SAP Concur Trust Platform

SAP Concur® recognizes the importance of maintaining the confidentiality, integrity, and availability of our customers' information and the protection of its valuable business assets and applications. This Trust Platform reflects our commitment to providing a secure environment and adopting effective security standards that align with industry best practices in the areas of security and service management. With the use of a variety of reliable security technologies as well as a unique combination of trained personnel, mature business processes, and regular third-party audits measured against several international and U.S. standards, SAP Concur delivers a high level of security and confidence that is unmatched in the industry.

This document describes in some detail each layer of this assurance approach to provide an overview of the compliance, data protection, and cybersecurity that SAP Concur provides. While open to sharing information with its customers, SAP Concur asks companies and entities who are not yet SAP Concur customers to sign an SAP nondisclosure agreement before making detailed inquiries into SAP Concur services.

Compliance

For most companies, employee spending management activities (such as travel procurement, expense reporting, and invoice processing) are financially relevant business functions, meaning that SAP Concur's solutions become an extension of our customers' financial operations. To become and remain the employee spending management partner of choice, SAP Concur's solutions are audited regularly for compliance with the following global standards for Security and Service Management:

- **BS10012:2017**. In conjunction with parent corporate SAP SE (the certificate covers all of SAP), we are audited to this privacy standard.
- **ISO 9001**. In conjunction with parent corporate SAP SE (the certificate covers all of SAP), we are audited to this quality standard
- **ISO 27001**. The global standard for IT security management practices. SAP Concur has been BS 7799-certified since 2004 and undergoes multiple audits every year.
- **PCI DSS.** SAP Concur is a Visa® Registered CISP-Compliant Service Provider. As a Level 1 Service Provider, SAP Concur is audited annually by a PCI Qualified Security Assessor (QSA).
- **Sarbanes-Oxley Act**. SAP Concur is audited once a year as part of its annual public audits.
- **SOC1 Type II**. SAP Concur transitioned to the SSAE18 and ISAE3402 standard in 2010 , with audits every six months.
- **SOC2 Type II**. SAP Concur has added a SOC2 security audit report, beginning in 2017, with audits every six months.

Internal and External Audits and Scans

SAP Concur provides Software-as-a-Service for over 48,000 customers. To assure that our customers' data confidentiality, integrity, and availability are maintained, SAP Concur conducts multiple internal audits as well as third-party audits on a scheduled basis. The written results of many of these audits are available on request.

SAP Concur also undergoes periodic external scans, which are available on request. The following table shows the types of audits and scans, plus the frequency in which they are conducted:

Audit	Type	Frequency
Secure SDLC	Internal	Continuous
BS10012:2017	Internal	Continuous
BS10012:2017	External	Once a year
Corporate Risk Assessment	Internal	Annual
External PCI Scanning	External	Monthly
ISO 9001	External	1+ a year
ISO 27001	Internal	Continuous
ISO 27001	External	1+ a year
Network Vulnerability Scanning	Internal	Bi-Weekly
Network Vulnerability Assessment	External	Once a year
PCI DSS	External	Once a year
Sarbanes-Oxley	Internal	Continuous
Sarbanes-Oxley	External	Once a year
SSAE18 & ISAE 3402 - SOC1	External	Every 6 months
SSAE18 & ISAE 3402 - SOC2	External	Every 6 months

SDLC
Software / System Development Life Cycle - SDLC
Requirement Analysis
Design
Implementation
Testing
Evolution

You can find publicly available certificates and audits in the SAP Cloud Audit Trust Center: https://www.sap.com/about/trust-center/certification-compliance.html

Privacy

SAP Concur policies and practices follow many privacy laws, including the following:

- Australia Information Privacy Principles
- Canada Personal Information Protection and Electronic Documents Act (PIPEDA)
- The European Union General Data Protection Regulation (GDPR) – more info at https://www.concur.com/gdpr
- Hong Kong Data Protection Principles
- Hong Kong Monetary Authority Supervisory Policy Manual
- United Kingdom Data Production Act of 2018
- United States and State PII (Personally Identifiable Information) privacy, security, information protection (Massachusetts, California)
- SAP (and SAP Concur) audited to BS-10012:2017 – Personal Information Management standard
- Singapore Personal Data Privacy Act
- Monetary Authority of Singapore (MAS)

Privacy Product Features

By configuring Data Retention, clients can simplify their compliance with data privacy regulations by removing data. Removal involves anonymizing, deleting, or obfuscating the data.

SAP Concur has internal-use Read and Change access logging on personal data fields to meet GDPR requirements.

