Security and Privacy Overview

Concur Business Services

Version 1.30

CONCUR PUBLIC
NO NDA REQUIRED

Proprietary Statement

This document contains proprietary information and data that is the exclusive property of Concur Technologies, Redmond, WA USA. No part of this document may be reproduced, transmitted, stored in a retrieval system, translated into any language, or otherwise used in any form or by any means, electronic or mechanical, for any purpose, without the prior consent of Concur.

The information contained in this document is subject to change without notice. Accordingly, Concur disclaims any warranties, express or implied, with respect to the information contained in this document, and assumes no liability for damages incurred directly or indirectly from any error, omission, or discrepancy between any Concur product or service and the information contained in this document.

Concur Small Business edition™, Concur Standard edition™, Concur Professional edition™, Concur Premium edition™, Concur Government edition™, Concur™, and their respective logos are all trademarks of Concur Technologies. All other company and product names are the property of their respective owners.

Published by Concur Technologies.

Table of Contents

Audience

This document has been written for the current or potential clientele of Concur Business Services. The client may be running a variety of services or products within the Information Services data center(s), including Concur Small Business edition, Concur Standard edition, Concur Professional edition, Concur Premium edition, and Concur Government edition,.

This document assumes knowledge of basic and best business security practices, and is an overview of Concur's comprehensive Security Services. If at any time a client or potential client requires additional information, a meeting will be arranged with Concur Security and Risk Management. All information and identified brand name solutions are subject to change or update, and should be considered a point-in-time reference. Contact Concur Security and Risk Management for the latest version of this document.

Author

This document has been prepared and authorized by Concur Security and Risk Management Group.

Additional information is available upon request from Concur's Security and Risk Management Group.

Introduction

Concur is the world's leading provider of automated on-demand Employee Spend Management business services. This document provides a security overview of Concur's services. There are several perspectives of security that are discussed in this document:

- Security and Risk Management
- Security Audits
- Business Controls
- Privacy
- Physical Security
- Logical Security – network, host, and application
- Software Development Life Cycle
- Service Resilience
- Concur Customer Audits
- Financial Industry Shared Assessments Program

Security and Risk Management

Concur has a dedicated Security and Risk Management group. This group has been chartered according to ISO 27001 Information Security Management System (ISMS) standards. This group is led by the Manager of Information Security and Risk Management, who reports to the Vice-President of Security and Compliance.

> *"The ISMS is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties."*
> -ISO27001:2005

Security and Risk Management coordinates Concur's ISMS and provides for:

- Integrity,
- Risk Acceptance,
- Risk Analysis and Assessment,
- Risk Evaluation,
- Risk Management and Treatment, and
- Statements of Applicability.

Security and Risk Management Responsibilities

Concur's Security and Risk Management Group has a broad range of responsibilities, including:

- **Security and Risk Management**
  - Semi-annual executive security steering committee meetings
  - Bi-weekly security steering group meetings
  - Risk assessments and risk analysis
  - Compliance to applicable laws and regulations
  - Internal audit of applicable systems and processes

- **Business Controls and Audit Compliance**
  - Development, management, and internal audit of IT controls for Sarbanes Oxley, ISO27001:2005, SOC 1 (also known as SSAE16 and ISAE 3402, and formerly as SAS70), and PCI DSS (Payment Card Industry Data Security Standard)
  - Sarbanes-Oxley General Computing Controls (GCC) and Entity Level Controls audits
  - SOC 1 Type II and PCI-DSS data center compliance audits
  - SOC 1 (also known as SSAE16 and ISAE 3402, and formerly SAS-70) Type II audit of Concur services
  - ISO 27001:2005 (Information Security Management System)
  - ISO 20000:2005 (IT Service Management)
  - PCI DSS (Payment Card Industry Data Security Standard)
  - FISAP (Financial Institution Shared Assessments Program)

- **Access Management**
  - Privileged access approvals
  - VPN Access Control List approvals

- **Privacy**
  - Defined uses of private information to only the specific Concur service functions as required
  - Compliance with privacy laws and directives in the U.S., Canada, EU, and other jurisdictions

