

APPLICATION SECURITY MANAGEMENT NACH ISO 27034



CeBIT 17.03.2015



HERZLICH WILLKOMMEN



**„ Applikationssicherheit beginnt
lange bevor auch nur eine Zeile
Code geschrieben wurde“**

Ulrich Heun

Geschäftsführender Gesellschafter der CARMAO GmbH

Vorstand des Kompetenzzentrum für Sicherheit in Bayern (KoSiB)

● Beratung, Dienstleistungen und Know-how-Transfer



Information Security



Information Risk



Compliance/Datenschutz



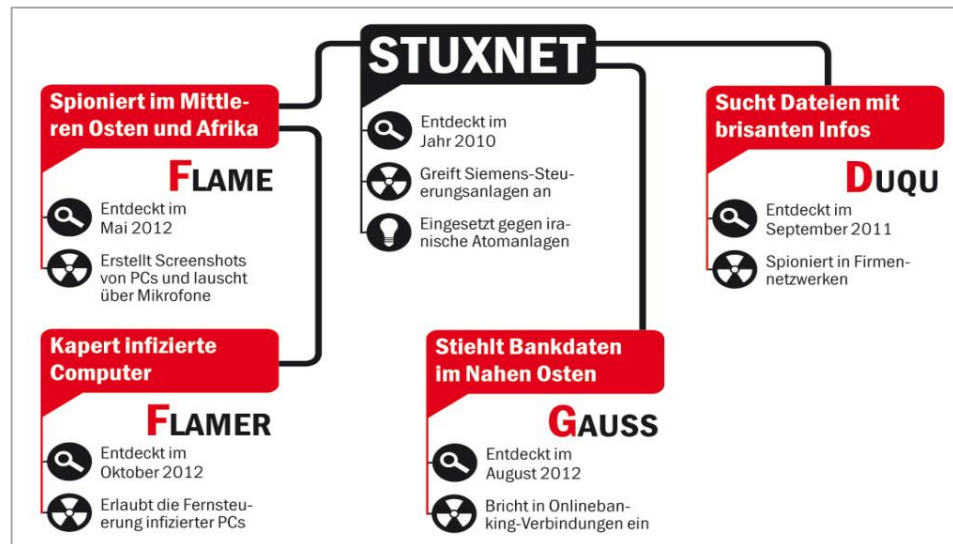
Business Continuity / IT-SCM / Notfallmanagement

Weitere Informationen auf www.carmao.de.

APPLICATION SECURITY MANAGEMENT



Quelle: ICT Kommunikation



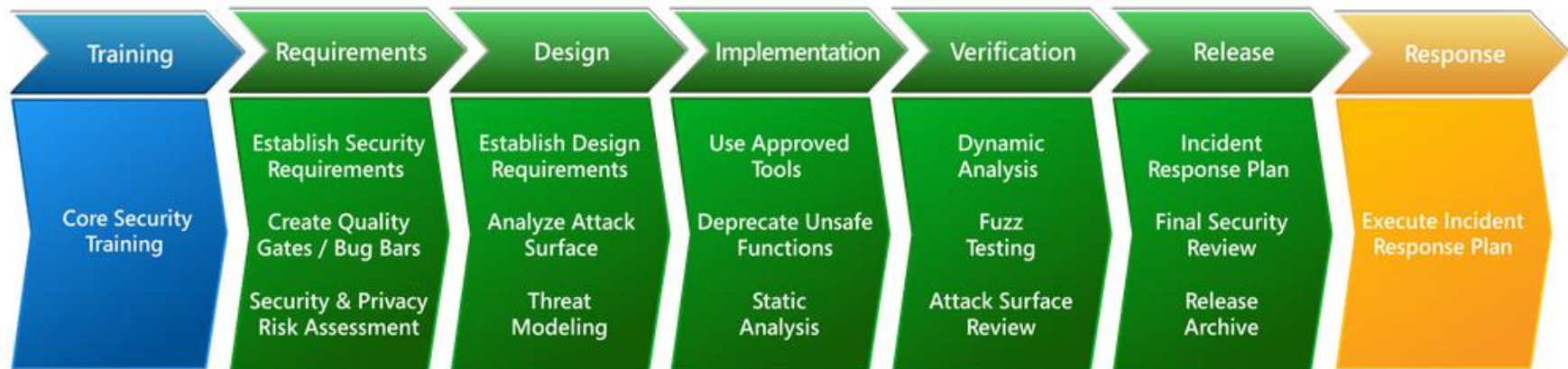
Quelle: Computerbild

- Focus der Softwareentwicklung
 - Funktionalität
 - Kostenoptimierung
- Herausforderung
 - Sicherheitslücken werden oft erst im Einsatz erkannt
 - Kritische Sicherheitslücken müssen immer sehr schnell und unter Zeitdruck behoben werden
 - Nachträgliche Korrekturen kosten in aller Regel sehr viel Geld
- **Fazit:**

