translation (PAT). 	Noted
6.11 cont.		<p>Distributed Denial of Service (DDoS) protection: All of our service locations are protected by a solution that protects the availability of our services even when under a distributed denial of service (DDoS) attack.</p> <ul style="list-style-type: none"> Activity Log Aggregation: Log activities from network devices and systems are aggregated through an activity log collection system. Alarms are generated for those events that warrant immediate attention. Proactive Monitoring: Security and Risk Management continuously monitors industry communities for news of security alerts, as well as vendor and partner security changes that may affect Information Services and our product line. Information Services has 24/7 automated monitoring with backup personnel. Intrusion Detection Systems: Intrusion Detection System (IDS) technology is an integral component of our comprehensive enterprise security strategy. The IDS alerts us of suspicious IP traffic or log activity that occurs on our systems and networks. Where possible, isolated IDS servers bear the security audit load, reducing overall consumption of resources within the application servers to zero levels. Active Vulnerability Assessment: Our Security Engineers perform infrastructure security scans on a regular basis using an approved PCI scanning vendor from the Internet as well as from internal scanning appliances. Discovered vulnerabilities are managed through our remediation process in accordance with industry best practice. Web Application Firewalls: Front-end web application firewalls protect our services by blocking traffic that could represent attempts to steal application data or break in to our web applications. These firewalls are highly distributed and monitored. 	
6.11 cont.		<ul style="list-style-type: none"> Multiple Firewall Layers: We utilize multiple layers of firewalls that protect applications and client databases. Application firewalls permit traffic only from web servers to reach application servers, and database firewalls permit database queries only from application servers. VPN: Our Operations personnel use VPN when connecting and transmitting from outside the trusted network. This VPN secure tunnel offers internal Operations personnel highly secure remote connectivity to perform after-hours maintenance or troubleshooting. Multi-factor authentication is required for all or our personnel with access to systems containing customer data. Data Protection: All networks, systems, databases, and applications that contain customer data are managed by full time employees within a Tier 4 datacenter. Access to customer data is granted on a least-privilege, need-to-know basis. Digital Certificates and SSL: Our services utilize web server digital certificates to verify the authenticity of all client sites. Digital certificates are used to encrypt all Internet web traffic between clients and servers. Our services utilize TLS 1.2 or higher to ensure that HTTP communication between our clients and our servers is encrypted. 	
6.12	Are communications between the user's computer and the software service encrypted: - User log in data only? - All data exchanged between user client and software service?	<p>For data in motion, all application access is encrypted-in-transit over HTTPS using (TLS) Transport Layer Security (TLS) 1.2 by default.</p> <p>We support SFTP for file exchange of PGP encrypted files.</p> <p>For data at rest, we support AES-256 with split keys for encryption of credit card numbers, passport number and banking information. Passwords are one-way hashed with SHA-2. Backup media are encrypted with AES-256.</p> <p>All outgoing e-mail notifications sent from the system are securely encrypted using TLS.</p>	Noted
6.13	Is data on your servers encrypted at rest?	<p>For data at rest, we support AES-256 with split keys for encryption of credit card numbers, passport number and banking information. Passwords are one-way hashed with SHA-2. Backup media are encrypted with AES-256.</p> <p>All outgoing e-mail notifications sent from the system are securely encrypted using TLS.</p>	Noted
6.14	What level of encryption is used?	see above	Noted
6.15	Is a staging environment provided that is an exact replica of production; which can be used for testing purposes?	Yes	Noted

Ref	Requirement	Response	Reviewer Comments
6.16	Is a test environment provided to test configuration changes? If so, is there an additional charge for this?	<p>Clients have the option of a dedicated and separate Test Environment for a fee.</p> <p>A Concur development environment is not necessary for clients as SAP Concur takes care of all development work on the Concur platform.</p> <p>We provide a Test User feature that can be used to test our functionality within the Production environment. This feature is especially helpful when customers will be implementing a new expense group where other expense groups are already in a Production environment.</p> <p>To use the Test User feature, the Employee Administrator tool is used to create one or more "test employees", each marked as a test user. Employees marked as test users work within a Production environment exactly like regular employees without worry that test users' transactional test data will affect "real" (Production) data within our solution.</p> <p>The system incorporates certain safeguards that, while allowing testing access to areas of our solution, prevent test data from being incorporated in "real" system operations, such as extracts. In addition, customers may generate test-only extracts useful for validating bridge programs for extracts. When customers complete the testing activities, customers may purge the system of all test employee transactional data.</p> <p>Clients can use the Test User feature for a variety of purposes, such as:</p> <ul style="list-style-type: none"> • Performing end-to-end testing beginning with report submission and ending with report extraction • Validating and adjusting our configurations such as workflow, forms and fields, audit rules, policies, email notification, imaging, and other configurations • Creating test extracts to validate bridge programs for extracts • Creating training materials from the working environment • Training employees directly in the working environment. 	Noted
Access to customer data			
6.17	What are the implications of the Data Protection Act over information held by the hosting service provider, and how does the vendor mitigate these?	<p>SAP Concur fully complies with applicable data protection laws, including the GDPR and other regional equivalents of the Data Protection Act. As a data processor, SAP Concur hosts and processes customer data on behalf of its clients under strict contractual and technical safeguards:</p> <p>Data Processing Agreements (DPAs): Customers sign a DPA with SAP Concur that outlines roles, responsibilities, and compliance measures related to data protection, privacy, and international data transfers.</p> <p>Hosting and Storage: Data is hosted in highly secure, ISO 27001 and ISO 22301-certified AWS data centers. Data residency options are available to meet regional compliance requirements.</p> <p>Access Controls and Encryption: Data is encrypted in transit and at rest. Strict access controls and role-based permissions ensure that only authorized personnel can access customer data, with all access being logged and monitored.</p> <p>Sub-processor Transparency: SAP Concur maintains a public list of authorized sub-processors and provides mechanisms for customers to be informed of any changes.</p> <p>Data Subject Rights: SAP Concur supports customers in fulfilling data subject rights requests (e.g., access, deletion) in accordance with legal obligations.</p> <p>These measures ensure that customer data is managed responsibly and in compliance with applicable data protection legislation.</p>	Noted
6.18	Are you subject to any legal or regulatory requirements obliging you to retain a copy of customer data?	Retention of necessary data: SAP Concur retains any necessary data for compliance purposes as required by law, ensuring adherence to regulatory standards.	Noted
6.19	Who will be able to access or see customer data?	<p>We have a layered security model that includes access controls based on ISO 27001, with the minimum level of privileges granted to appropriate Information Services personnel based on their specific job description and role.</p> <p>We ensure that access is granted based on the minimum level of privileges required to perform each specific job function. Roles are separate in such a way that a specific employee will not have access to multiple security layers.</p> <p>This is audited by ISO 27001 auditors.</p> <p>SAP Concur employees in support, implementation, and company administration are also able to access customer user and company data. All SAP Concur employees undergo a background check upon employment, at-hire & annual security awareness training & certification and only full-time employee staff, no 3rd party or temporary staff, are granted access to the management console where their role justifies it. All access to the management console is logged and in the event of an incident we will work with the customer to identify the employee who had access to the system. Where required by national legislation, we will provide details upon request of users who had access to a system at a given time.</p> <p>We have implemented a terminal services infrastructure to facilitate and control all access to applications, systems, and infrastructure that stores and processes SAP Concur customer data. This system ensures that only valid SAP Concur personnel may access customer systems, and that customer data cannot be exported from customer systems.</p>	Noted
6.20	Explain the procedures to prevent unauthorised access from staff, or contractors, working for the service provider or any other people with access to the service provider's internal systems.	see above	Noted

Ref	Requirement	Response	Reviewer Comments
6.21	Explain the release management procedures in place and the associated segregation of duties ?	<p>We use an agile process-driven approach incorporating specification, designs, schedules, QA rounds, defect tracking, source control, configuration management, and release management in its software development life cycle (SDLC). The net result is a rapid, efficient development environment focused on constant improvement and innovation. Primary characteristics of our SDLC include:</p> <ul style="list-style-type: none"> • Software is built in iterations. Each iteration delivers a functional version of the system. This iterative model is particularly well suited for the software as a service delivery. • Release tempo is typically 4 weeks; this is a long term sustainable pace. • Frequent product input from (Support, Services, and Product Management) is important. • Documentation is important; many revisions will be based on interpersonal, informal meetings and feedback. Program Management consolidates these items. • Development team needs the flexibility to re-organize project staffing and roles as necessary. • Development team focuses on how to improve process efficiency based on changing factors. • Focus on excellence. <p>SAP Concur employs role-based access control to ensure that users only have access to the functions necessary for their roles. This helps prevent conflicts of interest and reduces the risk of fraud.</p>	Noted