- **Incident Management**
  - Development, testing, and training for security incident response
  - Management of security incidents
  - Development of proactive incident avoidance controls
  - Escalation support for 24/7/365 IDS (Intrusion Detection Systems)

- **Vulnerability Management**
  - Scanning of application code as part of the software QA cycle
  - Perimeter vulnerability penetration scanning
  - Infrastructure vulnerability scanning
  - Structured remediation process

- **Corporate Business Continuity and Disaster Recovery Planning**
  - Development and testing of Concur's Disaster Recovery plan
  - Development and testing of Concur's Executive Disaster Response plan

- **Environment and Product Architecture**
  - Security and intrusion architecture validation
  - Security and risk mitigation of architecture proposals
  - Audit and detection system inclusion into proposals

- **Corporate Publishing and Contracts**
  - Corporate Information Security Policy
  - Corporate Information Security Awareness
  - DRP, BCP, Backup Processes

- Security and Risk Policies/Standards
- Review of Legal Agreements

Concur models the security posture of its technical operations by adopting, following, or seeking guidance from the following entities, standards, and frameworks:

- ISACA/ITGI/COBIT (Information Systems Audit and Control Association / IT Governance Institute / Control Objectives for Information and related Technology)
- COSO (Committee of Sponsoring Organizations of the Treadway Commission)
- FISAP (Financial Institution Shared Assessments Program)
- NIST Special Publication 800-53: Recommended Controls for Federal Information Systems and Organizations
- CSA (Cloud Security Alliance) Security Guidance for Critical Areas of Focus in Cloud Computing
- Privacy Legislation
  - GLBA (Gramm-Leach-Bliley Act – U.S. financial institution regulation)
  - SB1386 (California State PII regulation)
  - SB6043 (Washington State PII regulation)
  - EU Directive 95/46/EC (known as Safe Harbor in the U.S.)
  - PIPEDA (Personal Information Protection and Electronic Documents Act - Canada)
  - Data Protection Act of 1998 (UK)
- US-CERT (U.S. Computer Emergency Response Team, the operational arm of the National Cyber Security Division (NCSD) at the Department of Homeland Security (DHS))
- U.S. Internal Revenue Service Revenue Procedure 97-22
- NIST (U.S. National Institute for Standards and Technology)
- FISMA (Federal Information Security Management Act)
- OWASP (Open Web Applications Security Project)
- SANS Institute
- InfraGard

Security Audits

Concur undergoes several internal and external audits each year, as specified in Table 1.

Table 1. Concur internal and external audits

Audit	Frequency	Type
SOC 1 (also known as SSAE16 and ISAE 3402, formerly as SAS70) Type II)	Twice per year	External
ISO 27001	Twice per year	External
ISO 20000	Twice per year	External
PCI	Once per year	External
Application Vulnerability Assessment	Once per year	External
Network Vulnerability Assessment	Once per year	External
Sarbanes-Oxley	Once per year	External

Table 1. Concur internal and external audits

Audit	Frequency	Type
ISO 27001	Continuous	Internal
Sarbanes-Oxley	Continuous	Internal
Application vulnerability scanning	Monthly	Internal
Network penetration testing	Weekly	Internal
External PCI scanning	Quarterly	Internal
Corporate risk assessment	Annual	Internal

Business Controls

Concur has developed a comprehensive set of business controls that ensure the integrity and availability of Concur online services. These controls were developed to bring Concur into alignment with the following standards, regulations, and / or certifications:

- ISO 27001:2005
- ISO 20000 (the ISO version of ITIL, the IT Infrastructure Library)
- Sarbanes-Oxley General Computing Controls and Entity Level Controls
- SOC 1 (also known as SSAE16 and ISAE3402, and formerly SAS70 Type II)
- PCI DSS (Payment Card Industry Data Security Standard)
- FISMA (Financial Information Security Management Act)
- NIST Special Publication 800-53: Recommended Security Controls for Federal Information Systems and Organizations

ISO 27001:2005

Concur is certified to ISO27001:2005, the successor to BS 7799, the Code of Practice for Information Security Management. Concur first became BS7799 certified in 2004, and undergoes semi-annual audits for renewal of this certification. Concur was the 18th U.S. company to become ISO27001 certified. In order to earn this certification, Concur is required to show compliance in the following areas:

- Security Policy
- Organizational Security
- Asset Classification and Control
- Personnel Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Systems Development and Maintenance
- Business Continuity Management
- Compliance

ISO27001:2005
ISO20000:2005
IS 84383

Concur is in its eighth year of BS7799/ISO27001 audits, which take place twice each year.