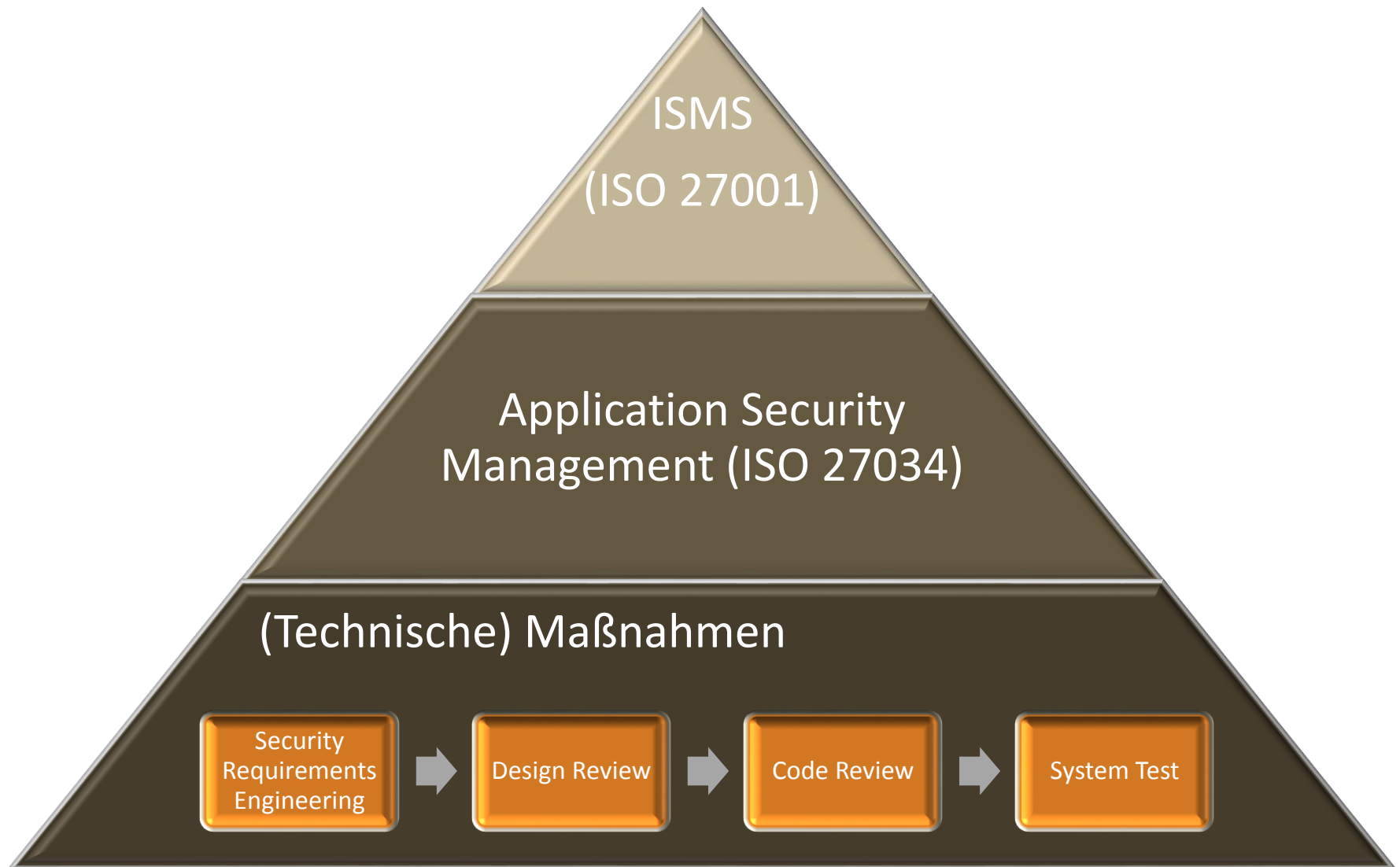
Sicherheitsanforderungen müssen wie funktionale Anforderungen von Beginn an berücksichtigt und im gesamten Application Lifecycle systematisch gemanaged werden

- Bisherige Ansätze
 - Microsoft SDL
 - Common Criteria
 - Open Software Assurance Maturity Model (SAMM)
 - OWASP Software Security Assurance Process
 - OWASP CLASP
 - Software Security Framework
 - Team Software Process for Secure Software Development
 - Security by Design with CMMI for Development
- Zum Teil deckungsgleich

- 7 Phasen
 - Softwarelifecyclophasen
- 17 Practices
 - Konkrete Sicherheits-Aktivitäten
 - Verteilt auf den gesamten Lifecycle



- Nachhaltigkeit
- Kostenersparnis
 - Schwachstellen in frühen Entwicklungsphasen leicht zu korrigieren
 - Kosten steigen exponentiell
 - Extremfall: Schwachstelle in fertigem Produkt (leider keine Ausnahme)
 - Vertragsstrafen, Regulatorische Strafen
- Reputation
 - Reputationsschaden durch ausgenutzte Schwachstellen
 - ⇒ Siemens mit Stuxnet
 - ⇒ OpenSSL mit Heartbleed
 - ⇒ ...
 - Mit gutem Beispiel vorangehen lohnt sich!



