Grundschutz++

Aufbau und Methodik

Bundesamt
für Sicherheit in der
Informationstechnik

Agenda

- Vision
- Methodik
- Ausblick

Bild: © AdobeStock/Liudmyla

Vision Grundschutz++

automatisier- und maschinenlesbar

definierend

Bewährte Inhalte, klarer formuliert und erklärt

prozessorientiert

messbar

anleitend

flexibel

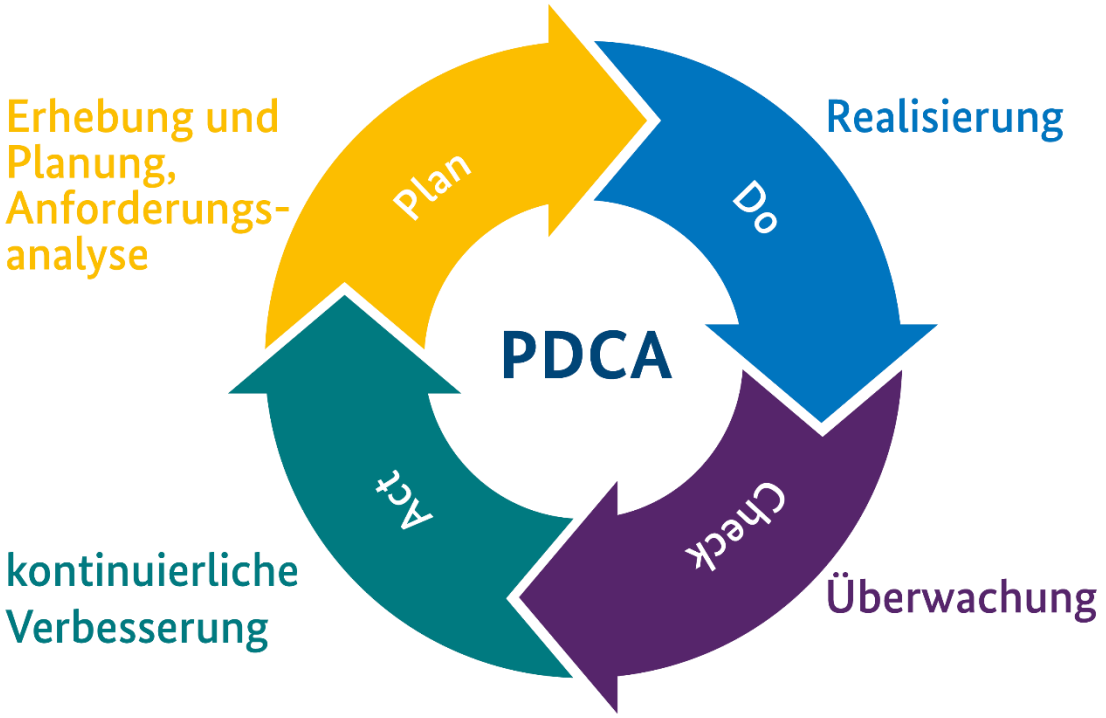
ISO27001 kompatibel

Methodik Grundschutz++

Methodik Grundschutz++

Der Sicherheitsprozess

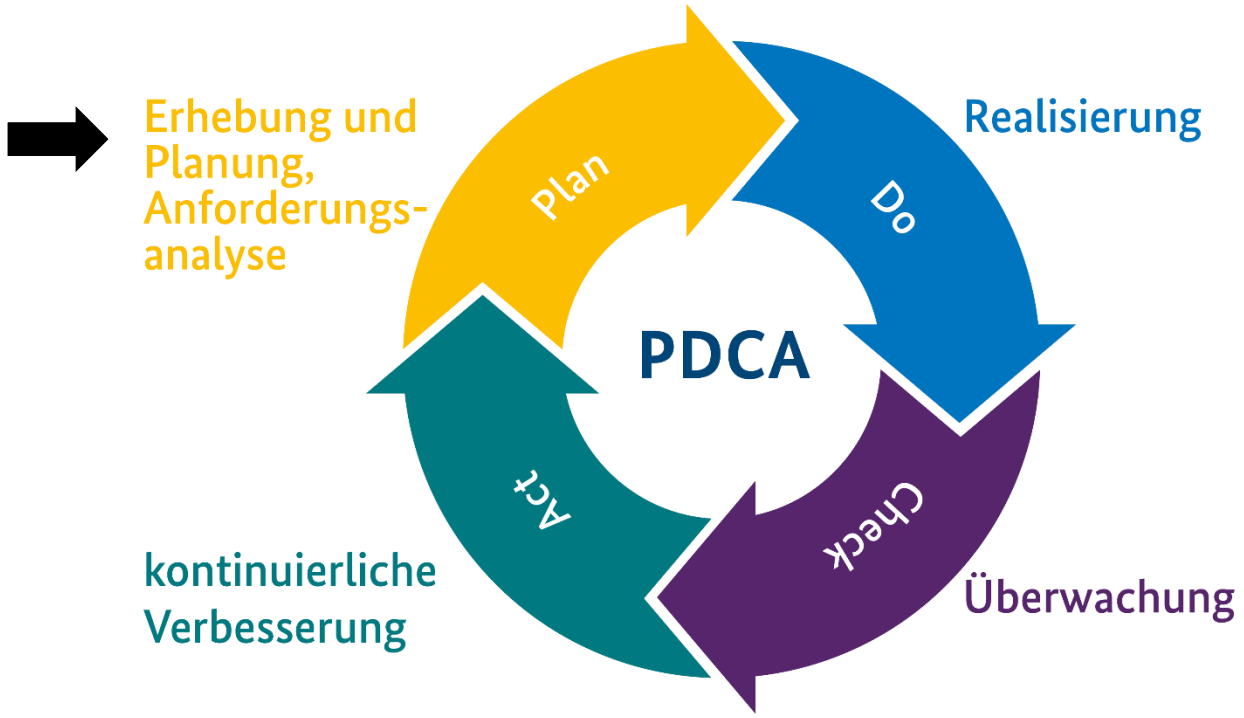
- fortwährend
- ganzheitlich
- PDCA-zyklisch
- prozessorientiert
- iterativ
- ISO27001 kompatibel
- zertifizierbar