ISO 20000

Concur is certified to ISO20000, the Code of Practice for Information Technology Service Management. This well-recognized standard provides a framework for the following business processes:

- Incident Management
- Problem Management
- Change Management
- Release management
- Configuration Management
- Service Level Management
- Cost Management
- Availability Management
- Capacity Management
- IT Service Continuity Management

ISO27001:2005
ISO20000:2005
IS 84383

Concur was initially certified to ISO 20000 in 2008 and undergoes twice-annual audits.

Sarbanes Oxley

As a public company, Concur is required to comply with U.S. Sarbanes Oxley Act of 2002 to ensure the integrity of its financial reporting and operations. Concur has adopted the control objective framework developed by Concur's public auditor of record. This framework consists of controls governing operations in the following functional areas:

- Access Management
- Change Management
- Governance
- Operations

Concur is audited once per year for Sarbanes Oxley compliance as part of its annual public audit.

Similar control objectives are asserted across a significant portion of U.S. public companies.

SOC 1 (SSAE16 and ISAE3402)

In order to meet the needs of its clients, Concur has established a control environment that ensures the integrity and security of Concur services. The controls are audited twice per year by Grant Thornton LLP, an American Institute of Certified Public Accountants (AICPA) licensed firm. The control objectives include:

- Security policies, procedures, and awareness
- Operational policies and procedures
- Change control process and procedures
- Physical security and access controls
- Vulnerability management
- Employee recruiting and hiring
- Protection of transmitted information
- Logical access control
- Concur Expense Service software and services

- Software development life cycle
- Performance and capacity management
- Security of offline data storage media

Concur transitioned to the SOC 1 (also known as SSAE16 and ISAE3402) standard, effective July 1, 2010. Concur's SOC 1 audits take place twice each year, from January through June and from July through December. Reports are available to existing Concur customers about sixty days after the end of each audit period

In addition to the Concur SOC 1 described above, Concur U.S.-based data centers for Concur Travel & Expense and Concur Expense Pro undergo annual SOC 1 and PCI audits.

Payment Card Industry Data Security Standard (PCI DSS)

Concur is a PCI compliant level 1 service provider, subject to an annual assessment and quarterly security scans. The high-level requirements in PCI are:

- Install and maintain a firewall configuration to protect data
- Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect stored data
- Encrypt transmission of cardholder data and sensitive information across public networks
- Use and regularly update anti-virus software
- Develop and maintain secure systems and applications
- Restrict access to data by business need-to-know
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data
- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes
- Maintain a policy that addresses information security

Concur is included on Visa's list of PCI compliant organizations as a Level 1 Service Provider.

PCI Standards Council

Concur is a Participating Member in the PCI Standards Council. As such, Concur plays a direct role in the ongoing development of PCI standards. This is a further example of Concur's leadership in the security and protection of sensitive corporate information.

Financial Information Security Management Act (FISMA)

Since 2003, Concur has operated an expense management solution that is FISMA certified and accredited at the "HIGH" sensitivity level (as defined by GSA IT Security Policy, CIO P 2100.1E and in NIST Special Publication 800-53) for the Department of Homeland Security's Travel Security Administration (TSA). This service was granted an Authority to Operate (ATO) in mid 2008 and renewed in 2009.

