SAP® Cloud: Focusing on security

So you can focus on business

Vinod Choudhary
William Harmer III
Ralph Salomon

The Best-Run Businesses Run SAP™

SAP® Cloud: Focusing on security

So you can focus on business

In the past, business software for everything from HR management to accounting and customer relationship management was accessible only to companies with deep pockets—firms that were capable of making massive up-front investments. Today, technology has leveled the playing field. But has security caught up with the new playbook? At SAP, we believe it has.

Thanks to cloud computing, core business applications are now available to everyone, from the largest enterprises to small and midsize businesses. Simply put, the applications—and their associated data—are delivered over the Internet. Software-as-a-Service, or SaaS, has become a business model as well as an application delivery model. SaaS offers the unique quality of multi-tenancy, which primarily differentiates it from the application service provider (ASP) model or from in-house applications. With SaaS, just one software instance can serve many customers (or tenants).

Core business applications are now available to everyone, from the largest enterprises to small and midsize businesses, through cloud computing

The ASP model, providing software over a network, forced business executives to confront their fears of putting mission-critical information on third-party servers[1]. Security concerns in a SaaS model are similar to those for the ASP model. Will people steal information? Will leaks compromise confidential data? The top security concerns for the SaaS model focus on identity management, data storage location, system operations and data transmission and flow controls.

SAP understands the critical importance of information protection and recognizes the contribution that information security makes to an organization's strategic initiatives and overall risk management. In cloud solutions from SAP, there are security controls and practices for its SaaS offerings that are designed to protect the confidentiality, integrity, and availability of customer information. Additionally, SAP continually works to strengthen and improve those security controls and practices. These controls also apply to any sub-contractors that provision SaaS cloud services for SAP.

The current best practices associated with information security involve a layered approach, what the industry calls "defense in depth." Regardless of the software delivery model, security cannot be implemented at a single "make or break" point. For a SaaS provider to ensure data security for sensitive information, it must have a comprehensive, multifaceted security program in place. The SAP Cloud portfolio offers a holistic approach to information security, implementing a multilayered defense at all the touch points in the information flow, providing complete data privacy, transparency, and audit controls. This approach includes both the physical and logical layers applied across the application as well as the middleware, database, operating system, network and communication layers, and the underlying datacenters.

This paper explores why SAP should be your trusted provider and it addresses the top security concerns associated with the SaaS model, the layers of information security, and the security controls and practices of SAP. The company has taken all the necessary steps—as well as a few extra—to help you meet the high demands of security in a SaaS world.

1 SaaS Security and Pricing, Progress Software, 2008

Top security concerns of the SaaS delivery model

As companies use software delivered through a SaaS model, their overarching concerns focus on vulnerabilities related to identity management, data storage and location strategy, and data transmission. The SaaS-based offerings from SAP include built-in security features to resolve these concerns.

Identity management

Modern SaaS architecture usually involves a Web-based application and communication that occurs over the Internet. With cloud solutions from SAP, customers can feel confident that the communication between them and SAP leverages Secure Sockets Layer (SSL) or Transport Layer Security (TLS) encryption. SAP solutions also support dedicated encrypted communication channels (WAN and VPN) for better access and integration. SAP also provides customers a choice: the management of all security from top to bottom, or the ability to integrate SAP Cloud with their own industry-standard identity management solutions. Cloud solutions from SAP also provide:

- **Internal authentication:** Cloud solutions from SAP use an internal repository of user profiles when customers choose not to integrate their identity management product with SAP solutions
- **Federated authentication (single sign-on):** For Web-based SaaS offerings, the single sign-on (SSO) functionality in cloud solutions from SAP requires users first to be authenticated by their authorizing system. Then they are redirected to SAP solutions. The trust mechanism passes the identity information between the customer and these solutions. The primary transport protocol for this trust mechanism is standard Hypertext Transfer Protocol Secure (HTTPS). In the SAP HANA® Enterprise Cloud service, a direct integration into the customer network and single-sign-on implementation is possible. Cloud solutions from SAP also use single sign-on features of the SAP NetWeaver® technology platform for system-to-system and administrator authentication.