6.22	Is there sufficient segregation of duties preventing system developers from accessing and changing live applications and data files?	Yes, Application development is performed on separate networks, and developers do not have access to customer cloud applications or infrastructure. Developers also have their own data and do not use customer data for testing.	Noted
6.23	Explain the review and approval procedures covering system operations staff when emergency changes need to be made to live applications and data?	<p>Any affected customers are notified without undue delay of any major upgrades or emergency maintenance. Customers can monitor up time at SAP Concur Open https://open.concur.com/</p> <p>Emergency changes are expedited with appropriate approvals and documentation, allowing SAP Concur to respond quickly to critical issues without bypassing necessary controls.</p> <p>Emergency monitoring has the objective to identify vulnerabilities rated as “very high” (critical). Vulnerability emergency candidates are: • Vulnerabilities with CVSS v3.1 scoring >= 9.0 • Vulnerabilities actively exploited in the wild • Vulnerabilities with high risk to SAP or SAP customers</p>	Noted
6.24	Is an audit trail always maintained of these emergency changes?	Yes	Noted
6.25	What procedures are in place when members of staff leave to ensure that their system access is stopped?	<p>Logical access to SAP Concur's production environment and its federated applications are removed within 7 business days of the user's termination date. To identify any discrepancies in access removal, a daily generation and comparison of termination reports for employees and external workers with Concur production environments is performed. Any discrepancies identified are investigated, and user access removal tickets are created to revoke access for terminated employees and external workers. We perform three types of quarterly access review processes, to ensure that only authorized personnel have access to SAP Concur systems.</p> <ul style="list-style-type: none"> • Termination review. This is a detailed check to ensure that all terminated actions have been carried out. • User re-certification. This is a detailed check to ensure that every person with access to a system is still required to have their access. • Dormant account review. This is a detailed check to check for user accounts that have not been used in the prior 90-180 days. Such unused accounts are subject to restriction or removal. 	Noted
Platform and service levels			
6.26	Which databases and servers are used to host the software?	<p>SAP Concur is a cloud-based SaaS solution hosted in SAP-managed data centers .By default, our platform ensures that all customers (regardless of region) benefit from the same multi-tenanted architecture and robust security measures, providing a consistent and secure experience globally.</p> <ul style="list-style-type: none"> • SAP Concur North America (US2) <ul style="list-style-type: none"> o Primary: AWS Oregon o Remote backup: AWS Ohio • SAP Concur EMEA (EU2) <ul style="list-style-type: none"> o Primary: AWS Frankfurt o Remote backup: AWS Ireland 	Noted
6.27	What forms of user authentication are supported e.g. user names, passwords certificates, tokens etc.?	SAP Concur offers Multi-Factor Authentication (MFA), combining knowledge-based (passwords) and possession-based (tokens) factors. This layered authentication mitigates risks of unauthorized access by requiring two or more verification steps. We also support SAML 2 based SSO.	Noted
6.28	What is the proposed product/service availability percentage?	<p>Contractual SLA for uptime is set at 99.7% and there is no downtime associated with maintenance windows "service-level-agreement-for-sap-cloud-services" (https://www.sap.com/about/trust-center/agreements.html)</p> <p>The solution is generally available during the maintenance window through the use of load balancers and pools of virtual servers that can be updated separately.</p>	Noted
6.29	What percentage availability has been achieved over the past 12 months?	99.99+ % for Expense , 99.99+% for Travel, 99.995 % for Invoice	Noted
6.30	Is a service level agreement ("SLA") offered regarding: - Service availability? - Data recovery?	Yes for service availability. Contractually we provide a monthly SLA of 99,7% with corresponding fines. There is no contractual agreement about RTO and RPO. However, as an internal goal and for our ISO22301, we have the target of achieving an RPO of 1h and an RTO of 12h.	Noted
6.31	Is the service available 24x7 or are there downtime periods for maintenance?	Yes, there is no downtime associated with maintenance windows.	Noted
6.32	Is the customer made aware of maintenance periods in advance?	A banner on the logon page reminds users of any standard maintenance windows, and warns of any upcoming unscheduled outages.	Noted

Ref	Requirement	Response	Reviewer Comments
6.33	Does the application software:- - Require any client software to be installed on the user's computer? - Work entirely within Internet Browser software on the user's computer?	No software needs to be installed. Our architecture is built on open standards. We offer Software as a Service (SaaS) which is designed to work within an HTML compatible, JavaScript enabled web browser. We support Windows and Mac operating systems as well as the current version of most popular browsers, including Microsoft Edge, Mozilla Firefox, Apple Safari and Google Chrome. We strongly encourage the use of Google Chrome for the best user experience. There are no applets, downloads or java needed by the user's browser to access the solution. While we believe most browsers will work without issue, we certify the most commonly used browsers, with each release as part of our QA process. Please get the most up-to-date list of supported browser and O/S combinations from the following link: https://help.sap.com/docs/SAP_CONCUR/df18cecb4b6b4bbdbe30219c0c15a208/1b96d5cb6caf1014bb02d36f8dc4cb81.html	Noted
6.34	Where the product/service relies upon downloading and running an executable program, has that program been secured with a digital certificate to verify the source and integrity of the program?	N/A	Noted
6.35	Does the product/service currently use any technologies which are obsolescent / out of support / soon to be end of life? If so, describe how the user can mitigate this risk.	As of now, SAP Concur does not rely on any technologies that are obsolete, out of support, or nearing end-of-life for its production services.	Noted
Platform security			
6.36	What security steps are taken to prevent and detect intrusion attempts?	Our network architecture ensures that sensitive client data is protected through best business practice security policies and procedures. Network security encompasses needs-based access, proper network segmentation, and Security and Risk Management oversight. <ul style="list-style-type: none">Secure Internal Administration Network: We employ a complete internal infrastructure to backup and monitor servers through secure connections. All web servers contain at least two Network Interface Cards (NICs). One NIC is connected to the production environment, and the other is connected to our Operations internal private network. The IP addresses of these servers are protected from third parties through our non-routable network.Hardened Router Configurations: Router configurations are used to correctly route packets to their proper destinations, and to restrict traffic. Access Control Lists (ACLs) on the front-end routers are used to stop common attacks that could affect the environment, including IP spoofing and limited denial-of-service attacks.Network Segmentation: Our multi-segmented network architecture prevents direct public contact or connection to our private network segment. This ensures client information is not accessible directly from the Internet. We utilize intrusion detection systems that monitor all TCP/IP incoming and outgoing traffic between network segments.Front-end Load Balancers: Access to our services is managed with redundant load balancers. The load balancers provide a variety of functions including session termination, load balancing, network address translation (NAT), and port address translation (PAT). Distributed Denial of Service (DDoS) protection: All of our service locations are protected by a solution that protects the availability of our services even when under a distributed denial of service (DDoS) attack.	Noted
6.36 cont.		<ul style="list-style-type: none">Activity Log Aggregation: Log activities from network devices and systems are aggregated through an activity log collection system. Alarms are generated for those events that warrant immediate attention.Proactive Monitoring: Security and Risk Management continuously monitors industry communities for news of security alerts, as well as vendor and partner security changes that may affect Information Services and our product line. Information Services has 24/7 automated monitoring with backup personnel.Intrusion Detection Systems: Intrusion Detection System (IDS) technology is an integral component of our comprehensive enterprise security strategy. The IDS alerts us of suspicious IP traffic or log activity that occurs on our systems and networks. Where possible, isolated IDS servers bear the security audit load, reducing overall consumption of resources within the application servers to zero levels.Active Vulnerability Assessment: Our Security Engineers perform infrastructure security scans on a regular basis using an approved PCI scanning vendor from the Internet as well as from internal scanning appliances. Discovered vulnerabilities are managed through our remediation process in accordance with industry best practices.Web Application Firewalls: Front-end web application firewalls protect our services by blocking traffic that could represent attempts to steal application data or break in to our web applications. These firewalls are highly distributed & monitored.Multiple Firewall Layers: We utilize multiple layers of firewalls that protect applications and client databases. Application firewalls permit traffic only from web servers to reach application servers, and database firewalls permit database queries only from application servers.	