Privacy

Concur collects only the minimum necessary PII (personally identifiable information) and uses it only for agreed upon purposes. Concur has enacted the following safeguards related to PII:

- Encrypted when transmitted over public networks
- Encrypted when stored in databases and flat files
- Encryption of e-mail messages sent from Concur Travel and Expense to customers[1]
- Encryption of e-receipt data sent from merchants to Concur
- Accessible only by vetted, authorized personnel
- Storage of PII prohibited on Concur workstations
- Published privacy policies

Concur complies with the following privacy laws:

- EU Privacy Directive 95/46/EC through Safe Harbor certification
- U.K. Data Protection Act of 1998
- Canada PIPEDA (Personal Information Protection and Electronic Documents Act)
- U.S. state PII privacy and security incident disclosure laws

Physical Security

Concur takes steps to ensure the availability and physical protection of its servers by carefully screening personnel, and by controlling personnel access to server environments. Audits that cover physical security include:

- ✓ ISO 27001:2005
- ✓ Sarbanes-Oxley
- ✓ SOC 1 (SSAE16 / ISAE3402, formerly SAS-70)
- ✓ PCI DSS
- ✓ FISMA

Personnel

Concur performs verification of employment, references, criminal, education, credit, and U.S. Treasury OFAC background checks on all employees (details and methods on background checks for Concur employees within and outside of the U.S. vary based upon local laws).

[1] - E-mail messages to users are encrypted for customers whose e-mail servers support it – this will include messages about incoming charges, items to approve, and traveler itineraries.

New employees are given training on company policies and procedures, including standards for corporate ethics and business conduct, a confidentiality notification, and a signed NDA (non-disclosure agreement). All new employees receive security awareness training as a part of New Employee Orientation (NEO), and are required to sign an acknowledgment of understanding of Concur's corporate information security policy. Selected employees are required to undergo security awareness training each year. Developers are required to undergo secure development training.

Performance appraisals are completed periodically to ensure that employees' knowledge remains current and they are aware of both new and updated policies and procedures. In addition, the importance of security to Concur is evident through the presence of physical and other security controls (e.g., personnel and visitors must pass through several levels of security to gain access to Concur's processing facilities).

Facilities

Access to the production data centers and internal Concur Operations Center is controlled with electronic security badges using proximity key cards. Only specifically authorized personnel are granted access to the server rooms. The electronic security badge system maintains an audit trail of all admissions to these facilities. In order to gain admittance, customers, contractors, and other visitors must be escorted by authorized personnel.

Concur outsources data center services to a third-party hosting facility. This contains Concur product line web servers and other infrastructure equipment. Concur relies on physical security in place at this facility. All United States data centers undergo twice-annual SOC 1 Type II and annual PCI audits. To gain assurance that these controls are maintained, Concur obtains a SOC 1 audit report on a semiannual basis. This report is available for client inspection through a separate NDA that is available upon request.

Logical Security

Network Security

Concur's network architecture ensures that sensitive client data is protected through best business practice security policies and procedures. These procedures are derived from ISO 27001 and 27002, PCI DSS, SOC 1, NIST 800-53, and other standards. Network security encompasses needs-based access, proper network segmentation, and Security and Risk Management oversight.

Audits that cover network security and integrity include:

- ✓ ISO 27001:2005
- ✓ Sarbanes-Oxley
- ✓ SOC 1 (SSAE16 / ISAE3402, formerly SAS-70)
- ✓ PCI DSS
- ✓ FISMA

Network security highlights include:

- **Secure Internal Administration Network:** Concur employs a complete internal infrastructure to backup and monitor servers through secure connections. All web servers contain two Network Interface Cards (NICs). One NIC is connected to the public Internet behind the firewall, and the other is connected to the Concur Operations internal private