  Cloud solutions from SAP support the Lightweight Directory Access Protocol (LDAP) and tokens, such as MD5, SHA-1, HMAC encryption, DES, and 3DES. The solution also supports Security Assertion Markup Language (SAML 1.1, 2.0) and SAP Supply Network Collaboration with encrypted remote function call (RFC) and client/server personal security environment (PSE) verification.
- **Separate authorization and authentication modules:** Authentication methods often change as a SaaS platform matures. However, because the authorization component is generally interwoven throughout the core code, cloud solutions from SAP ensure that user data and function permissions validation are separate from the authentication module(s). The authorization module in the SAP solutions also logs every action and validates every request to prevent cross-scripting attacks.

  The SAP Business ByDesign® solution and SAP HANA Enterprise Cloud use an access manager to track and manage internal users and permissions.
- **Password protection:** Cloud solutions from SAP require strong passwords that conform to industry standards and requirements (at least eight alphanumeric characters), and also mandates regular password changes (at least every six months). Passwords are not stored as clear text.
- **No administrator:** With cloud solutions from SAP, users have identities for accessing information instead of relying on a centralized administrator account. Additionally, the functionality in SAP HANA Enterprise Cloud allows people to access certain SAP components (for instance, the SAP HANA database) only with a dedicated and customer-specific administrator user.

Data storage and location

In an ASP model, each customer has unique hardware that keeps data segregated at all times. In a SaaS model, heterogeneous data may reside within a single instance of a database. To address information privacy concerns, current compliance regulations require the segregation of heterogeneous data within a SaaS environment. SaaS vendors must demonstrate that they can separate customer data for each customer not only to satisfy the regulations but also to give people peace of mind. If the "how" of data storage is a concern for your organization; a SaaS provider should be prepared to answer all your questions.

With cloud solutions from SAP, there is a logical isolation within a SaaS application that extends down to the virtual server layer. In certain environments like the SAP HANA Enterprise Cloud, organizations will also get physical isolation via dedicated SAP HANA database servers that reside in dedicated customer network segments (VLANS).

The physical storage location of customer data is of utmost importance for many organizations. This is the reason why cloud solutions from SAP give organizations location-specific choices (such as US- or Europe-based cloud data centers).

Every SAP location complies with the same standards and is interchangeable from a technical point of view. It is up to the customer which data storage location and local jurisdiction is preferred.

Cloud solutions from SAP segregate heterogeneous data by using the following approach to build the application architecture and store the data:

- **Unique database tables:** Most service providers offering shared Web access have one set of database tables in a normalized database that is shared by many customers. In contrast, organizations that use cloud solutions from SAP share the network security infrastructure, Web servers, application servers, and database instance. However, each customer has its own set of database tables within its own unique database schema, which ensures complete segregation of tenants' data.
- **Dedicated database Servers:** In case of a SAP HANA database, SAP provides a dedicated physical database server that is located in the customer cloud network segment.
- **Encrypted data storage:** When cloud solutions from SAP support database or file system encryption, all encrypted data is stored on disks using a minimum of AES 128-bit encryption.
- **Secure levels:** In SaaS services, the top two tiers (application and Web in later levels) are completely stateless. Cloud solutions from SAP dramatically reduce the security risk of these two tiers because no sessions are kept in memory or written to disk. This approach simplifies the construction of load-balanced server farms, as there is no need to keep the workloads on any given server.
- **Movement of data:** It is important to remember that data is moving through multiple tiers, and each level must ensure data security. Cloud solutions from SAP use a defense-in-depth strategy to provide segregation of data at all layers.

System Operations

SaaS providers must ensure that the general capabilities of secure and stable IT operation comply with industry standards and technology best practices. This is achieved by international- and country-specific certifications such as ISO27001, ISAE3402, and SSAE16. In some cases, industry-specific regulations and certifications are required to ensure that a cloud solution is as secure and compliant as those on premise.