Methodik Grundschutz++

Erhebung und Planung

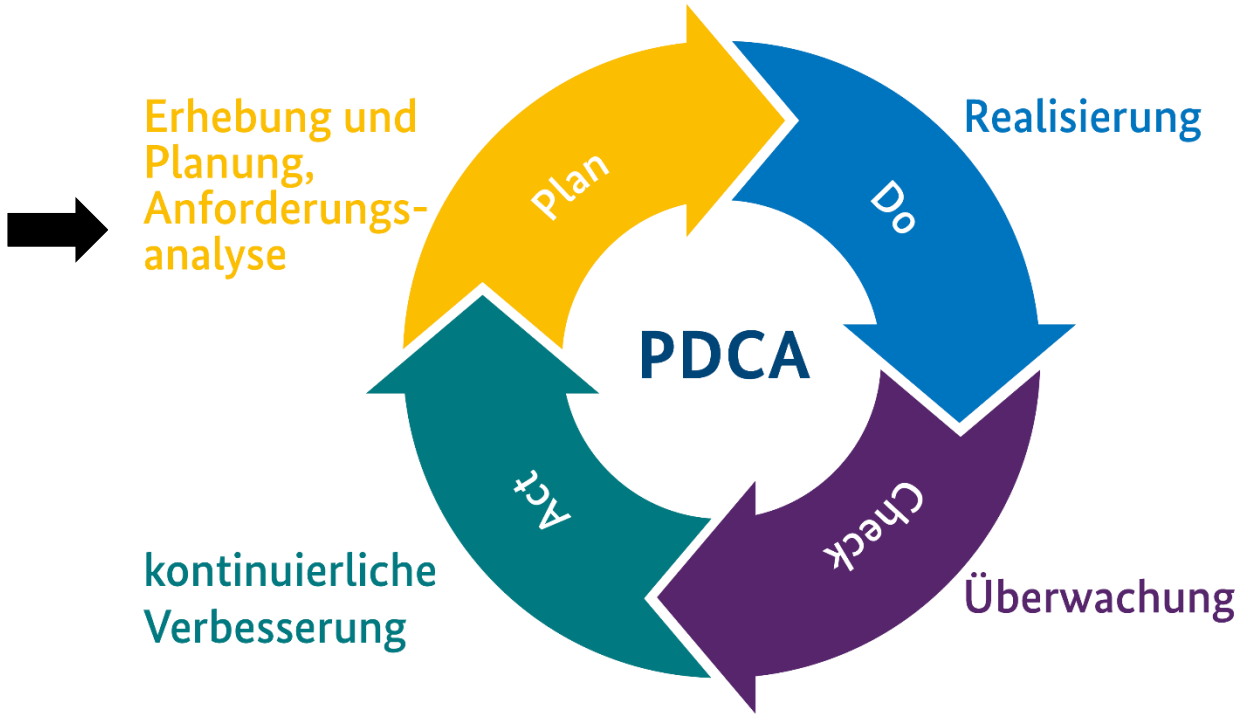
- Festlegung des Kontextes der Institution
- Analyse der interessierten Parteien
- Festlegung des Geltungsbereichs
- Identifizierung der Geschäftsprozesse
- Schutzbedarfsfeststellung
  - normal
  - hoch
- Entwicklung einer Informationssicherheitsleitlinie
- Implementierung des Compliance-Managements
- Festlegung von Rollen und Zuständigkeiten in der Sicherheitsorganisation
- Dokumentation und Kommunikation
- Festlegung und Freigabe der Vorgehensweise
- Initiierung des Risikomanagements