**INTERNATIONAL
STANDARD**

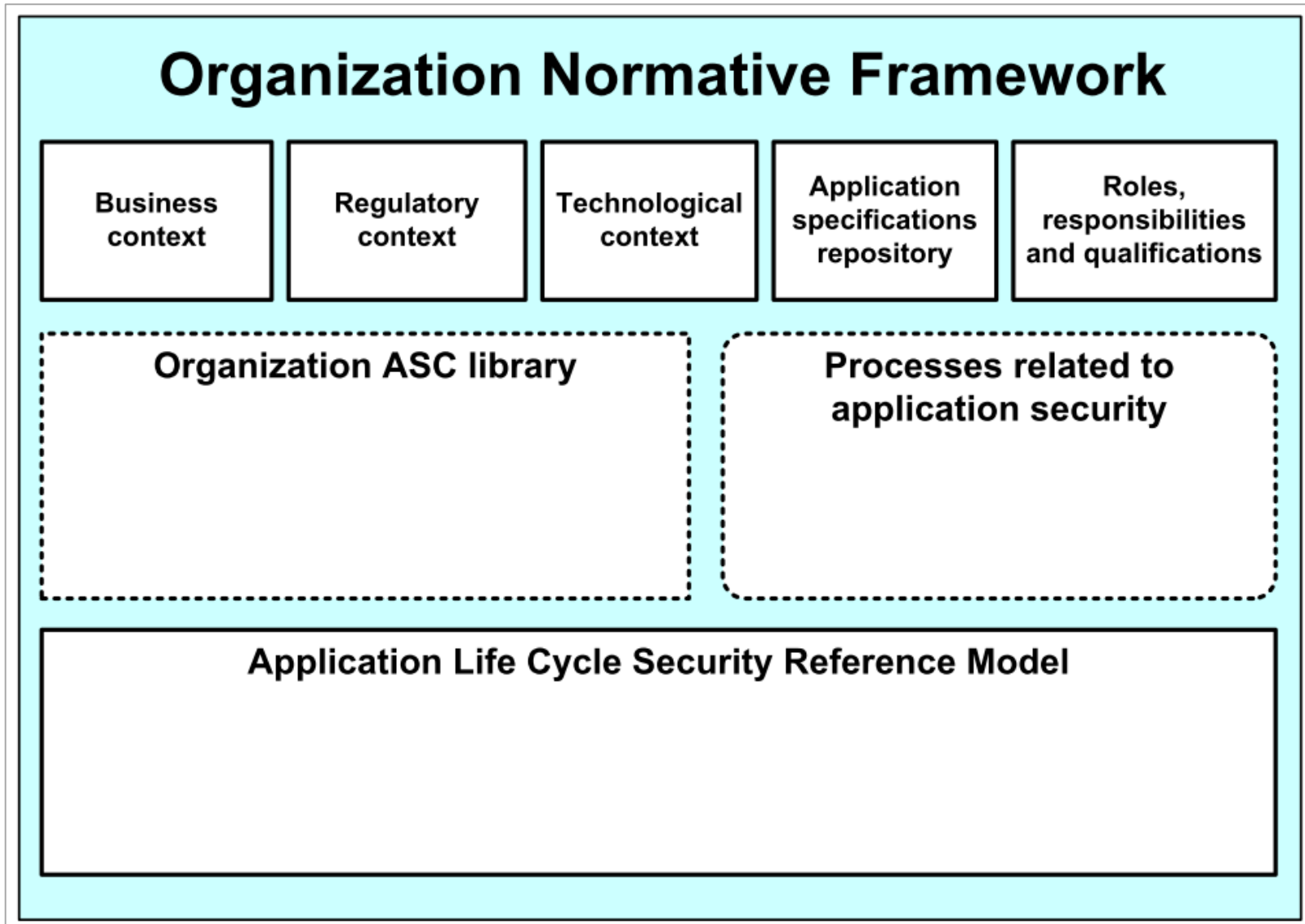
**ISO/IEC
27034-1**

First edition
2011-11-15

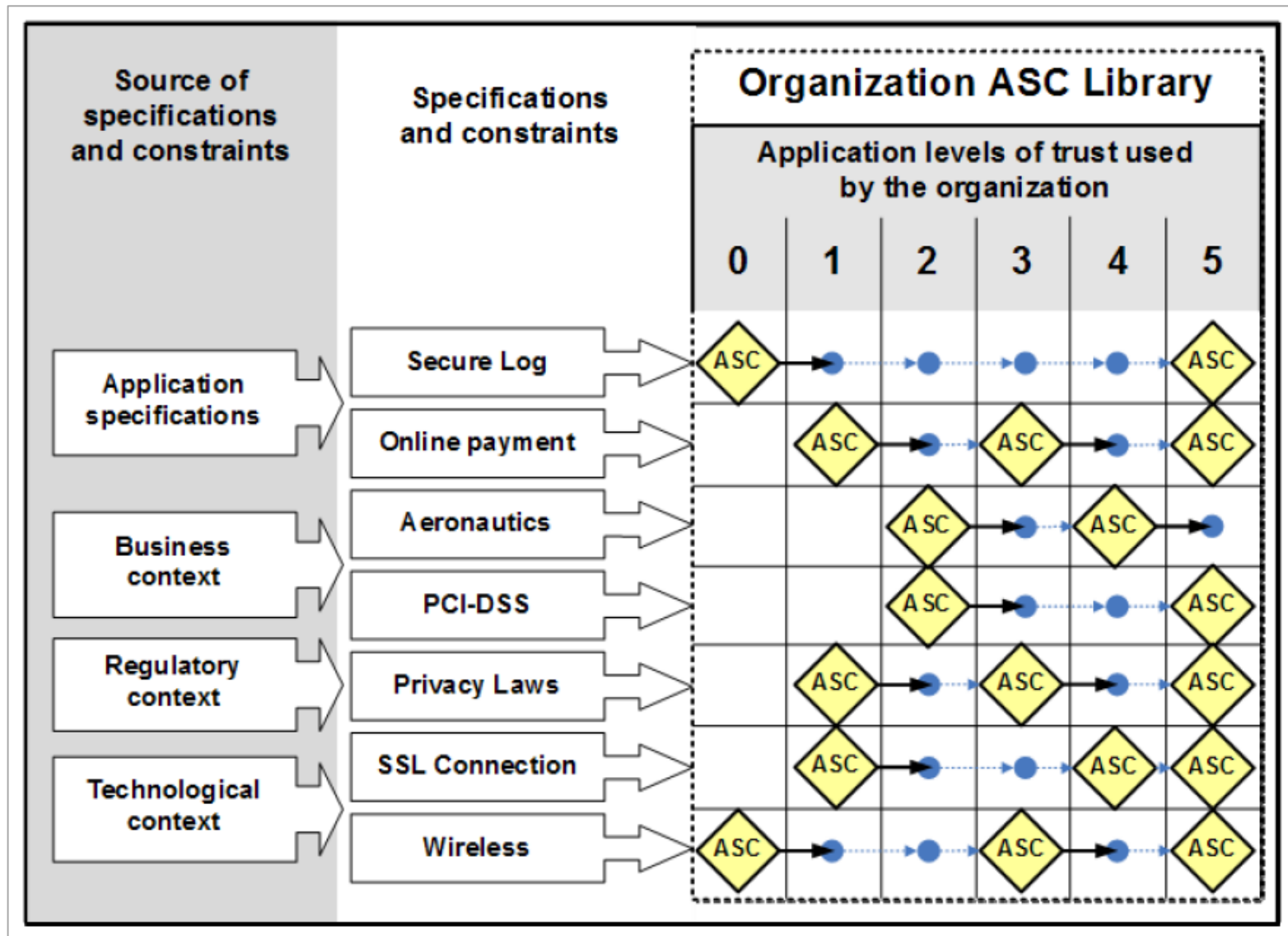
**Information technology — Security
techniques — Application security —
Part 1:
Overview and concepts**

- “Application security is a **process** performed to apply controls and measurements to an organization’s applications in order to manage the **risk** of using them.”
- Anforderungen und Maßnahmen betreffen den gesamten Application Lifecycle
 - Software
 - Daten
 - Technologie
 - Prozesse
 - Rollen

- 5 Teile
- Veröffentlicht:
 - Part 1: Overview and concepts
- In der Entwicklung
 - Part 2: Organization normative framework
 - Part 3: Application Security Management Process
 - Part 4: Application Security Validation
 - Part 5: Protocols and application security control data structure
- Geplant:
 - Part 6: Security guidance for specific applications