Cloud solutions from SAP help organizations meet these requirements by providing industry-standard certifications and ITIL-based operational processes that include security management and governance functionality such as the following:

- Change and security patch management processes
- Security incident management processes
- Identity management processes
- Monitoring inclusive security compliance (configuration management)
- Activity logging and vulnerability management solutions
- Asset management and system lifecycle management
- Virus and malware protection
- Network isolation (firewalls, routers, and VPN gateways)
- Surveillance solutions such as intrusion detection systems, load balancers with Web-based application firewalls, 24x7 security monitoring, and security and event management

SAP applies high security level not only to the cloud server environment but also to the administrator client infrastructure found in cloud solutions from SAP. Every PC or laptop used by SAP employees that work on providing these service offerings are monitored by antivirus software, intrusion prevention systems (IPS), and compliance monitoring tools. This helps ensure that the operating system and applications used by SAP employees comply with the company's security policy and that the security policy is enforced. Additionally, the hard drives in all client devices are encrypted and access to the SAP Intranet is restricted by a network access control solution that rejects unknown equipment or non-compliant SAP devices from the network.

Data transmission and data flow control

SaaS uses the public Internet to transmit data, requiring that transmission security, such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS), be designed into the system. The use of SSL and TLS creates secure tunnels for information transmissions. Unfortunately, the use of distinct communication channels for each customer is counterintuitive and costly, and can become a maintenance challenge. Therefore, the use of private lines should be avoided, and instead, service providers should focus on controls.

Within the SAP Cloud portfolio, there are solutions that use dedicated WAN connections between the customer and SAP. These connections include any of the following: an SSL solution, a VPN tunnel based on Internet Protocol Security (IPsec), or encrypted router communication over the Internet, the VPN or the WAN connection. Cloud solutions from SAP include functionality that prevents eavesdropping, tampering, and forgery through cryptographic controls, a defense-in depth strategy, and the enforcement of the following security requirements:

- **Confidentiality:** Data can be viewed only by the intended recipient.
- **Integrity:** Data cannot be altered without detection.
- **Nonrepudiation:** The recipient of the data has proof that the data originated from a cloud solution from SAP.

Furthermore, cloud solutions from SAP secure communications by employing many of these data transfer options:

- **Secure Web communication:** Cloud solutions from SAP implement SSL technology that comes with both a public and private key to protect sensitive information. The public key is used to encrypt information, and the private key is used to decipher it. When a Web browser points to a secured domain, an SSL handshake authenticates the server (Web site) and the client (Web browser). An encryption method is established with a unique session key. Customers may then begin a secure session that guarantees message privacy and message integrity.
- **Secure messaging:** Outgoing email notifications sent from cloud solutions from SAP can be securely encrypted using TLS, which makes it difficult to tamper with email message content or send spoofed emails.
- **Secure FTP with file encryption:** Data files can be transmitted by secure FTP, HTTPS, or sent to SAP FTP server or a customer's FTP server. Files can be encrypted using Pretty Good Privacy (PGP), Transparent Data Encryption (TDE), or Secure/Multipurpose Internet Mail Extensions (S/MIME) before transmission.
- **Encryption keys:** Encryption keys are securely protected and customers can request a new one at any time.
- **IPsec VPN Tunnels:** SAP solutions support various VPN-device vendors and specifications that can be used to setup a secure and encrypted tunnel between cloud solutions from SAP on the customer network segment and the customer site.
- **WAN connections:** Cloud solutions from SAP can be connected directly via a WAN connection to the customer network. In this scenario, even customer-specific or customer-provided WAN equipment can be setup in SAP data centers. Encryption keys are securely protected and customers can request a new one at any time.
- **Physical-encrypted and secured data transfer:** Physical data transfer is typically used by customers that have huge amounts of data (such as customer databases). It is also used by customers with slow connection speeds that would result in very slow transfer rates over the Internet. In such cases, the data can be shipped on physical disks or network-attached storage (NAS) with the following security measures:
    - **Encryption:** The file system on the disks use strong encryption (such as AES with 256-bit encryption
    - **Storage device wiping:** There is a secure data wipe process before reusing the disks or data storage.
    - **Transport and carrier process:** A tracking option is available for the carrier process. There is also an option, which includes documentation, such as the serial numbers of the disks in each data transfer that provides evidence against manipulation

Layers of information security

Cloud solutions from SAP help customers address security concerns at the physical, database, middleware, application, and network and communication layers.