Methodik Grundschutz++

Anforderungsanalyse

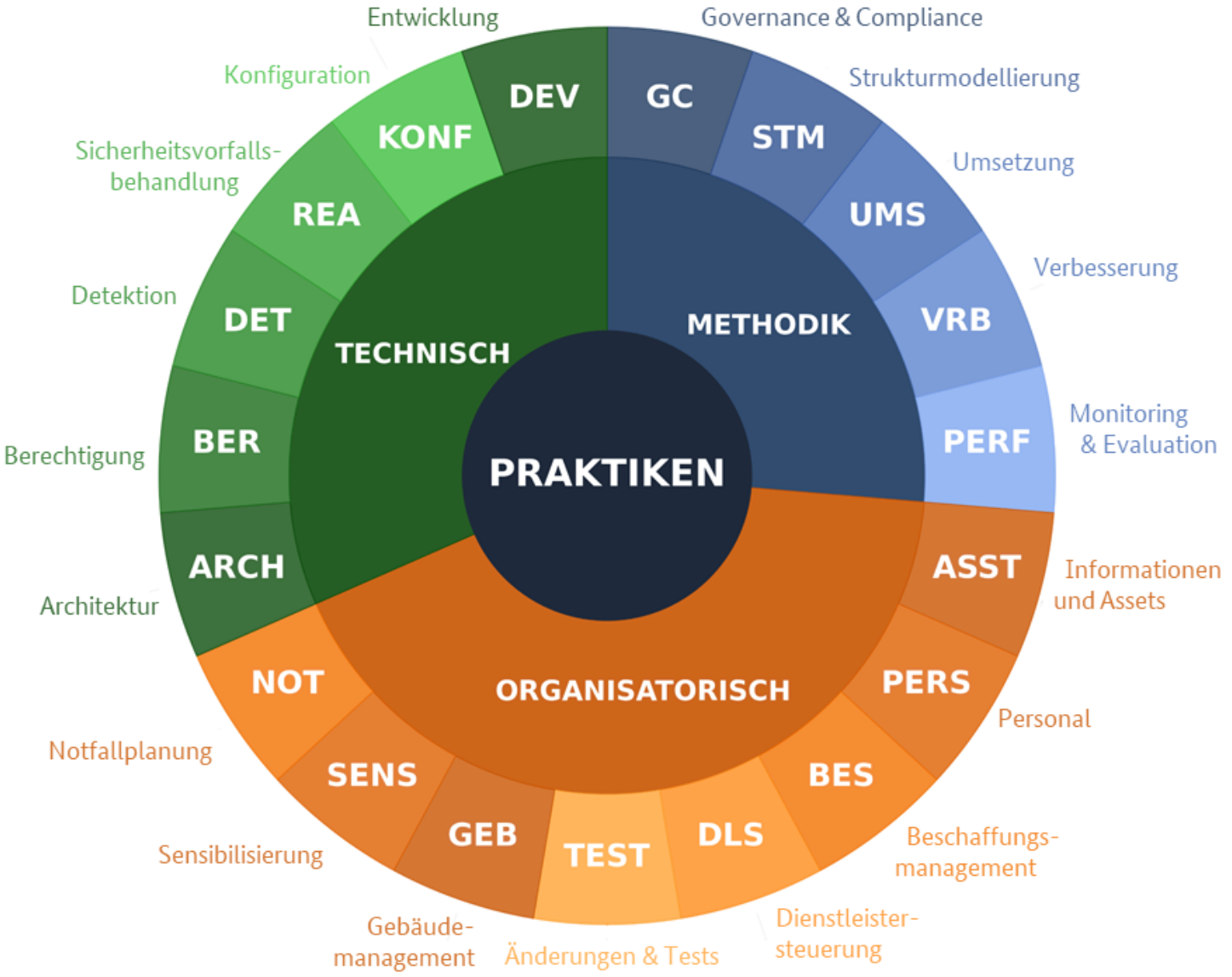
- Definition und Abgrenzung des Informationsverbunds
  - ➢ Assetanalyse
- Erstellung eines Anforderungspakets
  - ➢ Assetmodellierung auf die Zielobjektkategorien
- Ergänzung von Anforderungen
- Durchführung der Risikobetrachtung
  - ➢ Einstieg in die Risikobetrachtung
  - ➢ Ergebnisse fließen in das Anforderungspaket
- Gestaltungsentscheidung