6.36 cont.		<ul style="list-style-type: none">VPN: Our Operations personnel use VPN when connecting and transmitting from outside the trusted network. This VPN secure tunnel offers internal Operations personnel highly secure remote connectivity to perform after-hours maintenance or troubleshooting. Multi-factor authentication is required for all or our personnel with access to systems containing customer data.Data Protection: All networks, systems, databases, and applications that contain customer data are managed by full time employees within a Tier 4 datacenter. Access to customer data is granted on a least-privilege, need-to-know basis.Digital Certificates and SSL: Our services utilize web server digital certificates to verify the authenticity of all client sites. Digital certificates are used to encrypt all Internet web traffic between clients and servers. Our services utilize TLS 1.2 or higher to ensure that HTTP communication between our clients and our servers is encrypted.	
6.37	Is firewall hardware and software used to protect the live systems from unauthorised access?	Multiple Firewall Layers: We utilize multiple layers of firewalls that protect applications and client databases. Application firewalls permit traffic only from web servers to reach application servers, and database firewalls permit database queries only from application servers.	Noted

Ref	Requirement	Response	Reviewer Comments
6.38	Which monitoring software is used to create alerts when intrusion attempts are suspected?	Intrusion Detection Systems: Intrusion Detection System (IDS) technology is an integral component of our comprehensive enterprise security strategy. The IDS alerts us of suspicious IP traffic or log activity that occurs on our systems and networks. Where possible, isolated IDS servers bear the security audit load, reducing overall consumption of resources within the application servers to zero levels.	Noted
6.39	Are designated staff responsible for receiving and urgently responding to these alerts?	Yes, Security and Risk Management continuously monitors industry communities for news of security alerts, as well as vendor and partner security changes that may affect Information Services and our product line. Information Services has 24/7 automated monitoring with backup personnel.	Noted
6.40	Have clear procedures been established for identifying and responding to security incidents?	Yes, as an SAP company, incident management is provided and coordinated by our parent corporation, in conjunction with SAP Concur security. SAP Concur has adopted incident management best practices as prescribed by the Carnegie Mellon (CERT) Computer Emergency Response Team and by the SANS Institute. Both are recognized authorities in information security throughout the world. Incident Management is divided into three disciplines: Proactive Services, Responsive Services, and Quality Management Services. We maintain detailed procedures covering all three disciplines. These activities are audited by ISO 27001 auditors.	Noted
6.41	Is all security sensitive software, such as operating systems and databases, kept up to date with the latest software patches? Please indicate how regularly updates are applied.	Yes, Maintenance/updates conducted monthly to ensure the system is up to date and patches are in place to address any deficiencies. SAP Concur has a systematic patch management schedule to apply critical patches and security updates, ensuring that systems remain secure and resilient against vulnerabilities.	Noted
6.42	List the procedures and software tools in place to prevent or detect and eliminate interference from malicious code, such as viruses?	Centrally managed antivirus solutions are deployed and hourly signature update checks are in place. Our solution utilizes multiple virus protection software from multiple vendors on all servers and workstations. Malicious code protection is a part of the PCI DSS 1.2 requirements on which SAP Concur is audited and certified. Hosting Operations environments utilize virus scanning agents on the majority of systems within the environment. These systems centrally report viral infection alerts to Engineering and InfoSec. Secondary infection detection mechanisms exist within the firewall and Intrusion Detection System signatures and alerting mechanisms. Our Security Team continuously monitors industry communities for news of security alerts, as well as vendor and partner security changes that may affect us. Our Operations has 24/7 automated monitoring with backup personnel. All possible external security threats are thoroughly investigated and immediate steps to resolution and containment are taken. Detailed security logs are maintained, and data is used for heuristic research. The returned data is analysed and incorporated into new (rules) for violation recognition.	Noted
6.43	Is a system log maintained by the service provider that details - User access? - User activity? - Error messages? - Security violations?	Yes	Noted
6.44	Is this log available to the customer?	Clients have full access to transactions logs. Our personnel have access to server and infrastructure application logs only. Clients are able to use Intelligence to view their own transactions logging. SAP Concur provides two types of logging at the application level: change logging and access logging. Customers can access these logs to monitor various activities. If more detailed information is needed, such as a report of who logged in between specific dates, customers can contact the support team. While some information might not be directly available in the admin console, all application-level logging is accessible to customers. Additionally, SAP Concur manages 24/7 security monitoring and response teams, with alerts and triggers set up to ensure continuous oversight. All these measures are in place as part of the contractual agreement.	Noted
6.45	Have there been any successful unauthorised access attempts been made during the last year? If Yes:- - What was the effect on the business and users? - What steps are in place to prevent this happening again?	No.	Noted
6.46	Is penetration testing regularly carried out by (please indicate frequency of tests): - Staff specialising in this field? - External specialists?	At least annually, a third party performs a network and application penetration tests. Findings identified in the network penetration tests are submitted for remediation.	Noted
6.47	Are procedures in place to ensure that any weaknesses found by penetration testing are addressed quickly?	Findings identified in the network penetration tests are submitted for remediation.	Noted
6.48	If penetration testing by a specialist is not performed regularly, please indicate the main procedures in place to identify weaknesses?	N/A	Noted
6.49	Are security procedures regularly reviewed? Please indicate frequency of reviews.	SAP's Global Security Policy is on a continuous review cycle and outlines the mandatory security requirements for all SAP operations. This policy ensures that SAP provides a secure environment for our people, information, and assets, as well as those entrusted to SAP by our customers. This policy is owned by SAP Chief Security Officers.	Noted

Ref	Requirement	Response	Reviewer Comments
6.50	What security reporting is provided demonstrating compliance against certification(s) and policy(ies)?	<ul style="list-style-type: none"> • SOC 2 Type II report https://www.sap.com/about/trust-center/certification-compliance/sap-concur-soc-2-2024-h1.html • SAP Concur SOC 2 Bridge Letter Package https://www.sap.com/about/trust-center/certification-compliance/sap-concur-soc-2-isae3000-bridge-letter-latest.html • SOC 1 report https://www.sap.com/about/trust-center/certification-compliance/sap-concur-soc-1-2024-h1.html • SAP Concur SOC 1 Bridge Letter Package https://www.sap.com/about/trust-center/certification-compliance/sap-concur-soc-1-isae3402-bridge-letter-latest.html • ISO 27001 https://www.sap.com/about/trust-center/certification-compliance/compliance-finder.html?search=Concur ISO 27001&sort=latest_desc&pdf-asset=42edaa99-c17e-0010-bca6-c68f7e60039b&page=1 • ISO27018 https://www.sap.com/about/trust-center/certification-compliance/compliance-finder.html?search=concur&sort=latest_desc&pdf-asset=8a82aa99-c17e-0010-bca6-c68f7e60039b&page=1 • ISO27017 https://www.sap.com/about/trust-center/certification-compliance/compliance-finder.html?search=concur&sort=latest_desc&pdf-asset=02b0aa99-c17e-0010-bca6-c68f7e60039b&page=1 • ISO22301 https://www.sap.com/about/trust-center/certification-compliance/compliance-finder.html?search=concur&sort=latest_desc&pdf-asset=4e4aab99-c17e-0010-bca6-c68f7e60039b&page=1 	Noted