Layer 1: Physical site (SAP data centers)

For most businesses, downtime is simply not an option. That's why data centers, which house the servers that run mission-critical applications, require multilevel protection to guard against disruptions, whether it's a power outage or illegal access by an intruder. Investing in this level of security can be cost-prohibitive which is why many companies choose to outsource this to a trusted provider.

SAP operates its own data centers and also partners with localized world leaders in colocation hosting centers to provide environmentally controlled, secure facilities that use an integrated security management system. These security measures include electronic photo ID badging, cardholder access control, biometrics, recorded digital video surveillance, and alarm monitoring. All SAP data centers are ANSI/TIA/EIA-942 Tier III+ rated facilities. Each facility is equipped with continuous monitoring; multiple, redundant UPS-protected power circuits with generator backup; smoke detection units; fire suppression systems; 24-hour, year-round onsite security personnel; and intrusion detection alarm systems. Further details are available on the SAP Data Center Web site.

SaaS providers must provide multilevel protection to guard against business disruptions, from power outages to illegal access by an intruder

In addition, the facilities include safeguards that:

- **Block illegal entry** via biometric readers, bulletproof walls, and concrete pillars
- **Monitor the entire facility** by using closed-circuit cameras located in equipment areas, corridors, mechanical, shipping, and receiving areas
- **Immediately act on security breaches** through the use of silent alarms, which automatically notify security and law enforcement personnel if a breach occurs
- **Avoid downtime** by preventing power spikes, surges, and brownouts with redundant power links to local utilities, backup batteries, and uninterruptible power supplies and by interconnecting to the largest aggregation of global Tier 1 networks
- **Shield against fire, natural disasters, and weather shifts** with fire-suppression systems; heat, temperature, airflow, and humidity monitoring; and earthquake-safe designs

Technical vulnerability management

SAP has implemented technical vulnerability management in its solutions to reduce risks resulting from the exploitation of technical vulnerabilities. The use of operator logs and fault logging helps ensure the identification of system problems. System monitoring checks the effectiveness of the controls that are implemented and verifies conformity to the information security policies and standards found in cloud solutions from SAP. The company uses industry-leading security partners to conduct daily and monthly penetration tests on the production environment, and customers also can perform their own application vulnerability testing.

Layer 2: Database

Database environments used in cloud computing can vary significantly. For example, some environments support a multi-instance model, while others support a multi-tenant model. Cloud solutions from SAP support both models depending on the service offering. Data must be secured while at rest, in transit, and in use, and access to the data must be controlled. The use of advanced security mechanisms in cloud solutions from SAP not only secure data while at rest but also secure access to the data through these measures:

- **Advanced security:** Cloud solutions from SAP use an advanced security method based on dynamic data and encoded session identifications. SAP hosts the database in a secure server environment that uses multiple firewalls, access controls, intrusion detection systems, and other advanced technology to prevent interference or access from outside intruders.
- **Load balancing:** Cloud solutions from SAP are load balanced at every tier in the infrastructure, from the network to the database servers. Database servers are also clustered for failover. Internet-facing load balancers provide the option to use a Web-based application firewall to shield customer-specific applications and data flows from unauthorized access or malicious attacks.
- **Attack prevention:** With activity monitoring and blocking, cloud solutions from SAP employ a protection layer for databases that analyzes network traffic to prevent attacks. In some SAP services, an application-level firewall can be used to monitor and validate all traffic between the application and database tiers to prevent attacks, such as SQL injections, from reaching the database server.
- **Access control:** SAP requires that all access to information processing facilities and business processes be controlled according to business and security requirements. In all cases, the concept of least privilege determines computer access. Users are limited to the minimum set of privileges required to perform a required function.
- **Database audits:** Through regular database audits, SAP solutions maintain records demonstrating proof of origin, any alterations, additions, or deletions, the date time-stamp of a data change, and approvals. To maintain viability, an audit log cannot be altered, if needed encrypted, and kept on a system (or within the SAP Security Monitoring center) to which system engineers do not have access.
- **Classification of information:** All information, regardless of medium or form, is classified to reflect its level of confidentiality or importance to SAP and its customers. For instance, customer data is typically classified as "confidential."
- **Data encryption:** Many of the cloud solutions from SAP encrypt data in a way that doesn't affect applications—they decrypt the data on the fly when applications access the data, but keep the data encrypted for other types of access. . These solutions, which have passed the Federal Information Processing Standards (FIPS) 140-2 Level 3 certification testing, use a minimum of AES 128-bit encryption to secure data at the block level of the SAP storage systems.
- **Backup and restore:** Cloud solutions from SAP run full and incremental data backups on a daily, weekly, and monthly basis. In multitenant environments, these solutions store backed-up data on an encrypted disk using AES 128-bit encryption. This data is available for rapid reimplementation and system restores if the original data becomes corrupt.