network. The IP addresses of these servers are protected from third parties through Concur's 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:** Concur's multi-segmented network architecture prevents direct public contact or connection to Concur's private network segment. This ensures client information is not accessible directly from the Internet. Concur utilizes intrusion detection systems that monitor all TCP/IP incoming and outgoing traffic between network segments.
- **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 Concur's product line. Information Services has 24/7 automated monitoring with backup personnel. Security threats are thoroughly investigated. Procedures exist for immediate steps to resolution and containment of security incidents.
- **Intrusion Detection Systems:** Intrusion Detection System (IDS) technology is an integral component of Concur's comprehensive enterprise security strategy. The IDS alerts Concur of suspicious IP traffic or log activity that occurs on Concur's 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:** Security and Risk Management performs infrastructure security scans on a regular basis using an approved PCI scanning vendor. Scans are performed from the Internet as well as from internal scanning appliances. Concur also scans its online application software for vulnerabilities. Any vulnerability found is managed through a remediation process, where this occurs, and dependent on the nature of the vulnerability a re-scan is required prior to implementation into production.
- **Application Firewalls:** Front-end firewalls protect applications and data by validating information flowing in and out of Information Services through an Access Control List. The Firewall and proxy application inspects data and records its origin before being accepted into the network. The Firewall denies all connections except those specifically allowed. The firewall also protects the network from random "ping sweeps" and unauthorized users by hiding or blocking unused network ports. Security violation attempts are logged, monitored and escalated when discovered by Concur Operations.
- **Application and Database Firewalls:** Concur utilizes three layers of firewalls that protect applications and client databases. Application firewalls permit traffic only from Concur web servers to reach Concur application servers, and database firewalls permit database queries only from Concur application servers.
- **VPN:** Concur Operations personnel use a best-in-class VPN when connecting and transmitting from outside the trusted network. The VPN secure tunnel offers internal Operations personnel highly secure remote connectivity to perform after-hours maintenance or troubleshooting. Two-factor authentication is used.
- **Data Protection:** Concur's services are located in one of two U.S.-based data centers. All customer data is located in one or more of these data centers on systems that are owned and managed by Concur. Full time Concur employees manage all networks, systems, databases,

and applications that contain customer data. Access to customer data is granted on a least-privilege, need-to-know basis.

- **Digital Certificates and SSL:** Concur's 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 with 128-bit or stronger key length. Concur uses a leading Certificate Authority for this process. Concur solutions utilize secure sockets layer (SSL) technology to ensure that HTTP communication between Concur clients and Concur servers is encrypted. Through SSL protected HTTP transactions, sensitive information such as financial and personal information passing through the Internet is reasonably protected.

Host-Based Security

Concur online services provide high levels of security through a specialized server build process. 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 down unnecessary or potentially dangerous services, and removes processes that are not required. In addition, all available and approved security patches are installed. Concur utilizes dedicated engineers responsible for continually updating, optimizing, and securing the standard build procedures.

Audits that cover server security and integrity include:

- ✓ ISO 27001:2005
- ✓ Sarbanes-Oxley
- ✓ SOC 1 (SSAE16 / ISAE3402, formerly SAS-70)
- ✓ PCI DSS
- ✓ FISMA

Host security highlights include:

- **Database SAN (Storage Area Network) Cluster:** 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 will be used automatically in the event of a drive failure. The RAID types vary with each tier of storage; types in use include RAID10, RAID6 and RAID5. Database Servers use N+1 clustering to prevent downtime in the event of a Server failure. The fiber channel connection to the SAN can handle 4GB/sec of bandwidth.
- **Standard server builds.** Windows and UNIX builds are based upon well-known server hardening standards. The latest software and security patches are regularly applied to the standard builds. Security methodology includes locking down and/or disabling / removing appropriate files and services. Security features include encryption services through SSL and password authentication, combined with rapid notification and response to security threats. All modules (software, firmware and hardware) and processes are routinely audited and updated to further mitigate security risk. Server configurations are managed through an enterprise configuration management tool that further ensures server security and integrity.
- **Data Backup.** Backup media for Concur's online services are fully encrypted with AES-128. Media that is stored offsite is safely transported by secure courier to a hardened off-site media storage facility.
- **Alert monitoring.** Security and Risk Management monitors vendor security updates, hacker sites, and security industry sites to understand where the next vulnerability and threat will surface.

- **File Integrity Monitoring:** Concur's services utilize file integrity monitoring (FIM) tools that alert operations personnel of any unauthorized or unexpected changes on any server.
- **Centralized Logging.** Events from all systems are collected, aggregated, and alerted via a centralized log collection engine.
- **Standard patch process.** All patch fixes are tested through a standard 3-step process to ensure proper functioning within the operating environment before they are applied to the servers.
  1. Patch is applied to a mirror site of affected environment
  2. Patch is migrated to a demonstration site to monitor real-world performance
  3. Patch is applied to production
- **Standard change control process.** All changes to any part of Concur's infrastructure must pass a strict Change Control Process to ensure best practices and minimal service interruption for our clients. Every effort is taken to ensure that all client sites are safe for critical e-business processing.