6.51	How are security breaches communicated to customers?	We maintain security incident management policies and procedures, including detailed security incident escalation procedures. SAP Concur will notify the Customer as soon as reasonably possible with its confirmation of a security breach of the Service that results in a compromise of the confidentiality and/or integrity of Customer Data. SAP will notify customer without undue delay after becoming aware of any Personal Data Breach and provide reasonable information in its possession to assist Customer in meeting Customer's obligations to report a Personal Data Breach as required under Data Protection Law. More information can be found within the SAP Data Processing Agreement that can be found in the SAP Trust Center.	Noted
Backups by the service provider			
6.52	In relation to backups undertaken by the system provider please explain: - How is a customer's data backed up? - How often is this undertaken? - What is backed up? - What's the media used? - Where are backups stored? - How many copies are there? - How long are they retained for? - Who has access to them? - Is the data encrypted?	<p>Our solution maintains a formal backup policy and process. Backup and restore methodologies are covered under SOC 1 and ISO 27001 audits. We are ISO 22301 compliant. Backup media is AES-256 encrypted.</p> <p>Our solution uses ExaGrid's replication capabilities to back up from our main site in Germany to our EMEA warm site in Ireland.</p> <p>In general, our most critical data (databases or their transaction logs) are backed up on a daily basis.</p> <p>Less critical data may be backed up on a weekly basis or a custom schedule of multiple selected days of the week or month.</p> <p>They are replicated online from our main DC in Germany using our VPN connection to our warm site in Ireland.</p> <p>Client Databases</p> <ul style="list-style-type: none"> • Most recent backups available on nearline storage • Two-Month Availability Window <p>Windows Domain Controllers</p> <ul style="list-style-type: none"> • Backup three times per week, One-Week Availability Window <p>File Servers</p> <ul style="list-style-type: none"> • Backup Each Week (Full) with three-week retention • Backup Each Day (Incremental), one-week Availability Window <p>UNIX Infrastructure Systems (SMTP, DNS, Syslog, PGP)</p> <ul style="list-style-type: none"> • Backup Twice a Week • Two Month Availability Window <p>We do not use any offsite tape media. Offsite backup is via disk replication to the disaster recovery location.</p>	Noted
6.53	How frequently is a test-restore of backups undertaken?	<p>SAP has a formal system backup process and schedule for the SAP Cloud solutions, which includes hardware independent restore and recovery capabilities.</p> <p>Backups are run automatically; their respective frequency depends on system availability requirements. The restore of data can be requested via ticket and needs approval before being executed. Appropriate processes and automated tools are in place to validate backup integrity and backup logs are reviewed daily to detect and correct backup failures.</p> <p>Backups are stored in data center locations on redundant media in the designated region. Retention of data applies to backup data as well.</p>	Noted
6.54	Can the provider restore from a backups that it has taken at a customer request?	see above	Noted
6.55	Does a customer have the ability to undertake their own backups?	<p>No. As a cloud-based SaaS solution, all data backups are managed by SAP Concur as part of the platform's standard operations.</p> <p>SAP Concur performs regular, automated backups to ensure data integrity and disaster recovery capabilities. These backups are stored in secure, redundant environments, aligned with ISO 22301 and other relevant certifications.</p> <p>If needed, customers can extract data via standard reports, custom reports, or APIs to retain their own copies for archival or integration purposes.</p>	Noted - this is not unusual for a SaaS product
6.56	If so, can a customer restore data a backup that they have taken?	N/A	Noted

Ref	Requirement	Response	Reviewer Comments
Platform recovery			
6.57	What contingency plans are in place to enable a quick recovery from: - Database or application software corruption? - Hardware failure or theft? - Fire, flood and other disasters? - Communication failures?	SAP Concur is hosted in Amazon Web Services (AWS), with contingency plans in place for: Data corruption: Regular backups enable quick restoration. Hardware failure/theft: AWS provides built-in redundancy and secure infrastructure. Disasters (fire, flood, etc.): AWS facilities have strong physical and environmental protections. Communication failures: Redundant network paths ensure stable access. These measures are aligned with ISO 22301 and regularly tested to ensure rapid recovery.	Noted
6.58	How often are these plans tested?	Yearly	Noted
6.59	How often are these plans reviewed and updated?	Cloud disaster recovery plans are documented and updated by the Disaster Recovery Facilitator at least every 12 months. The current version of the plan is made available to all critical personnel identified in the plan.	Noted
6.60	What is the longest period of time envisaged that service may not be available?	Our DRP provides Recovery Point Objective (RPO) target of 1 hours and Recovery Time Objective (RTO) target of 12 hours. These are non contractual but internal targets. Data is backed up using enterprise-level client-server software tools such as Veritas NetBackup, Zmanda, and SQL Server. Specified data is copied from the client to the server, where it may be written to disk-based appliances, or copied to a remote location. The catalogue from each backup server is protected periodically through replication, copying to a file share, or other acceptable method. Backup jobs that are managed through a central backup server are grouped in policies that match similar characteristics such as client operating system, data type, retention period, and frequency of backup. These policies can be found in the backup server management interface. Online - Internal hard disk, direct-attached disk array, network-attached storage, SAN attached. Convenient, speedy, expensive, vulnerable to deletion, overwriting & viruses. Offline - Requires human action to access. Mostly immune to online backup failures. Access time depends on personnel availability and whether the media is on or offsite. Offsite - Media that is stored in a location distant from where the live data is stored; typically, a third-party vault, but could be a remote office. This can be the best protected copy of the data but may take the longest to recover since it must be physically transported back to the datacenter. Backup Site or DR Site - Entire duplicate environment in case of facility loss. Recovery times depend on many factors. Usually includes continuous data protection and virtual server resources for faster recovery. This location is often hundreds of miles away.	Noted
6.61	What are your: - Recovery Point Object (RPO) standards? - Recovery Time Objective (RTO) minimum standards?	Contractually we provide a monthly system availability SLA of 99.7% with corresponding service credits. There is no contractual agreement about RTO and RPO. However, as an internal goal and for our ISO22301, we have the target of achieving an RPO of 1h and an RTO of 12h. “System Availability SLA” means a 99.7% System Availability Percentage during each Month for the production version of the Cloud Service.	Noted