Layer 3: Middleware

The architecture of the software and hardware used to deliver cloud services can vary significantly among public cloud providers. The cloud provider determines the physical location of the infrastructure as well as the design and implementation of the reliability, resource pooling, scalability, and other logic needed in the support framework. Application servers are built on the programming interfaces of Internet-accessible services, which typically involve multiple cloud components communicating with each other over application programming interfaces (APIs). It is important to understand the technologies the cloud provider uses and the implications that any technical controls have on the security and privacy of the system throughout its life cycle.

Cloud solutions from SAP help ensure that safeguards are in place to enforce authentication, authorization, and other identity and access management functions. Multifactor authentication is superior to standard password authentication because it requires another layer, such as biometrics or a dongle, to authenticate the user. The three basic pillars of multifactor authentication include who you are, what you know, and what you have. At SAP Cloud, multifactor authentication is an absolute must for SAP administrators that manage the production environment. Other safeguards include the following:

- Single sign-on and identity federation
- Security Assertion Markup Language (SAML) 2.0 assertion
- Integration between the SAP public cloud and identity management systems on the premises
- Fully delegated administration

Layer 4: Application

Most cloud solutions from SAP are written in Java and adhere to the J2EE specification. The applications dynamically produce every page, encrypt them and send them to a user's desktop using SSL. No content or static HTML pages are delivered by the applications unless required by the customer. The cloud solutions from SAP employ a unique and proprietary XML schema that provides a single consistent software code base and is configurable to a customer's business requirements. This approach allows for the continual testing of software to help ensure security, since every customer runs the same version of the code. Cloud solutions from SAP employ extensive security measures to protect against the loss, misuse, and unauthorized alteration of data.

If a customer's cloud service includes SAP standard software (such as the SAP NetWeaver Application Server component), the solution includes the same security features and measures as any on-premise installation would. This includes, but is not limited to, secure and encrypted communication, security parameters, user profile and role-based authorizations, advanced logging, transport management, and transaction controls.

The SaaS solutions from SAP help customers:

- **Protect applications from insider threats,** with tight encryption through a 128-bit SSL connection. Using open standards (HTML and JavaScript) ensures that applications do not require any changes or special permissions on a user's desktop.
- **Avoid risky plug-ins and downloads** that can cause viruses or other threats by using browser-based administrative functions, such as password resets.
- **Guard against phishing and pharming** by using email encryption and regular virus scans, as well as plain text emails, to eliminate the possibility of a hidden link that can gather information from users.
- **Protect against improper logins** by requiring user logins each time the application is opened as well as one-way SHA-1 hash encrypted passwords, automatic logouts after a c, and account locks after multiple failed logins.
- **Provide best practice security at all levels**—function, transaction, field, and data—by using role-based permissions (RBP).
- **Enforce segregation of duties** by ensuring that no individual can breach security through dual privileges. No person can hold a role that exercises audit, control, or review authority over another concurrently held role.

Phishing and pharming:

SAP Cloud protects you against both

"Phishing" is an attempt to obtain access credentials such as user names and passwords by using fake email or messaging (text, instant, or direct) to unsuspecting recipients. "Pharming" is an attempt to redirect a Web site's traffic to another site for malicious intent. Cloud solutions from SAP take extra precautions because even if most people in a customer's organization know how to protect themselves, others may not.