Application Security

Audits that cover application security and integrity include:

- ✓ ISO 27001:2005
- ✓ Sarbanes-Oxley
- ✓ SOC 1 (SSAE16 / ISAE3402, formerly SAS-70)
- ✓ PCI DSS
- ✓ FISMA

The Internet service models of Concur online services are delivered to clients via a Software as a Service (SaaS) model. Concur has specified browser settings to enhance Internet speed and performance of the application. Concur uses a combination of technologies, including HTML and JavaScript.

The Concur online services facilitate enforcement of individual client corporate travel policies by allowing custom definitions of:

- Rules for each travel policy, such as approval hierarchies, authorized vendors, and spending limits;
- Actions to take in the event of policy violations;
- Exceptions that merit overriding the approval workflow;
- Role-based security within the application.

Concur authorizes and creates administrator rights for the client organization, which is responsible for additional rights granted to personnel using the system.

Protected Information

Concur protects sensitive information in applications so that it is accessible to authorized persons only as needed. Details regarding the methods used to protect information are available upon request.

E-Mail Messages to End Users

Concur Premier issues e-mail notifications to end users for a variety of activities, including but not limited to notification of new credit card charges, new expense reports to approve, expense reports returned to a

user for additional work, and traveler itineraries. For organizations that support it, these e-mail messages are encrypted between Concur's outbound e-mail server and organizations' inbound e-mail servers, for organizations whose e-mail servers support encryption.

Concur Mobile

Concur's mobile application enables Concur customers to access core features of Concur through mobile devices including Blackberry, Android, and iPhone. All data transmitted to and from Concur Mobile is encrypted with SSL-128, and any local data storage is encrypted. All mobile platforms require authentication to Concur before any local or remote data can be viewed. Some platforms enable "remote wipe" capabilities.

Concur Single-Sign On

Concur offers SAML- and HMAC-based single-sign on, which permits client organizations to extend their SSO environment to include Concur. Single sign-on enables client organizations to have a higher degree of control over userid management and authentication policy than would otherwise be available.

Concur Download Server

This download server maintains general ledger data that is extracted from each Concur client database for accounting and reporting. This server contains downloadable reports that are provided to clients through a secured HTTPS site. These reports are designed to integrate with each client's accounting system. Concur client information is stored on a secure file server in an archive directory. Individual information is available for up to 7 years.

Concur FTP Site

Concur utilizes FTP for the transferal and retrieval of client information. The FTP sessions require client-specific accounts and complex, often-changed passwords. Each file is PGP encrypted with client-specific keys, and each file set resides in client-specific directories. Supported transfer protocols include FTP, SFTP, and FTPS. All processes are logged whether successful or not. Files contain validation tables and customer information to be imported into the Concur system, or general ledger data extracted from the application for client use. Files available for download by the customer must be deleted at completion of the download process. All files transmitted and received are stored and available for up to 1 year.

Credit card charges data is received directly from Credit Card providers or from aggregators such as Yodlee via secure communications over public or private networks. The processes used for the transfer and processing of this data is regularly audited by PCI auditors.

Software Development Life Cycle

Audits that cover application security and integrity include:

- ✓ ISO 27001:2005
- ✓ Sarbanes-Oxley
- ✓ SOC 1 (SSAE16 / ISAE3402, formerly SAS-70)
- ✓ PCI DSS
- ✓ FISMA

Concur utilizes a software development life cycle (SDLC) process to manage the integrity and reliability of its products and services. Elements of the life cycle include:

- Inception
- Requirements and specifications
- Design
- Coding
- Testing
- Scanning for software vulnerabilities
- Release to production

Each step is subject to a formal review and release to the next step in the life cycle. Key security activities that occur in the SDLC include:

- Risk analysis of all new features and changes
- Vulnerability scanning of new software releases
- Change Control Board review prior to release into production

Service Resilience

Concur's services are designed with resilience and availability in mind. The services infrastructure utilizes load balancing, redundant network, server and storage components, and recoverability. A disaster recovery plan ensures that Concur's hosted services are recoverable in the unlikely event that a disaster occurs.