6.62	If transaction records are dated and time stamped are the times used local to the user or based on where the server is located?	Transaction records in SAP Concur are timestamped based on the server's time zone (usually UTC or the data center's local time). The time zone used is typically consistent across all users for consistency and reliability. However, user-facing timestamps may be displayed in the user's local time zone for convenience, depending on their settings and preferences.	Noted
6.63	What protection is in place to enable users to able to access their accounting and other data if the service provider should experience serious difficulties, cease trading or decide to stop providing the service?	SAP Concur is part of SAP, a financially stable and globally recognized provider. In the unlikely event of service disruption or discontinuation, customers can extract their data via standard reports, custom reports, or APIs. Data ownership remains with the customer, and SAP Concur provides options for data export during offboarding or contract termination, ensuring continued access to accounting and other records.	Noted
6.64	Do these arrangements include: - Standby arrangements for another organisation to continue providing the full service? - Minimal arrangements to at least enable customers to access their data for a sufficient period of time to extract data copies, produce reports and make alternative arrangements?	see above	Noted
6.65	If the system is hosted are there arrangements in place for this third party to continue providing a hosting service in the short term to allow time for customers to negotiate their own arrangements? If so, how long does the arrangement allow?	While there is no formal arrangement for AWS to continue hosting independently of SAP, customers would be given a transition period as part of standard contract offboarding to retrieve their data and make alternative arrangements. Specific timelines would be communicated based on the situation.	Noted
6.66	Are there any individual members of the vendor's staff whose leaving or illness would significantly reduce, or even stop, the service provider's ability to provide a full and reliable service to customers?	No, SAP Concur does not rely on any single individual to deliver its services. The organization has well-established processes, team structures, and knowledge-sharing practices to ensure service continuity regardless of individual staff availability. Roles are distributed across redundant global support and operations teams, minimizing any risk of service disruption due to personnel changes.	Noted
Platform change management			
6.67	Describe your approach to upgrades including what option customers have not to take upgrades (if any)?	Our solutions are delivered on-demand using a true SaaS architecture. Our solution is a single build of the solution that is automatically updated on a monthly basis to the latest build at no additional cost to customers. We maintain the current code line and infrastructure, and updates the service monthly with added functionality and bug fixes. There are no client resources required. As new functionality is introduced, it is delivered as opt-in basis. Release schedules are provided to clients in advance. Customers are able to decide whether to implement new functionality at a time that is most convenient for the customer. This ensures that clients are on the latest code line, while giving individual customers control over their unique configuration. We manage the development, QA, testing, and roll out of all builds of the service following our SOC 1, Type II audit change management processes.	Noted

Ref	Requirement	Response	Reviewer Comments
6.68	Are users able to test the application before new versions go into live use?	see 6.67	Noted
6.69	Are users given notice before application changes are applied to the live system?	see 6.67	Noted
6.70	Are changes delivered into the live environment "switched off" to enable users to test them before enabling them for their environment?	see 6.67	Noted
6.71	Describe what testing and QA processes are undertaken before upgrades and other changes are made live/available to customers?	<p>Quality Assurance - R&D has established a centralized QE (Quality Engineering) organization focused on delivering quality services to our clients. The QE organization is responsible for validation, packaging and delivery of all software updates to the service. The group has been organized into teams focused on validating Concur services on a release over release basis.</p> <p>QE Operations Team - QE ops are responsible for implementing the systems required to manage, maintain and deliver service updates to operations. A series of systems, controls and processes have been established and monitored by the team. An audit of these controls is performed on a quarterly basis.</p> <p>Integrated Test Environments - A series of integrated test environments have been created to validate all services. Code changes are promoted from BAT, to RQA and HQA environments based on a series of validations steps.</p> <p>Any issues identified during validation need to be resolved prior to be promoted.</p> <ul style="list-style-type: none"> • Unit Test Environment - A Continuous Integration unit test environment has been implemented to ensure all code check-ins pass an automated validation suite of tests prior to building and deploying to test environments. Developers are notified of issues and are required to fix them prior to building the code. • BAT Environment - All code changes are deployed in the Build Acceptance Test environments and an automated set of tests are executed prior to promotion to the RQA and HQA environments. • RQA Environments - Development environments allow testers to execute functional, integration and end 2 end validations against our integrated offerings. • HQA Environments - Staging environments that allow QE to validate scrubbed client entities, configurations and data. 	Noted
6.71 cont.		<ul style="list-style-type: none"> • QE Feature Teams - The QE Feature teams have been established for each of the services we deliver. The QE teams are involved from requirements gathering through the delivery to operations. They are responsible for building test plans, scenarios and test cases and client validation scenarios to validate each of the services. Test cases and scenarios are executed against the RQA and HQA environments, issues are identified and logged in Jira throughout the SDLC. QE is responsible for tracking issues and ensuring that All issues are resolved prior to delivery to production. • Planning - QE is involved in gathering and vetting of requirements. • Development - QE is responsible for building Feature Test Plans, Test Cases and scenarios to validate that the service works as specified. All Test Cases and Scenarios are reviewed by the cross-functional teams and are stored within HP Quality Center, our test case management tool. • Validation - QE is responsible for executing test cases and scenarios, logging defects and issues, and driving to resolve all issues prior to release. • Release - QE is responsible for regression and sign-off of changes to their respective services. <p>QE Automation Team - The QE Automation team is responsible for building automation frameworks/tools to allow us to deliver consistent and repeatable validation of the Concur family of services. Over 65,000 total validations are run per monthly release.</p> <ul style="list-style-type: none"> • Unit Test - Build time automation scripts are kicked off with every check-in to validate that the build has not been broken. Defects are logged and fixed prior to updating systems with the identified code changes. • Deployment Validation - BAT/BVT Build Acceptance Test-suite and Build Validation Test-Suites have been established • Integration Validation - A series of integration validations are performed with every deployment to ensure unintended changes do not get introduced. 	
6.71 cont.		<ul style="list-style-type: none"> • E2E - The QE team works with clients to build a series of automated tests to validate key features and functionality, within a scrubbed copy of their entity. End 2 End tests are run multiple times per release and results are published to clients. All defects are logged in Jira and fixed prior to release. 	