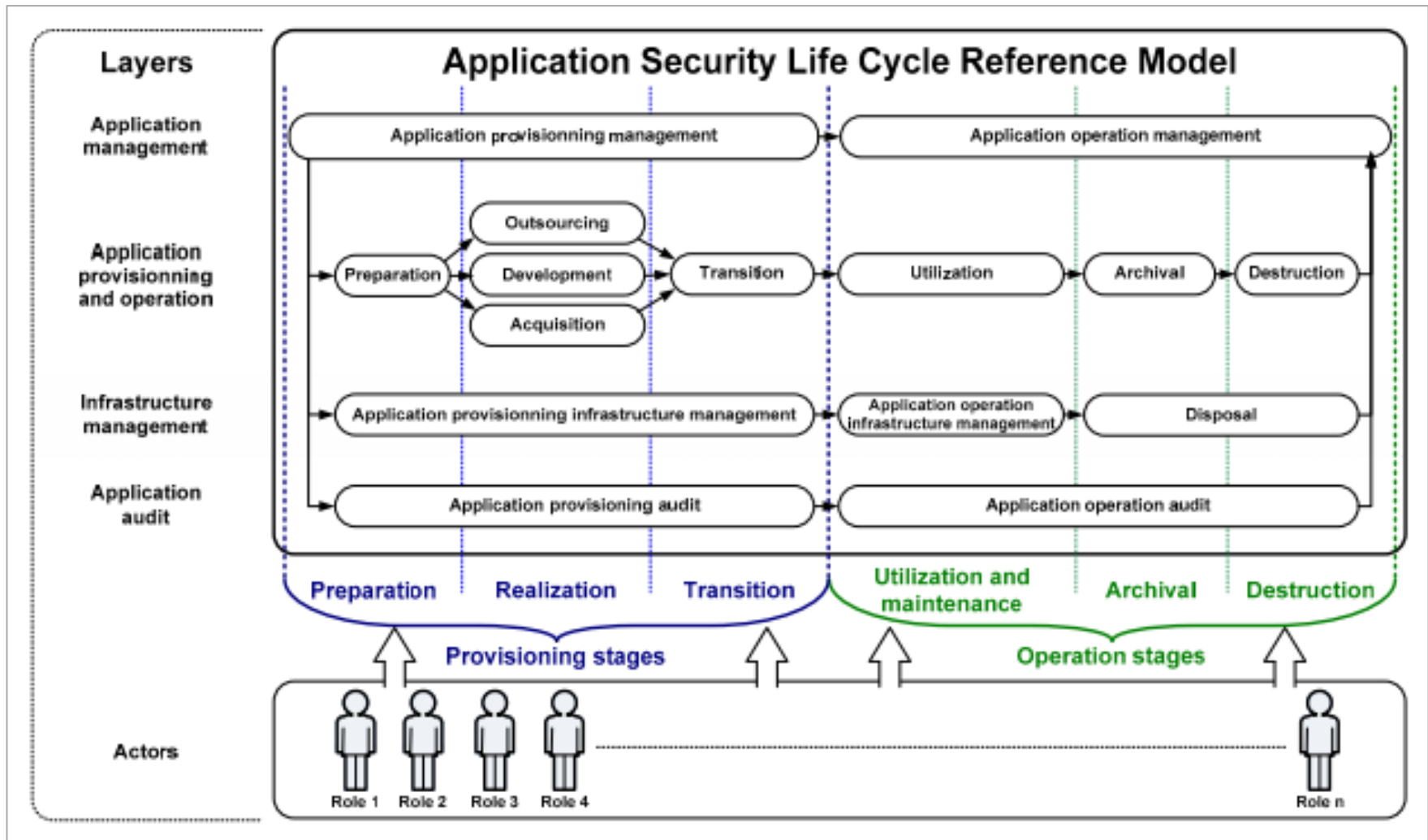


Quelle: ISO 27034

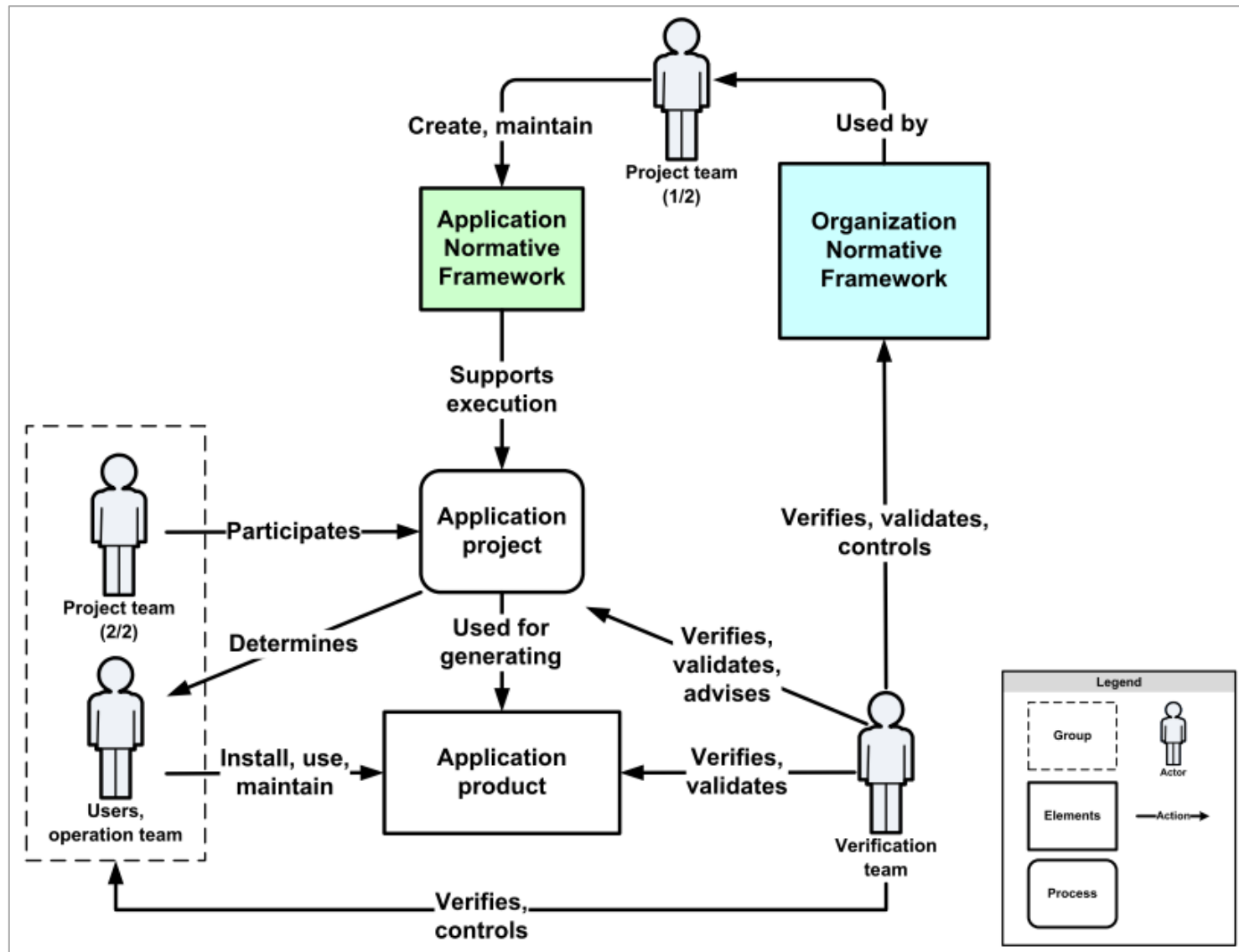


Quelle: ISO 27034

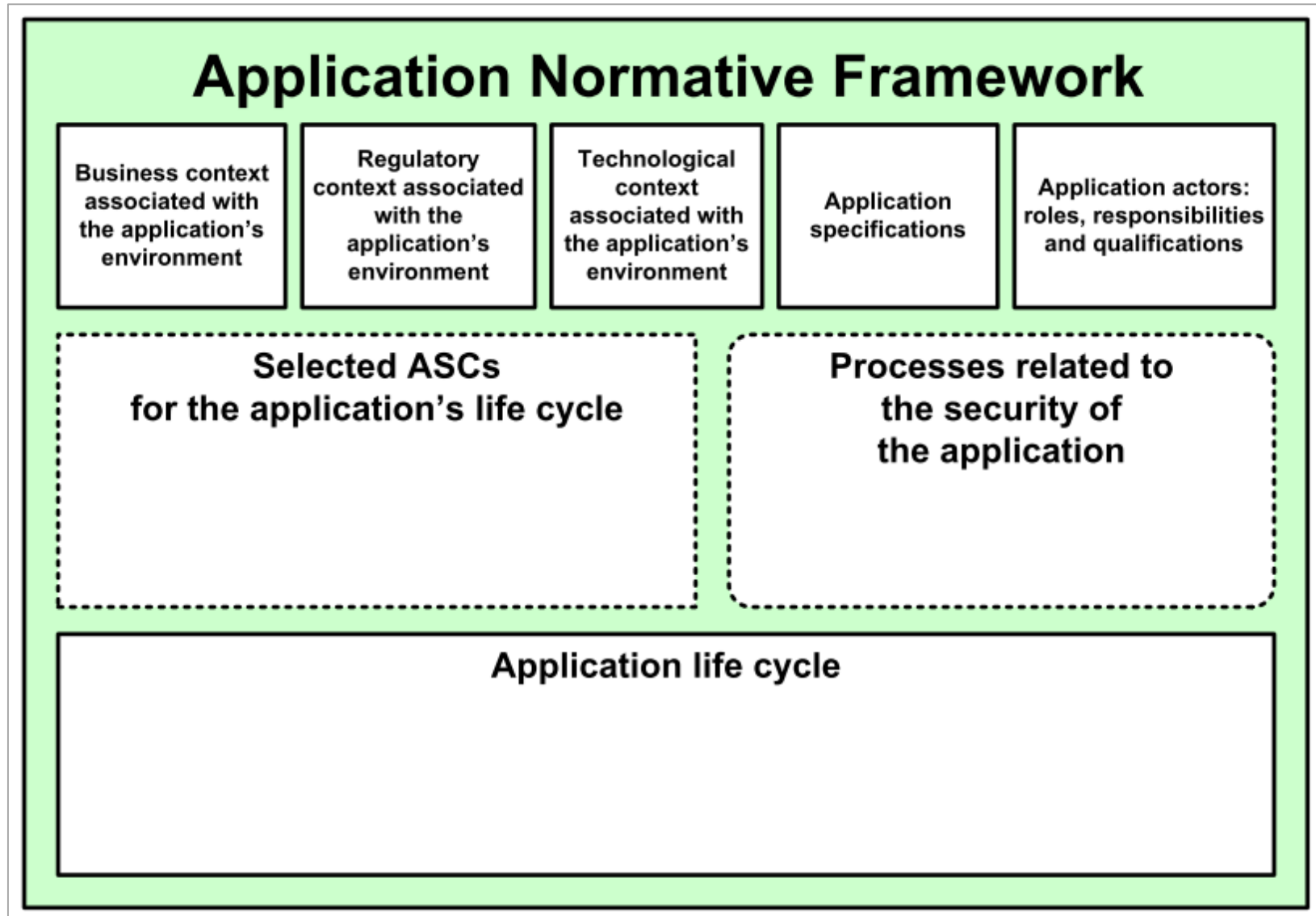
- Analog zu Controls nach ISO 27001
- Bestandteile
 - Security Activity
 - Verification Measurement
- ASC Generierung
 - Analyse vorhandener Applikationen
 - ⇒ Risikoanalyse
 - ⇒ Sicherheitsanforderungen
 - Ableitung aus Normen/Best Practices (ISO 15408, SAMM, ...)
- ASC Bibliotheken
 - https://www.owasp.org/index.php/OWASP_ISO_IEC_27034_Application_Security_Controls_Project
- Beispiel ASC:
 - Security Activity: Durchführen eines Design Reviews
 - Verification Measurement: Prüfung des Reviews durch Audit