Third-Party Providers

Before third-party providers are approved to offer parts of SAP Concur's services, they must go through a formal vendor management program review to confirm and monitor that they provide an adequate level of security and comply with relevant data protection requirements. SAP Concur collects only the minimum necessary personal data and uses it only for agreed-on purposes.

Data Protection

SAP Concur has established the following safeguards for personal data protection:

- Data is encrypted when transmitted over public networks.
- Select personal data is encrypted when stored in databases.
- Email messages sent from SAP Concur Premier to customers are encrypted (this requires opportunistic TLS to be enabled on the customer side).
- Data is accessible only by vetted, authorized personnel.
- Client data is prohibited from being stored on SAP Concur workstations, and mobile devices.
- Multiple DLP systems (network, server, and email) prevent data exfiltration.

Data at Rest

- Credit-card numbers – Encrypted (AES-256) with unique keys that are never stored in full (split keys).
- Passwords (stored only when SAP Concur authentication is enabled) – one-way hashed and salted (SHA-256).
- SAP Concur uses Self Encrypting Drives (SED).
- All backups– Encrypted (AES-256).

Data in motion

- Web Browser User Sessions – TLS 1.1 & 1.2 (and above if available).
- Webservice APIs – TLS 1.1 & 1.2 (and above if available).
- Batch data feeds SFTP + PGP-2048 encryption, regardless of transport.

Data Centers

SAP Concur's cloud platform is based on a high-availability architecture with no single point of failure that is hosted on SAP Concur-owned hardware or in Amazon Web Services (AWS). SAP Concur's production hardware is co-located in several Tier 3+/Tier 4 data center facilities in Europe and the United States. For details on specific data center platforms, see below:

- Lynnwood, WA (US Primary) https://go.evoquedcs.com/SE1-Lynnwood-WA-Brief
- Dallas, TX (US warm site) https://go.evoquedcs.com/t/DA2-Webb%20Chapel-Brief
- Paris, FR (EMEA Primary) https://www.equinix.com/locations/europe-colocation/france-colocation/paris-data-centers/pa3/
- Amsterdam, NL (EMEA warm site) https://go.evoquedcs.com/Amsterdan-AMS1-Brief
- AWS https://aws.amazon.com/compliance/data-center/data-centers/

Environment	Primary site	Disaster recovery site
U.S. production	Lynnwood, WA	Dallas, TX
EMEA production	Paris, France	Amsterdam, Netherlands

Amazon Web Services

SAP Concur is in the process of moving from a pure private cloud operation, where all equipment is owned and operated by SAP Concur, to a more hybrid cloud. In the future, more and more of the SAP Concur stack will be implemented in Amazon Web Services (AWS). Some portions of the SAP Concur stack (microservices) are already active in AWS today, including:

- In-product messaging
- The App Center
- Receipt Ingestion
- New Hotel Services
- Hipmunk™
- TripIt®

Application Security

Secure Software Development Lifecycle

SAP Concur has implemented a secure software development lifecycle (secure SDL), requiring our product teams to include security training, tools, and processes that are in alignment with the Open Web Application Security Project (OWASP), NIST, and PCI DSS. These guidelines include secure coding implementation in application architecture, authentication, session management, access controls and authorization, event logging, and data validation.

Required processes for SAP Concur's product teams include threat modeling, inline and continuous security scanning and monitoring, and mandatory security reviews that enable product teams to deliver security as a feature. SAP Concur integrates static, interactive, and dynamic security testing into the secure SDL. SAP Concur also has an active responsible disclosure program managed through Bugcrowd (bugcrowd.com/concur).

AP Concur applications and services are designed to ensure that only authorized users can perform allowed actions within their privilege level, to control access to protected resources using decisions based on role or privilege level, and to prevent privilege-escalation attacks.

Role-based Access

- User roles can be defined both at the group level and at the user level.
- User roles can be used to adhere to Segregation of Duties (SoD).
- User and group access can be defined down to the form and field level.

Mobile Security

SAP Concur's mobile application (Concur for Mobile) is a proprietary application installed on a mobile device (not accessed via the device's web browser). Most security capabilities available to SAP Concur's web applications are also in place for mobile, plus the device's local security features. SAP Concur's mobile applications have extensive native MDM controls, described below.

Mobile Application Security Features

- Remote Device Wipe
- Will not install on Jailbroken or Rooted devices
- Device PIN Requirement
- Optional IdP/SSO enforcement
- Support for a localized MFA configuration
- All communications over TLS (1.2 or above)
- TLS CA verification and pinning enforcement
- All user data encrypted at rest
- Principle of Least Privilege
- No administrative interfaces

Data Display

- Symbolic credit card name (that is, My Corporate Card) and the last four digits of the credit card number may be displayed for reference.
- Full credit card information is never displayed on, transmitted to, or stored on the mobile device.

