Überblick der 10 Goldenen Regeln für die beteiligten, unterschiedlichen Rollen im Softwarelebenszyklus

Nr.	Analyst/Auftraggeber	Planer (Architekt)	Entwickler	Tester	Projektleiter
1	Denken Sie über geschäftliche Konsequenzen von IT-Sicherheitsfragen nach	Nutzen Sie die Erfahrung von anderen: Erfinden Sie Schwachstellen nicht neu Entwickeln Sie keine eigenen Sicherheitsfunktionen! Internationale Sicherheitsstandards (technische Standards)	Misstrauen Sie jeder (Benutzer-) Eingabe (Validate Input)	Testen Sie priorisiert Hauptangriffspunkte	Sie sind verantwortlich für die Umsetzung aller Anforderungen, lesen Sie zunächst also alle anderen "Goldenen Regeln"
2	Berücksichtigen Sie gesetzliche und regulatorische Anforderungen	„Minimale Rechte"-Prinzip, Berechtigungskonzept erstellen	„Minimale Rechte"-Prinzip	Machen Sie Code-Reviews	Fordern Sie die fachlichen Sicherheitsanforderungen ein
3	Definieren Sie fachliche Rollen, Zuständigkeiten und Prozesse	Trust Zones: Welchen eingehenden Daten darf vertraut werden und welchen nicht	Keine unnötige Veröffentlichung von internen Daten! (Sanitize Output)	Machen Sie Regressionstests (einmal behobene Fehler sollen zukünftig nicht mehr auftauchen)	IT-Sicherheit gleich von Beginn an, nicht erst am Ende oder hinterher
4	Berücksichtigen Sie auch Anforderungen an die Nachvollziehbarkeit	Machen Sie es einfach!	Nutzen Sie die Erfahrung von anderen (do's und dont's) • Erfinden Sie Schwachstellen nicht neu • Entwickeln Sie keine eigenen Sicherheitsfunktionen!	Binden Sie externe Sicherheitsexperten mit ein (für Schwachstellentest und/oder –reviews)	In allen Projektphasen gibt es Arbeitspakete für IT-Sicherheit
5	Verfügbarkeit und Business Continuity können spezielle Anforderungen sein	Niemals „Security by Obscurity"	Sichere Einstellungen • Sichere Voreinstellungen • Alle Benutzerkennungen, Passwörter und Verschlüsselungsschlüssel änderbar! • Machen Sie es einfach! • Sicherheitsdokumentation	Nutzen Sie vorhandene Testfälle und Tools	Planen Sie hinreichende Ressourcen für IT-Sicherheit
6	Sicherheitsanforderungen sollten bekannt, vereinbart und fixiert sein	Sichere Voreinstellungen	Niemals „Security by Obscurity" und niemals „Hintertüren" • „Security by Obscurity" • Keine „Hintertüren"	Testen Sie funktionale Sicherheitsanforderungen	Vergessen Sie nicht Ihre (Projekt-) Mitarbeiter, planen Sie Sensibilisierung und Know-How
7	Die Erfüllung von Sicherheitsanforderungen sollte abnahmerelevant sein	Machen Sie einArchitekturreview	Gute Fehlerbehandlung (Fail securely)	Testen Sie auf Schwachstellen	Nutzen Sie Standards, sichere Komponenten und existierende Erfahrungen
8	Beachten Sie Restrisiken und treffen Sie ggf. Vorkehrungen	Mehrere Sicherheitshürden (Defense in Depth)	Denken Sie an Nachvollziehbarkeit (Trace, Audit, Logs)	Erstellen Sie einen Testplan	Bewahren Sie Handlungsspielraum für mögliche Veränderungen
9	Vergessen Sie nicht Ihre eigenen Prozesse, organisatorischen Maßnahmen und Leute	Rechtliche Anforderungen beachten Datenschutz ermöglichen Machen Sie alles nachvollziehbar (sofern sinnvoll)!	Machen Sie Code-Reviews	Führen Sie Sicherheitstests nicht gleichzeitig mit fachlichen Tests durch	Machen Sie Restrisiken transparent und lassen sich diese abzeichnen
10	Alles kann sich ändern, seien Sie darauf vorbereitet	Rechnen Sie mit Schwachstellen: sehen Sie Patches vor	Rechnen Sie mit Schwachstellen: sehen Sie Patches vor	Sehen Sie für alle ("normalen") Testfälle Negativbeispiele vor	Denken Sie an diejenigen, die später mit dem Produkt umgehen müssen

Aus *Die 10 goldenen Regeln der IT-Sicherheit*, Commerzbank / SAP, http://www.secologic.org/downloads/software/070205_10GoldenRules_SAP_CoBa_V1.pdf
Weitere Best Practices, White-Paper und Tools zur Entwicklung sicherer Webanwendungen finden Sie auf den Seiten des Secologic Projekts http://www.secologic.org

COMMERZBANK
Bundesministerium für Wirtschaft und Technologie
SAP