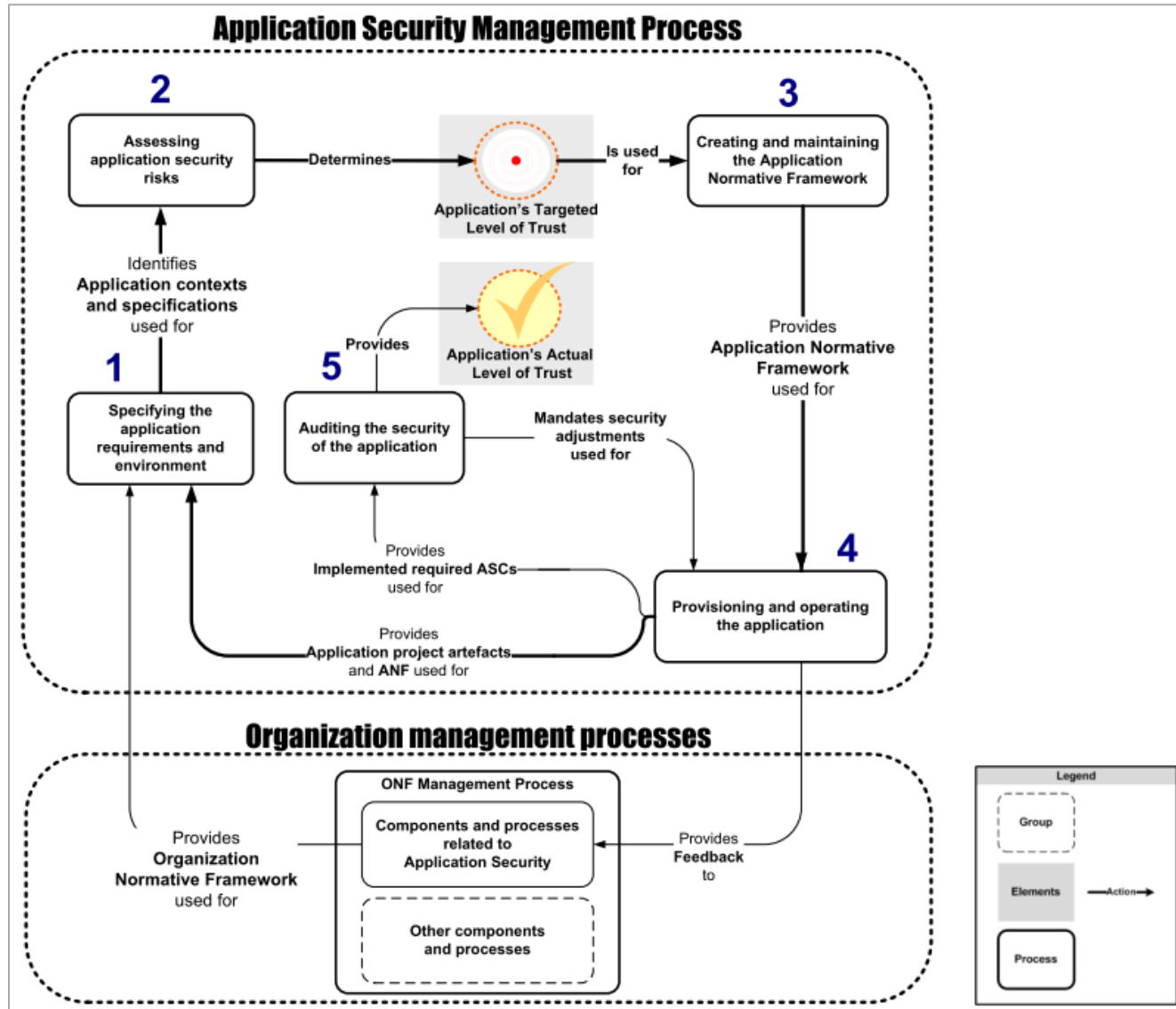
Quelle: ISO 27034



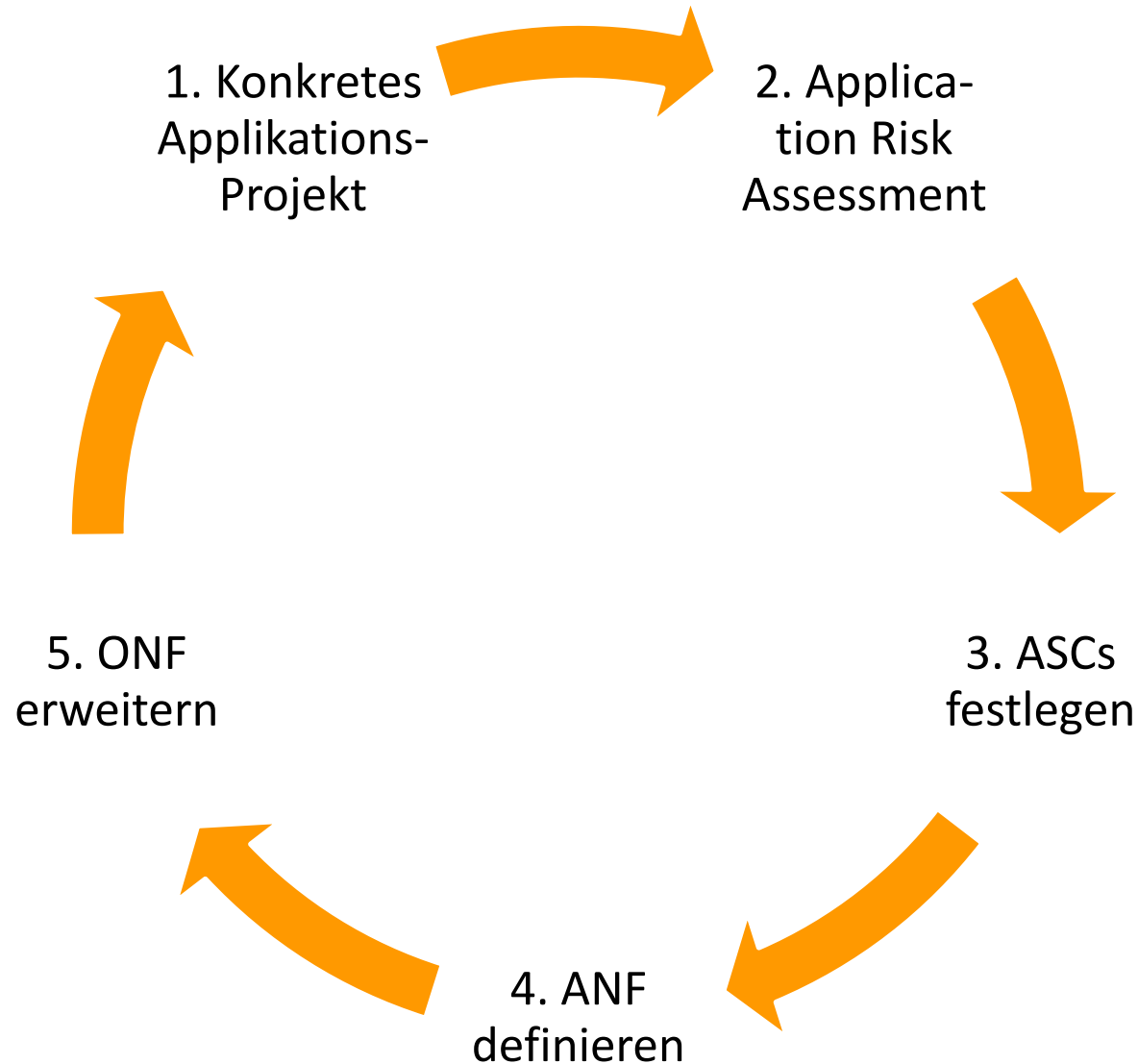
Quelle: ISO 27034



Quelle: ISO 27034



Quelle: ISO 27034



ISO 27034

- Sehr gute Integration in das ISMS nach ISO 27001
- Beschreibt ein Managementsystem zur Identifikation und Umsetzung von Application Security Controls
- Integriert existierende und bewährte Methoden zum Application Security wie Threat Modeling, Secure Code Analyse und Application Penetration Testing
- ASC-Kataloge in Vorbereitung (z.B. durch OWASP)



Rathausstraße 17
65611 Brechen

Fon +49 6438 9249-20
Fax +49 6438 9249-23
kontakt@carmao.de
www.carmao.de

Ihre **ERFOLGE** verdienen Achtung, Ihre **WERTE** verlangen Schutz!