6.72	Explain the release management procedures in place and the associated segregation of duties?	SAP has defined a Framework for Secure Development as part of the SAP Global Development Policy. The SAP Global Development Policy defines for secure development a mandatory secure Software Development Lifecycle (secure SDL) as well as a Product Standard Security. The secure SDL defines minimum and risk-based controls to help ensure that product plan, implement and test security controls are in place to achieve a risk-adequate security level for each product. An important part of the secure SDL is the risk assessment that identifies and classifies security risks as a pre-requisite to proper risk response planning. The Product Standard Security enhanced by Secure Development Guides serves as a threat Library for the risk assessment, security knowledge base as well as guidance for developers on how to write secure code.	Noted
6.73	Are users informed when they next login of the application changes that have gone into live use?	Yes, users are informed of key application changes through in-app notifications, release notes, and messages on the login page when relevant. SAP Concur also provides quarterly release updates.	Noted
6.74	Do customer staff have to take any action (e.g. regression testing) when new editions, patches or upgrades are released? If so, please describe what they should ordinarily do.	No customer action is typically required when SAP Concur releases updates, as upgrades are automatically applied and fully tested by SAP before release.	Noted
Subscription options			
6.75	What is the minimum level of commitment must the customer sign up to, e.g. 36 months?	12months	Noted
6.76	Where online payment is used, what type of security is used to protect sensitive information?	All customers receive an invoice for the services provided. We have recently introduced an Autopay service that allows customers to pay via their credit card. Credit Card security would be applicable in these scenarios.	Noted

Ref	Requirement	Response	Reviewer Comments
6.77	Where online subscription / payment is used, is an invoice provided to the customer and, if so, in what format?	Yes- Customer Invoices are provided in a pdf format	Noted
6.78	When subscriptions need to be renewed, what advance notice is provided and what is the time limit for renewal?	<p>Clients have the option to sign up for a 12, 24, or 36-month period. Once this term concludes, they transition to a rolling contract automatically. At that point, the notice period for modifying or discontinuing services is adjusted to 90 days.</p> <p>Clients can consult with their Concur representatives to explore the possibility of returning to a fixed-term contract.</p>	Noted
6.79	Is there a procedure for late renewal and is there a time limit after which subscriptions cannot be renewed?	No, contracts, even when elapsed, will continue to be evergreen.	Noted
6.80	How soon after creating or renewing a subscription (if applicable) can the system / service be used?	<p>Setting up a new instance requires going through the implementation process, which can vary based on services, timeframes, and any additional projects.</p> <p>Renewing a term or subscription does not disrupt the service, ensuring continued access.</p>	Noted
6.81	What notifications / confirmations are provided to the customer regarding subscriptions and payments?	In addition to the signed Order Form, Invoices detailing costs are provided to customers monthly. If a customer has unpaid bills, our billing team will regularly notify them until the payment is made or the dunning process begins.	Noted
6.82	<p>To what extent are users able to access their accounting and other data if:</p> <ul style="list-style-type: none"> - They miss one or two payments? - They cease being customers? 	Clients are not restricted access to their data if they miss one or two payments. If a client terminates then the client's data is provided to them in a file format.	Noted
6.83	At the end of the contract term, how long does a customer have to obtain a copy of their data from you?	At the end of the contract term, Customers may extend the Subscription Term for up to ninety (90) days by notifying us at least (30) days prior to the effective date of termination or expiration and paying subscription fees for such extension period. During this 90-day period, customers will be able to download their data. Export data is a pipe delimited flat file. We have also implemented Web Services utilizing XML/HTTP for integrating real time.	Noted
6.84	At the end of the contract term, how is a customer's data destroyed (if appropriate) and will that destruction be certified?	At the end of the Agreement, Customer hereby instructs SAP to delete the Personal Data remaining with SAP (if any) within a reasonable time period in line with Data Protection Law (not to exceed 6 months), unless applicable law requires retention. Should the Customer require a certificate of deletion, the account manager for the Customer must submit the request to the "certificate of deletion" intake. The team will validate the deletion and provide a certificate.	Noted
6.85	What is your processes regarding disposal of end-of-life and failed hardware devices that were used to operate your service?	Media storage devices used to store customer data are classified by AWS as Critical and treated accordingly, as high impact, throughout their life cycles. AWS has exacting standards on how to install, service, and eventually destroy the devices when they are no longer useful. When a storage device has reached the end of its useful life, AWS decommissions media using techniques detailed in NIST 800-88. Media that stored customer data is not removed from AWS control until it has been securely decommissioned.	Noted
SaaS/Hosted Reporting			
6.86	Are reports produced from the same software as the financial applications or is separate reporting software used?	SAP Concur has an inbuilt reporting solution using Cognos technology.	Noted
6.87	Does any application software (i.e. other than a web browser or PDF reader) need to be installed on the user's computer in order to prepare or view the reports?	As we are a SAAS provider nothing needs to be installed on the user's computer.	Noted
6.88	<p>What browser versions are support:</p> <ul style="list-style-type: none"> - On desktop/laptop (PC, Mac, Linux)? - On Tablets? - On mobiles? 	<p>Our architecture is built on open standards. We offer Software as a Service (SaaS) which is designed to work within an HTML compatible, JavaScript enabled web browser. We support Windows and Mac operating systems as well as the current version of most popular browsers, including Microsoft Edge, Mozilla Firefox, Apple Safari and Google Chrome. We strongly encourage the use of Google Chrome for the best user experience. There are no applets, downloads or java needed by the user's browser to access the solution.</p> <p>While we believe most browsers will work without issue, we certify the most commonly used browsers, with each release as part of our QA process.</p> <p>Please get the most up-to-date list of supported browser and O/S combinations from the following link: https://help.sap.com/docs/SAP_CONCUR/df18cecb4b6b4bbdbe30219c0c15a208/1b96d5cb6caf1014bb02d36f8dc4cb81.html</p>	Noted
6.89	Is access to the reporting facilities and data controlled by the same procedures as access to the main application?	Yes. Access to reporting is role based access control at a user level.	Noted
6.90	If it's different, explain the user access control facilities available to ensure information is only viewed by users with appropriate authority?	NA, see above.	N/A
6.91	<p>In what electronic formats are reports produced:-</p> <ul style="list-style-type: none"> - PDF? - XML? - MS Excel spreadsheet? - CSV file? - As html for viewing in a web browser? - Other, please specify? 	Reports can be generated and downloaded into HTML, PDF, XLS, CSV and XML.	Noted
6.92	<p>Are report documents stored on the web server or on the user's computer?</p> <p>If stored on the web server, are they secure to ensure only users with appropriate authority can get access?</p>	<p>Report documents in SAP Concur are typically stored on the web server rather than on the user's computer. This centralized storage approach ensures that documents are accessible from any device with internet access, providing convenience and consistency.</p> <p>To ensure security, SAP Concur implements several measures:</p> <p>Access Control: Only users with the appropriate permissions can access specific documents.</p> <p>Encryption: Data is encrypted both in transit and at rest to protect it from unauthorized access.</p> <p>Compliance: The system adheres to various security standards and regulations, such as GDPR and SOC 2.</p> <p>Monitoring and Auditing: Regular monitoring and auditing help detect and respond to any unauthorized access attempts.</p>	Noted

Ref	Requirement	Response	Reviewer Comments
6.93	For documents viewable in a browser is any data stored on the user's computer in a web browser cache or temporary file? If Yes: - Is there any protection against other users viewing the report or data on which it is based? - Is it clear on the reports when they were produced and the date of the data on which they are based, so the user can tell whether they are viewing out of date information?	Yes, some data may be temporarily stored in the web browser's cache or temporary files when viewing documents in a browser. However: Protection: Data is secured through browser security protocols (e.g., HTTPS) and users are encouraged to clear their cache regularly. Access to reports is protected by authentication and user permissions. Date and versioning: Reports display clear timestamps indicating when they were produced and the date of the underlying data, ensuring users can verify if they are viewing up-to-date information.	Noted
6.94	Are communications between the browser and the server encrypted for any report related communications?	For data in motion, all application access is encrypted-in-transit over HTTPS using (TLS) Transport Layer Security (TLS) 1.2 by default. We support SFTP for file exchange of PGP encrypted files. For data at rest, we support AES-256 with split keys for encryption of credit card numbers, passport number and banking information. Passwords are one-way hashed with SHA-2. Backup media are encrypted with AES-256. All outgoing e-mail notifications sent from the system are securely encrypted using TLS.	Noted
6.95	If reports are produced dynamically each time the user views them can historical reports be reproduced at any time?	If an employee has the correct permissions to create a report then historic reports can be created and run.	Noted
6.96	Can reports viewable in a browser be navigated dynamically by users? For example: - Enabling drill down to more detailed information? - Altering which columns and rows of data are displayed. - Choosing time periods? - Specifying selection criteria?	Yes, reports are able to be drilled down to more detailed information.	Noted
6.97	Can report data be reliably copied and pasted direct from browser viewable reports to an MS Excel spreadsheet retaining any table layout?	N/A, report data can be exported in a variety of formats, including csv.	N/A
6.98	If reports are incomplete, for instance due to a poor Internet connection, is sufficient information provided to enable the user to notice that some of the report is missing?	No this is not supported. If poor internet interrupts the running of a report the report will fail; it won't present half the data of the report.	Noted

Ref	Requirement	Response	Reviewer Comments
7.	<u>EXPENSE MANAGEMENT</u>	SAP Concur consists of three main products, namely: Expense, Travel and Invoice. For this accreditation only Expense is being reviewed - all comments below are only representative of Expense functionality.	