Concur's services are housed in state-of-the-art data centers in Washington State and Texas. Audits that cover service resilience include:

- ✓ ISO 27001:2005
- ✓ SOC 1 (SSAE16 / ISAE3402, formerly SAS-70)
- ✓ PCI DSS

Concur has developed and tested a disaster recovery capability for Concur services since 2007. Additional details are available upon request.

Disaster Recovery and Prevention / Redundancy

Disaster Recovery Testing

Concur has formal disaster recovery plans that are tested annually. Additional information, including RTO (Recovery Time Objective), RPO (Recovery Point Objective) targets, and test results, are available upon request.

Client Data Centers

Concur data centers have an uninterruptible power supply (UPS) and backup generators to support the facility in case of a power outage. UPS systems are designed to support all equipment until diesel generators are activated. Data center physical risk mitigation is covered under the data center provider's SOC 1 Type II audit. Data center component and connectivity is covered by Concur.

Concur has designed a minimum of N+1 physical redundancy for the Concur application servers. All servers are backed up on a daily basis. Backup media is taken offsite and stored with a third party, secured media storage vendor. Servers have mirrored disk drives and Concur holds spares onsite in case of drive failure. The SAN database and file servers have redundant arrays of independent disks (RAID) fault tolerance for increased reliability and performance.

Redundancy is maintained for routers, switches, firewalls, load balancers, application and database servers. On fail-over the redundant device is configured to take over immediately. Logs are reviewed and trends

are analyzed to identify the potential impact on system availability objectives. Concur has consistently exceeded the standard SLA for uptime for both services, as defined in client service level agreements.

Global Operations Center

The Concur Global Operations Center is located in Eden Prairie, Minnesota and Dallas, Texas. Operations centers also exist within each of the data centers in the event of a central operations failure. The Global Operations Centers have a UPS with a minimum one hour run time, backed up by a generator. Hardened remote VPN circuits ensure that a total loss of the Global Operations Center will not affect employee connectivity to the data centers.

Concur Customer Audits

Concur does not support customers, or their auditors, performing audits of any Concur service. Instead, Concur undergoes several external audits that are performed by competent and qualified external audit firms, as described earlier in this document. The written results of many of these audits are available upon request.

Concur does not support any form of security scanning or penetration scanning of any Concur service. Concur does not have separate infrastructure available for such activities; scanning of production environments is prohibited because of the risk of service disruption to other customers. Instead, Concur undergoes periodic external scans, some of which are available upon request.

Financial Industry Shared Assessments Program (FISAP)

BITS is a not-for-profit, CEO-driven financial service industry consortium made up of 100 of the largest financial institutions in the US. One of the products is the Financial Industry Shared Assessments Program (FISAP), which consists of a standard-form, highly detailed questionnaire that suppliers can use when bidding for financially related services. Concur utilizes this questionnaire, which contains more than 3,000 individual questions about the security of Concur services. In many cases, this questionnaire will contain most or all of the detailed information that customers require regarding Concur service security. Because the questionnaire is already completed, Concur can deliver this immediately, resulting in a substantial time savings during the procurement cycle.

Summary

Concur Technologies protects its hosted services using a defense in depth strategy that includes business controls in the following areas:

- ✓ Organizational – well defined roles and responsibilities for security, development, and support processes
- ✓ Privacy – protection and handling of sensitive information
- ✓ Physical – personnel and facilities
- ✓ Logical – network, host, database, and application
- ✓ Development – life cycle processes
- ✓ Resiliency – disaster recovery and continuous monitoring

To ensure that Concur is doing the best possible job in all of these areas, Concur is regularly audited in these functional areas against the following standards and / or regulations:

- ✓ ISO 27001:2005
- ✓ ISO 20000:2005
- ✓ Sarbanes-Oxley
- ✓ SOC 1 (SSAE16 / ISAE3402, formerly SAS-70)
- ✓ PCI DSS
- ✓ FISMA

Concur makes every effort to protect client data and the client's online experience.

Concur will continue to evolve its security policies and practices to meet changing technology conditions to ensure client data is protected, while meeting our primary objective of delivering the most reliable and secure application with optimal product performance.