Layer 5: Network and communication

When securing a network infrastructure, it's important to strike a balance between security and availability of applications. This is why every component of an IT network—from the point of entry on the network down to the final place where information is stored—must be meticulously configured, deployed, maintained, and continually tested for optimal performance.

Every component of the IT network must be meticulously configured, deployed, maintained, and continually tested for optimal performance

Highly dependable equipment, such as routers, switches, and load balancers, are configured to provide secure, high availability access. Additionally, cloud solutions from SAP have taken extra measures to maintain the balance between rigorous protection and continuous availability. SAP solutions have the functionality to accomplish the following:

- **Reinforce security** with connections to multiple Tier 1 Internet service providers (ISPs) for highly available network access. All network equipment is redundant, providing seamless failover between devices. Web, application, and database tiers are configured as secure segments and tuned for maximum performance.
- **Limit internal network traffic** to pass along only the data required by the application. Several cloud solutions from SAP use a multitiered network architecture, which limits end-user traffic to the front "demilitarized zone" (DMZ) tier of Web servers or directly to the customer's virtual local area network (VLAN) segments. A firewall-controlled, segregated VLAN isolates each tier of the system from the other tiers, and each tier is set up on its own hardware stack. All requests are individually validated before independent requests to the next tier are generated. Incoming customer user requests are, for example, passed through the firewall down to the load balancers, which distribute traffic to the appropriate Web server (presentation tier) for processing. The Web server then makes independent requests to the application tier, and the application tier makes independent requests to the database tier. At each level, an incoming request is validated against business and security rules to protect against malicious access. Requests that fail validation are terminated. Traffic within each tier is restricted. Only required ports are enabled on servers and permitted between VLANs. The firewall separating the application and database tiers uses a default policy that drops all traffic unless specifically required. SuccessFactors, an SAP company, has implemented 11 security patents at this point.

Industry-leading security partners

SAP works with the best security and monitoring service providers to:

- **Ensure individual server performance and uptime** by using remote server monitoring
- **Maintain a smooth user experience** through global, transaction-based monitoring
- **Stop network intrusions** by using complete security coverage, including separate 24-hour, year-round security teams
- **Prevent malicious server attacks** with host-based and network-based intrusion detection
- **Protect against potential threats** by using thorough and proven application and infrastructure vulnerability testing
- **Identify information-system problems** by using detailed logs
- **Verify the effectiveness of security controls and compliance** with information-security policies and standards via system monitoring and audit controls

Security controls and practices in SAP Cloud

Implementing procedures to control what and how changes occur, providing user education, and fostering security awareness are as important as the firewalls in front of a customer's sensitive data. This section describes the controls SAP Cloud has put in place, including information security incident management, consistent and proven security measures, information security standards, security education and awareness, and compliance standards.

Information security incident management

SAP Cloud implements formal event reporting and follows escalation procedures if an information security incident occurs. Real-time notifications of vulnerabilities and security incidents are entered into the SAP ticketing system, and the appropriate SAP personnel are notified. All actions taken to resolve a problem are documented, so all problems can be tracked to completion. Information security staff will generate a report regarding the need for enhanced or additional controls to limit the frequency, damage, and cost of future occurrences, as well as required revisions to information security policies.

Consistently proven security measures

Security controls and processes are vital, but establishing the right procedures can be challenging. Strong security measures are necessary, but there is also a need to maintain the continuity of business operations. Security measures that interrupt the daily flow of information are counterproductive. SAP was one of the first SaaS companies to successfully complete the newest SSAE 16 SOC 2 audit in 2011. Customers can review all of the procedures, along with the auditors' findings, used to secure their data in cloud solutions from SAP. SAP Cloud also certifies against ISO27001.

Security measures that interrupt the daily flow of information are counterproductive

The multitiered approach found in cloud solutions from SAP help ensure a balance between control and ease of use. Users can stay productive, while customers' information stays secure. And when changes are made to the environment, they are logged, approved, and verified through a centralized, online application.