Data Storage

- Concur for Mobile application data is cached on a device to increase the performance of the application and to provide offline functionality. All user data is encrypted at rest (AES-256). Only information from the last user who logged into Concur for Mobile is stored on the device. If a user logs out of Concur for Mobile via the settings screen, all cached data is deleted. User passwords are not stored on the device. Expense and itinerary data are cached for offline viewing.
- Static data is cached for increased performance during look-up searches.
- Cached data is automatically removed (wiped) upon failed logins (either due to user error or the user's profile being marked inactive in SAP Concur).

Data Transmission

- SAP Concur supports TLS 1.2 (or higher) with a secure cypher suite that is reviewed bi-annually. HTTP Strict Transport Security (HSTS) with long duration is enforced. Support is provided for TLS 1.1 when TLS 1.2 or higher is not available.
- Certificate pinning is implemented for iOS and Android as an additional defense against man-in-the-middle (MITM) attacks.

Authentication

- All mobile platforms require authentication before accessing any data.
- Concur for Mobile does not store the user's password. When a user selects the auto-login feature, the system generates a unique authentication token that is stored securely on the device.
- Multiple SSO options, including enabling additional authentication methods such as biometrics and mobile only PIN, are available.
- Multifactor Authentication (MFA) can also be enforced by using a company Identity Provider (IdP).

Network-Based Security

SAP Concur's network architecture ensures that sensitive data is protected through best business practice security policies and procedures.

- **Hardened router configurations**. Router configurations correctly route packets to their proper destinations and restrict traffic. Access Control Lists (ACLs) on the front-end routers stop common attacks.
- **Network segmentation**. SAP Concur's multi-segmented network architecture prevents direct public contact or connection to SAP Concur's private network segment.
- **Front-end load balancers**. Access to SAP Concur services is managed with redundant load balancers. These provide a variety of functions, including TLS session termination, load balancing, network address translation (NAT), and port address translation (PAT).
- **Distributed denial-of-service (DDoS) protection.** A service protects the availability of SAP Concur services, even when they are under a distributed denial-of-service (DDoS) attack.
- **Activity log aggregation**. Log activities from network devices and systems are aggregated through an activity log collection system. Logs are fed to a SIEM, where alarms are generated for those events that warrant immediate attention
- **Proactive monitoring**. Security and Risk Management continuously monitor industry communities for news of security alerts, as well as vendor and partner security changes that may affect Information Services and SAP Concur's product line. Information Services has 24/7 automated monitoring with backup personnel.
- **Intrusion detection systems (IDS)**. Intrusion detection system (IDS) technologies are an integral component of SAP Concur's comprehensive enterprise security strategy. The IDS alerts SAP Concur when suspicious IP traffic or log activity occurs on SAP Concur's systems and networks.
- **Active vulnerability assessment**. Security scans of SAP Concur applications and infrastructure are performed on a regular basis by approved third-party PCI assessment vendors, SAP Concur Security Engineers, and internal scanning appliances (see table of audits and scans above). These scans check for vulnerabilities in both our external (public-facing) internet applications and our internal (private) networks. Discovered vulnerabilities are managed through SAP Concur's remediation process in accordance with industry best practices.
- **Web application firewalls**. Front-end web application firewalls protect SAP Concur services by blocking traffic that could represent attempts to steal application data or break in to SAP Concur web applications. These firewalls are highly distributed and monitored continuously.
- **VPN**. SAP Concur Global Operations Center personnel use a best-in-class VPN when connecting and processing from outside the trusted network. The VPN secure tunnel offers Internal Operations personnel highly secure remote connectivity to perform after-hours maintenance or trouble-shooting. Multifactor authentication is required for all SAP Concur personnel with direct access to production systems.
- **Digital certificates and TLS**. SAP Concur's services use 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.

Host-Based Security

Information Services employs a hardened, approved, and standardized build for every type of server used within the infrastructure. This procedure disables unnecessary default user IDs, closes unnecessary or potentially dangerous services and ports, and removes processes that are not required.

Servers are built, scanned for vulnerabilities, and remediated before being put out into the wild. This process is repeated every 30 days, with servers being rebuilt from scratch.

All patches are tested using a standard process to ensure proper functioning within the operating environment before they are applied to the servers.

The same process is used for SAP Concur co-locations and for AWS – we control the server builds.

SAP Concur uses dedicated engineers to continually update, optimize, and secure the standard build procedures, while adhering to industry best practices and regulatory requirements.