System overview			
7.01	What are the high level process steps required when a client implements the software?	<p>c.80% of a customer's site is able to be self-activated using self-guided tools, on-demand chat in product, instructional how-to videos for setup, and self-guided rollout resources. Customers will also have access to a delivery coach via phone, email, and chat, and integration specialist (if required).</p> <p>Clients implement the software through the following steps:</p> <p>(1) Customers receive log in credentials. The customer will use the Activation Wizard to gather and self-enter in requirements. Various levels of support help assist with setup are available via chat, phone, or email. Once completed, Activation Teams review together to set up and train on the services purchased.</p> <p>(2) Customers will activate add-on services, validate any financial systems postings, review admin training tools and resources, develop their deployment plan, and do a site validation review.</p> <p>(3) Customers are now ready to deploy their site to end users. Concur recommends leveraging the customer's power user or validation users to help train end users.</p> <p>A detailed guide is available to customers to utilise.</p>	Noted the overarching process, and confirmed / viewed the supporting activation guide
7.02	What is the high level process flow for the expense tool and what are the key user access roles?	End users ("employees") are able to create expenses and add these to claims for reimbursement. The standard workflow is an employee raises a claim, an "approver" approves (approver logic can be based on defined line managers, project managers for specific codes etc.), followed by "finance" approval and processing. There is also an administrator role (limited to 1-2 users per client) who is able to amend configuration such as expense types, mandatory fields, alerting, user access, VAT rates, etc.	Confirmed
Workflow - raising and managing claims		The employee view demo was conducted on a mobile app. Therefore, all findings and review comments reflect the mobile functionality and not the web version. While it is understood that there are minimal differences between the web and mobile versions, it is important to note that the web version has not been reviewed.	
7.03	How does a user create an expense claim?	Users can create an expense claim either through the web application or mobile application.	Confirmed
7.04	What information is required when creating an expense claim?	This can vary depending on the client set up. A name for that expense claim is always required, but further fields could include selecting specific claim months, client / internal codes to charge the claim to (although this can also be pre-filled based on the employee's cost centre information within the business).	Noted - this was verbally explained throughout the demo however not sighted.
7.05	How are expenses captured ?	<p>Out of pocket expenses can be raised either manually through creating a manual expense, or through scanning and uploading a receipt. Expenses can also automatically be created through a linked company card account.</p> <p>Manual expense</p> <p>The user can select from a list of expenses (which can be modified for specific client instances of Concur) and manually key in the required fields. Most expense types will require a receipt which will require attaching.</p> <p>Receipt upload & OCR technology</p> <p>Using OCR (optical character recognition) technology, the receipt is scanned by the software which will capture the key information. This can be manually uploaded or sent via email to a dedicated inbox. Machine learning within the tool suggests an expense type based on details on the receipt (e.g. location, time, individual cost items). The user (employee) has the opportunity to review the information captured and change it if incorrect.</p> <p>Manual and receipt upload Expenses can be raised within the home screen of the application, and then moved to a claim, or these can be directly created within a claim.</p> <p>Corporate cards</p> <p>Charges raised on linked company cards will appear in the users expense list. Using ML technology, Concur will again attempt to identify an expense type based on the vendor, time and amount. The user (employee) has the opportunity to review the information captured and change it if incorrect, and attach a receipt as necessary. This can then be moved to an open claim.</p>	Confirmed - manual expense entry and receipt upload. Not witnessed sending via email, e-receipts or company card transactions.
7.05 cont.		<p>E-receipts</p> <p>E-receipts are electronic receipt images sent to SAP Concur directly from the vendor. They help eliminate paper receipts and make it easier for customers to complete customers' expense reports. SAP Concur has built relationships with hundreds of Airlines, Hotel brands, Rental car and ground transportation companies to simplify customers' Travel and Expense experience.</p>	

7.06	How are expenses relating to multiple client codes treated?	<p>Allocations can be done on a per claim or per expense basis.</p> <p>When creating a claim users can allocate expenses to specific cost centres or client codes when creating an expense report. Users can use the allocation form to distribute an expense across different business entities, such as departments, cost centres, projects, or client codes. This is useful for splitting costs between multiple entities.</p> <p>Users select the expense item they want to allocate. They then choose the 'Allocate' option and specify the percentage or amount to be allocated to each cost centre or client code.</p> <p>Users can add multiple allocations for a single expense item, ensuring precise distribution.</p>	Noted
7.07	How are alerts used throughout the software?	<p>Alerts are used to draw the employees attention to anything that needs to be completed based on the predefined requirements before the claim can be submitted. These often reduce the 'chasing' that finance and admin users have to do at the approval stages. Alerts include Amber (soft stop) - will allow claim to be submitted for approval however alert has been triggered Red (hard stop) - will not allow claims to be submitted without addressing the alert action.</p> <p>There are different type of alert rules, often the client / customer will define their policy rules which is in line with their relevant expense policy. This rules are configured within the implementation stage.</p> <p>Example alerts include: <i>This entry requires attendees other than yourself.</i> <i>This exceeds the £40 limit for dinner, please reduce the value of the expense to submit.</i> <i>Missing required field(s): Meals Type.</i> <i>Missing required field(s): Business Purpose.</i> <i>Expense is over the policy limit set by your company. Please leave a comment for your manager before submitting.</i></p>	Confirmed
7.08	Are there other technologies / methods used to help a user accurately capture their expenses?	<p>Yes - in relation to mileage capture, Concur has two options which support the accurate capture of mileage:</p> <p>Google Maps Integration (Included as standard functionality): Route Calculation (Google Maps): Google Maps can be integrated to calculate vehicle mileage based on the route taken. This can be configured to be either optional or mandatory for mileage calculation. For trips with multiple stops, Google Maps can calculate the total mileage, even if the stops are not in a straight line and allow the user adjust the route taken, identify if some of the mileage was personal (and not to be expensed) or whether it was a round trip.</p> <p>Concur Drive (GPS) - Additional Service not included as standard functionality Often used for companies where employees are doing multiple trips per day (i.e. real-estate agents etc.). This functionality tracks the GPS movements of vehicles and identifies the mileage of the trip. This is only possible for personal vehicles and not company vehicles. This can be configured through manual and automatic tracking. For manual tracking, employees manually start and stop tracking their journey through the app, whereas for automatic tracking allows the employee to set specific times when they regularly travel for business. During these times, the app uses GPS tracking and mobile sensors to measure the distance travelled automatically, without needing to be actively in the app. Once the tracking period is over, this will create a personal mileage expense item in the expense list which can be added to a claim where additional information can be added if required.</p>	Noted
7.09	How are expenses allocated to cost centres/ client codes? If claims need to be allocated to different cost centres / client codes. How is this done?	<p>Administrators can customise which cost centres are visible to an employee at the allocation level.</p> <p>From the user's perspective the user will go into the 'Allocate' section and be able to split the claim by amount or percentage to different cost centres/ client codes or project codes as required. This is then reflected in the data extract when this is transferred to the accounting system.</p>	Confirmed
7.10	How does a user manage their claims?	An employee is able to see all of their expense claims raised and saved, and Concur will categorise based on whether this has not been submitted, pending approval, pending accounting review, approved pending payment or sent for payment.	Confirmed
Workflow - approvals		Approver view demo was conducted on the website - mobile app version has not be sighted.	
