

SAP Security Concepts and Implementation

The Security Development Lifecycle at SAP

How SAP Builds Security into Software Products



The Best-Run Businesses Run SAP™

Table of Contents

4 Integrating Security Right from the Start

4 Establishing a Standard for Product Security

5 Quality Gates

5 Regulatory Compliance

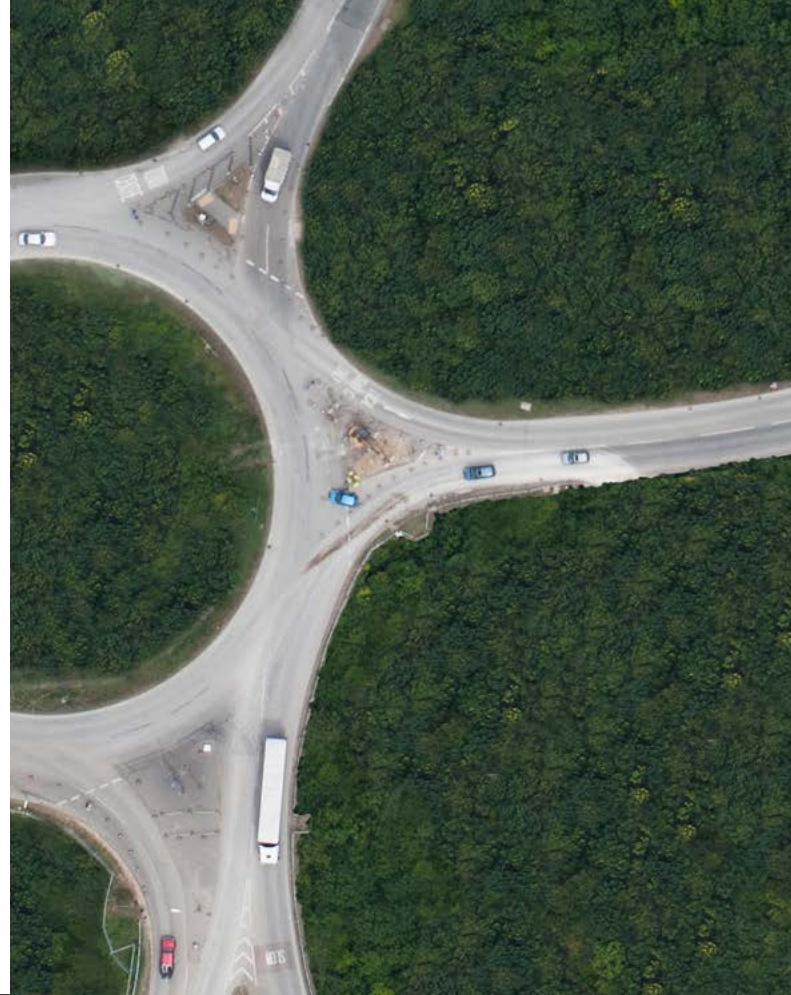
5 Testing During Development

5 Product Security Consulting

6 Product Security Education and Training

6 Threat Modeling

6 Find Out More





Developing secure software requires a strategy that covers not just the entire product lifecycle but the product's complete investment program as well, starting with product concept and embracing design, development, and even shipment. Postdelivery, SAP continues to protect its software by providing security patches, so customers can **mitigate the latest-breaking challenges to software security.**

SAP builds security into its software right from the beginning. Because the strategy to achieve and maintain security in SAP® software is so thorough and so well conceived, SAP customers can:

- Know they are running business processes on products that have been carefully tested
- Benefit from stable, secure software today and in the long run
- Achieve sustained regulatory compliance
- Rely on a group of world-class security experts professionally dedicated to managing product security at SAP



Integrating Security Right from the Start

Even the most effective security measure will fail to deliver on expectations if it is implemented poorly. High-quality code is the most important basis for building secure products. To address this key issue, SAP approaches product security holistically to make sure there is no missing link. And the security development lifecycle in place at SAP makes sure product code is of the highest quality.

ESTABLISHING A STANDARD FOR PRODUCT SECURITY

SAP employs a framework for product development to enforce a standard for achieving high product security and quality. The framework covers all organizational phases associated with product investment, from the initial decision to create the product to project execution and postdelivery. The framework is designed to see that security is built right into the software

so that all security and privacy requirements are fulfilled. The set of requirements is not static, however. It is updated on a continual basis from information provided by public sources dedicated to ferreting out and publishing software vulnerabilities. Just some of these sources include Common Weakness Enumeration (CWE), a software community that maintains a catalog of detected software vulnerabilities; Common Vulnerabilities and Exposures (CVE), a database of documented computer security weaknesses; SANS Institute; and Open Web Application Security Project (OWASP), an open-source Web application project.

The product standard for security at SAP is based on SAP's long tradition of building reliable and secure software. The standard encompasses a wide range of methodologies and measures, such as threat modeling, security assessment, security consulting for development teams, and training.





The product standard for security at SAP is based on SAP's long tradition of building reliable and secure software.

Quality Gates

SAP products in development undergo checks at specific points called quality gates (Q-gates). These are mandatory milestones that occur at each major stage in the development of a product. Not only is the quality of the software product assessed at these Q-gates, but the product must pass each Q-gate before it can move on to the next lifecycle phase. Q-gates verify the functionality and security of a product, along with performance and usability.

Regulatory Compliance

SAP has governance policies in place to oversee that whatever work is performed during the security development lifecycle complies with applicable legal requirements. These policies also require that each SAP software product meets all applicable legal regulations in the markets to which the software is to be shipped.

Testing During Development

Source code reviews, architecture audits, penetration tests, and security source code scans (static analysis) are integral parts of the security development lifecycle at SAP. SAP runs a scalable test infrastructure that seamlessly integrates with product development. This infrastructure ensures that every product is thoroughly tested before it is released.

Product Security Consulting

A team of world-class security experts helps product teams understand, address, and resolve complex security issues. This highly specialized internal security consulting enables SAP product teams to get architectures right from the outset and helps them eliminate potential security issues early on in the development process – before any code is committed.





Product Security Education and Training

Awareness drives improvement. Security consulting plus in-depth training are key elements for enabling the development community at SAP to build and maintain secure software. In addition to developers, the vast majority of customer-facing people at SAP are familiar with the security “big picture” at SAP.

Threat Modeling

SAP introduced a refined threat modeling process within its security development lifecycle. Threat modeling is a proven method for achieving high product security. In addition, threat modeling provides tangible economic advantages by enabling developers to find and eliminate design issues at an early stage.

Find Out More

To learn more about the framework SAP uses to achieve world-class product security, please contact your SAP representative.



© 2013 SAP AG or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries.

Please see <http://www.sap.com/corporate-en/legal/copyright/index.epx#trademark> for additional trademark information and notices.



The Best-Run Businesses Run SAP™