This multitiered approach is one of the reasons why some of the cloud solutions from SAP have been able to successfully release product updates and enhancements four times a year without fail.

Information security standards

SAP Cloud's business assets include information and the information-processing environment that supports it. Identifying, implementing, maintaining, and improving information security is essential to maintaining legal compliance and a competitive edge. SAP has strict policies, standards, and procedures regarding all activities associated with how employees, contractors, and third-party vendors approach information-processing environment of SAP solutions.

In addition to its high security standards, SAP Cloud documents critical processes to help ensure consistent, predictable results. The importance of information security is reflected in the standards of SAP and in the company's requirement that all employees acknowledge in writing that they understand their roles and responsibilities regarding information security.

Security education and awareness

Around the globe, some of the biggest data leaks have been the result of social engineering or simple carelessness. Employees who unwittingly give access to confidential data—through lost or stolen laptops left unencrypted—have caused some of the largest data leaks of all time. Ongoing security training for all employees about the latest scams, periodic reviews of security policies, and signed acknowledgments that the employees have read and understand the policies contribute to keeping information security top of mind.

At SAP, security responsibilities are addressed throughout a person's tenure with the company to help ensure that employees, as well as contractors and third-party vendors, understand their responsibilities. SAP involves all employees, contractors, and third-party vendors in annual security awareness training.

Compliance standards

Cloud solutions from SAP comply with the latest standards, including [2,3] :

- All policies based on ISO 27002
- Applications tested to Open Web Application Security Project (OWASP) standards
- Infrastructure hardened to Center for Internet Security (CIS) standards
- U.S. government Federal Information Security Management Act of 2002 (FISMA) accreditation (OPM/DHS/NTIS) for certain SaaS offerings
- PCI certified in certain areas and for various SaaS offerings
- SSAE 16 SOC 2 auditing every year
- SSAE 16 SOC 2 or ISO 27002 certification for the SAP data center
- Safe Harbor certification
- BS 10012 standard for the management of personal information

SAP Cloud has established agreements internally that permit the company to manage data using all of its resources globally. All contracts with sub-processors include appropriate provisions to ensure that SAP adheres to all of the European Union data privacy requirements.

Conclusion

As malicious software, identity theft, and online system exploitation threaten today's computing environments, securing sensitive corporate data has never been more imperative. Government regulations require—and end users demand—higher levels of security, yet businesses struggle to implement a sound security infrastructure that protects them from existing and emerging threats.

At SAP, a seasoned team of industry experts who specialize in creating secure, reliable environments will help you save on IT staffing and build-out costs to safeguard your critical applications and data while keeping your business operations intact. We relentlessly focus on security—so you don't have to.

Our comprehensive approach—at the physical, database, middleware, application, and network and communication layers—literally builds security into every aspect of the business. In fact, SAP works to help companies around the globe achieve the best possible business results, with solutions that incorporate the latest research, the smartest technology, and the most secure systems on the planet. Providing a safe yet highly accessible environment is something that many corporate "behind-the-firewall" implementations are struggling to achieve. The ability of the company to offer applications that are affordable, configurable, and secure makes SAP the industry leader.

2 ByDesign is BS10012, SSAE 16 SOC 2 and PS880 German GaaP certified
3 Hana Enterprise Cloud is in the certification process for SSAE 16 SOC 1 and SOC 2 (both Type I). Effectiveness of controls will be reviewed and certified with ISAE3402/SOC 1 and SOC 2 (both Type II) beginning of 2014.

About SAP

SAP is at the center of today's technology revolution, developing innovations that not only help businesses run like never before, but also improve the lives of people everywhere. As the market leader in enterprise application software, we help companies of all sizes and industries run better. From back office to boardroom, warehouse to storefront, desktop to mobile device—SAP empowers people and organizations to work together more efficiently and use business insight more effectively to stay ahead of the competition. SAP applications and services enable more than 248,500 customers to operate profitably, adapt continuously, and grow sustainably. For more information, go to www.SAP.com.

The Best-Run Businesses Run SAP™