- **Database storage-area-network (SAN) cluster**. SAP Concur databases are stored on a fully redundant SAN. Drives are configured with RAID for all tiers of storage, and each segment of data has, at a minimum, two standby drives that are used automatically in the event of a drive failure. Database servers use N+1 clustering to prevent downtime in the event of a server failure.

- **File-integrity monitoring (FIM)**. SAP Concur's services use file-integrity monitoring (FIM) tools that alert operations personnel to any unauthorized or unexpected changes on any server.

- **Centralized logging**. Events from all systems are collected and aggregated, and alerts are sent, via a centralized log collection engine (SIEM) that is monitored by the SAP Concur Global Operations Center.

- **Standard change control process**. All changes to any part of SAP Concur's infrastructure must pass a strict Change Control Process to ensure best practices and minimal service interruption for our clients.

- **Security information and event management**. SAP Concur receives real-time alerts for a variety of activities that may indicate malicious activity.

Vulnerability Management

SAP Concur regularly tests application code and scans the network and systems for security vulnerabilities. Third-party assessments are also conducted regularly (see table of audits and scans above), including:

- Application vulnerability threat assessments
- Network vulnerability threat assessments
- Selected penetration testing and code review
- Static scanning of each release
- Continuous integrated application security testing of each release
- Bug bounty programs
- 24x7 advanced scanning of all services
- Security control framework review and testing

SAP Concur Personnel

- Background checks are performed on all candidates before hiring, including screening of education, past employment, credit checks, criminal record, OFAC, and other checks (depending on requirements and local laws).

- SAP Concur personnel are provided training regularly on security policies and procedures, including company policies and procedures, corporate ethics and business standards, and secure development training based on OWASP. Completion of security training is tied to system access.

- To ensure that personnel's knowledge of company security policies and procedures is current, regular updates are released and periodic performance appraisals are performed.

Disaster Recovery

SAP Concur uses a high-availability architecture to ensure that, in the event of a failure, service performance continues to meet client expectations.

SAP Concur's services are located at Tier 3+/Tier 4 co-location facilities. These were built using a "fortress" approach so that core services, telecom, and power are diversely supplied to the building and physical access is managed through state-of-the-art technology. These facilities are audited annually by a third-party . SAP Concur is also compliant with 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. The DRP is tested annually

In addition, real-time intersite data replication is performed between the production data center and the disaster recovery center.

.

Recovery Objective	Target
Recovery Point Objective	4 hours
Recovery Time Objective	2 business days

For the parts of the service that are hosted in AWS, a similar approach has been taken with disaster recovery environments that are maintained in the same region.

Backups

SAP Concur maintains a backup policy, process, and audit schedule for client information and critical infrastructure. Data is backed up nightly to disk. Backups are AES256-encrypted and stored locally, as well as copied to a secondary data center for remote storage in a Data Archive.

To enable support of GDPR and customer-specified data retention policies, the SAP Concur feature set makes it possible for clients to control how long SAP Concur stores their data--based on "who, when, and where" criteria.

By configuring this feature, clients can make it easier to comply with data privacy regulations by removing data. This feature removes data by anonymizing, deleting, or obfuscating it.

Ancillary data, such as extracts, are retained for only one year. Customer organizations that want to retain extract data for longer periods of time need to archive their copy of extracts.

When a customer relationship ends, SAP Concur destroys all customer data. SAP Concur also returns data to the former customer in accordance with the terms of the business services agreement between the parties.

SAP Concur Single-Sign On

SAP Concur SAML-based Single Sign-On (SSO) enables client organizations to have a higher degree of control over user ID management and authentication policy. It supports many SSO partners; for more information, see https://www.concur.com/app-center/category/it-solutions.

SAP Concur Web Services (APIs)

SAP Concur customers can build real-time connectors to SAP Concur Travel and Expense services to more tightly integrate SAP Concur systems into their own. Connections are established using TLS and OAuth authentication. For more information, see https://developer.concur.com/.

SAP Concur FTP Site

SAP Concur customers must use FTP with Secure Shell (SSH) Key Authentication for the transfer and retrieval of client information. The FTP sessions require client-specific accounts and complex, frequently changed passwords. Each file is PGP-encrypted with client-specific keys, and each file set resides in client-specific directories. FTP directories are chrooted and have extremely limited function calls.

Disclaimer

This document provides information gathered for convenience from different publicly available sources provided by SAP Concur. This document is for information purposes only and is by no means legally binding. Information in this document refers to the situation as of August 2019.

About SAP Concur

SAP Concur is a leading provider of integrated travel and expense management solutions, helping 48,000 companies in more than 190 countries control costs and save time.