7.11	What is the approval process flow following user submission?	<p>Within the home page on SAP Concur, an approver is able to view the list of claims that have been submitted and are pending approval (alongside viewing their own expenses and claims).</p> <p>The approver is asked to:</p> <ul style="list-style-type: none"> - Check the information provided, including receipts and any comments from the employee. - Verify that the receipts match the expense details, such as date, amount, vendor, and expense type. - Read any comments provided by the employee, especially for out-of-policy expenses. - Assess the justification for such expenses. <p>Approval Options: Approve: If the claim is accurate and compliant, click "Approve" to route it to the next stage in the process (e.g., finance processor queue). Send Back: If there are discrepancies or additional information is needed, send the claim back to the employee with a mandatory comment explaining the issue. Approve and Forward: If another approver needs to review the claim, use the "Approve and Forward" option to insert an additional ad hoc approver.</p>	Confirmed - approval of a claim was sighted. Other elements were not.

7.11 cont.		<p>Other elements to note:</p> <p>Amend Approved Amount: If necessary, amend the approved amount field. Other fields are locked and should be sent back to the employee for correction if needed.</p> <p>Delegate Approvers: If on annual leave or unavailable, ensure a delegate approver is set up to cover approvals.</p> <p>Escalation rules can be set to automatically escalate the claim to the manager's manager after a specified period (e.g., two or three working days).</p> <p>Dynamic Workflow: The approval workflow in Concur can be dynamic and flexible. Claims can be routed based on various criteria, such as client or project codes.</p> <p>Different line items within a claim can be routed to different approvers if coded to different clients or projects.</p> <p>The workflow of requiring line manager approval prior to finance approval is configurable and will depend on the clients requirements</p>	
7.12	What controls are in place to avoid self-approved expense claims?	<p>SAP Concur uses segregation of duties controls to reduce this risk. This includes:</p> <ul style="list-style-type: none"> - SAP Concur assigns distinct roles to users, each role has specific permissions and responsibilities. - Users cannot hold conflicting roles that would allow them to perform multiple stages of the expense claim process. - The system automatically prevents users from approving their own expense reports. If a user submits an expense report, it will be routed to another approver. - Delegates assigned to approve expenses cannot approve their own expense reports. <p>This ensures that even in cases of delegation, self-approval is not possible.</p>	Noted
Workflow - finance			
7.13	How are claims approved/processed by finance?	<p>Once a claim has been approved by an approver(s), they are then within "Accounting review" for final finance review. This stage is for the finance team to check against company policies and correct receipts uploaded (i.e. to drive VAT calculations). Finance users are able to amend data in the expense claim (unlike a standard approver), including nominal and cost centre codes if there has been a misallocation.</p> <p>Finance users can also sight the VAT breakdown for the claims to verify this amount.</p> <p>A finance user can approve the claim, send back to the approver or send back to the employee (which restarts the workflow). Once approved, that claim goes into a batch for processing to the accounting system. SAP Concur generates a standard accounting extract file containing all necessary information for the finance system. This file is essential for accurate financial reporting and reconciliation.</p> <p>Finance approval has to be done via the website - not via the mobile app</p>	Confirmed
7.14	What data are finance users able to view?	<p>Finance can view claims pending approval or already approved and therefore pending accounting review. They can also manage their own expenses and claims.</p> <p>Expense claims are summarised in a table with information including Name, Date, Employee Name, Approval Status, Claim Total, Payment Status, Executives, Receipt Image viability, Amount Due on Company Card, all of which can be filtered.</p> <p>The finance user can further query the data including:</p> <ul style="list-style-type: none"> Claims Ready for Processing Claims Review In Progress Claims Review In Progress By Me Claims Financial Posting Failed Approved 	Confirmed
Administration / configuration			
7.15	Are there differences between the mobile app and website functionality?	<p>The majority of "employee" and "approver" functionality is available on both the mobile app and website. Key differences include:</p> <ul style="list-style-type: none"> - Concur Drive only available on mobile app <p>The finance and administration view is only available on the website.</p> <p>Web: Full functionality, including detailed reporting, configuration, and policy management.</p> <p>Mobile: Streamlined functions like expense reporting, receipt capture, travel booking, and approvals.</p>	Noted
7.16	Can customers amend expense types, alerts, data fields, etc.?	<p>Yes:</p> <p>SAP Concur has a bank of pre-defined expense types but these can be amended by a user with administrator rights.</p> <p>Concur has a number of pre-defined alerts /audit rules (e.g. missing receipt) which can be turned on/off, but custom audit rules such as defining policy limits, soft vs hard stops, defining required fields can be added.</p> <p>Data fields for expense types are pre-defined for expense types, but additional fields can be added. Depending on whether the user takes out the standard or professional edition would drive whether these fields would be applied to all expense types (standard) or could be applied to specific expense types).</p>	Noted - the reviewer did not sight any custom or unique policy rules within the demo, however audit bot did explain that this does sometimes happen with particular clients.
7.17	Does the solution support other countries?	<p>Yes - Concur has a number of country packs which can be localised which updates to local language, their VAT rates, localized mileage rates, language, currencies, units used (e.g. mile vs km).</p>	Confirmed - sighted in the admin screen, not visualised as an employee using the system
7.18	How are different country limits / tax rates managed?	<p>Concur has a number of country packs which support clients globally, which includes the various tax rates against expense types for a number of countries globally, including special handling fields (e.g. parking on street vs off street has different VAT rates). These country packs can be modified and client created expense types can be assigned to the relevant VAT handling group.</p> <p>These are pre-configured and updated by Concur when changes to legislation takes place.</p>	Confirmed - sighted in the admin screen, not visualised as an employee using the system
7.19	Does Concur have tools to help identify fraudulent AI generated receipts?	<p>No - whilst the receipt audit service will provide an additional review as part of the process, this is not designed to specifically identify AI generated receipts.</p>	Noted

7.20	Does SAP Concur integrate with client's finance systems?	SAP Concur is 'finance system agnostic' meaning that it can integrate with any and all client accounting systems. Concur supports flat file import, SFTP, web services (REST APIs - note this requires an additional subscription) or pre-built connector (depending on the target system). (See questions 5.48 & 5.49).	Noted
Additional Services			
7.21	Are there additional products clients can procure to further enhance the product?	<p>Yes - there are many additional services that SAP Concur offers dependent on client requirements; Concur Drive which was mentioned above, Intelligence and Consultative Intelligence (see Q37) as well as the Receipt Audit Service.</p> <p>The receipt audit service is an additional step in the workflow, in between the employee and the approver. This service uses a mix of automated and manual checking (provided by Concur) to review the receipts uploaded against expense claims to ensure compliance and accuracy in expense reporting by validating receipts against submitted expenses. This service is unique to Concur and involves both AI and human auditors. Features include:</p> <ul style="list-style-type: none"> - Receipt substantiation: checks the data within the estate matches the expense claim (i.e. vendor, date, expense type, value etc.). This uses a mix of AI and human auditors. If any issues were identified, this would be returned to the employee to amend. - VAT capture: confirms the correct receipt type has been selected to ensure the correct amount of VAT is reclaimed by the client. This also verifies the VAT amount on the receipt to the calculation in the system. - Policy review: review against defined policies for a company (e.g. policy limits). This stage also reviews receipts to identify items which are not appropriate / able to be claimed against (e.g. personal items on a broader receipt). The audit service helps identify potential fraud by flagging suspicious or non-compliant receipts. <p>This service also reduces risks by catching discrepancies early in the process as opposed to being identified e.g. by the finance team at the final stage in the workflow.</p>	Noted