Anforderungen im Grundschutz++

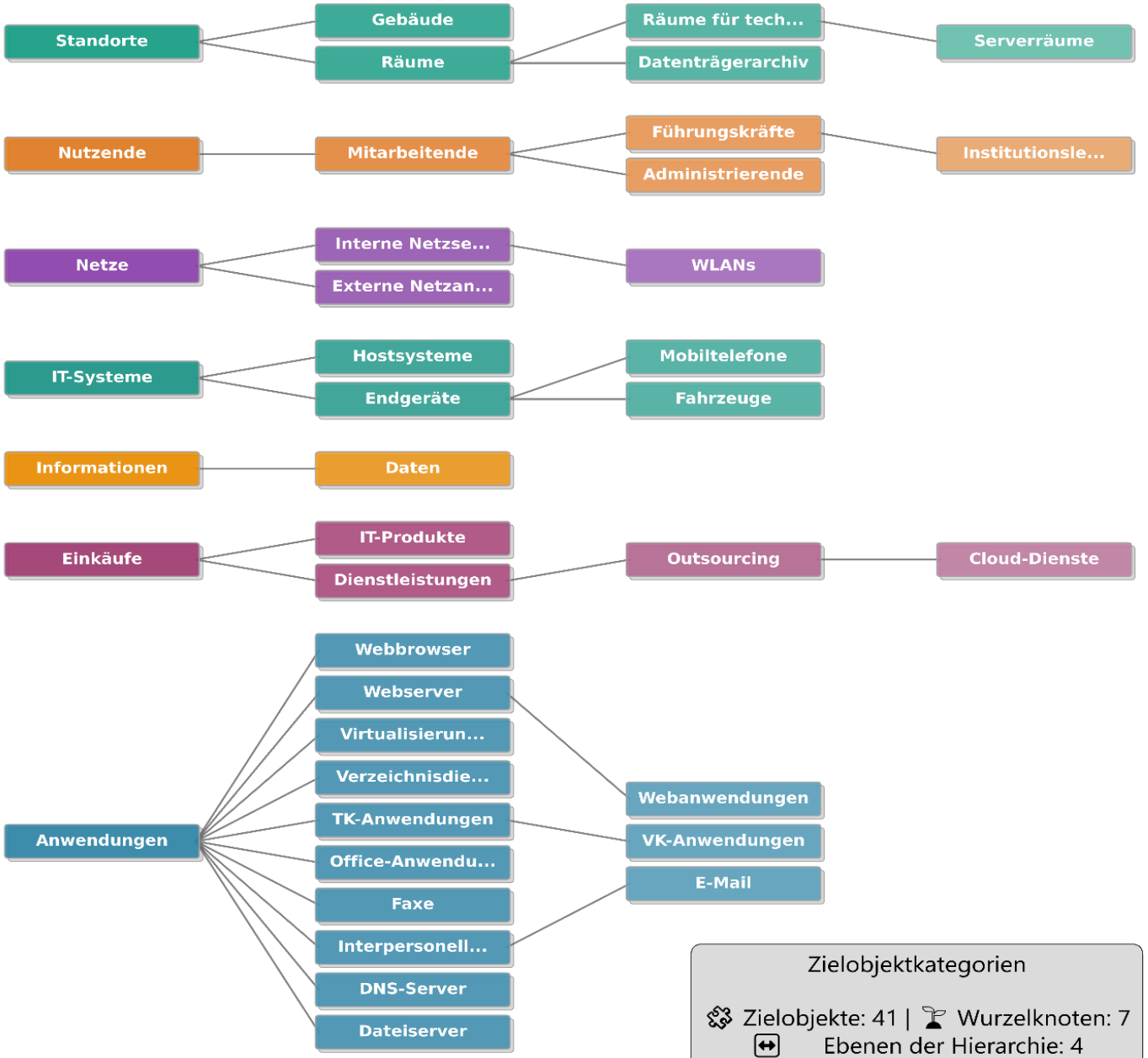
Anforderungen im Grundschutz++

Praktiken



Anforderungen im Grundschutz++

Zielobjektkategorien



Zielobjektkategorien

Zielobjekte: 41 | Wurzelknoten: 7
Ebenen der Hierarchie: 4
← Elternknoten | Kindknoten →
(Allgemein → Speziell)

Anforderungen im Grundschutz++

Beispiel

SENS.2.4 **Nutzung unautorisierter Assets** NORMAL-SDT AUFWAND 3

Sensibilisierung für Nutzende SOLLTE die Nutzung unautorisierter Assets untersagen.

▶ Hinweise

Die Nutzung unautorisierter Assets bezeichnet hier den Einsatz von IT-Systemen, Datenträgern, Anwendungen oder Cloud-Diensten, die nicht durch die Institution freigegeben und inventarisiert sind. Hierzu gehört auch der Anschluss privater Peripheriegeräte wie Tastaturen oder das Telefonieren mit nicht autorisierten Telefonen. Der Sinn und Zweck der Anforderung liegt darin, unkontrollierte Schatten-IT und damit verbundene Risiken zu reduzieren. So könnte etwa ein unautorisiertes USB-Gerät Schadsoftware einschleusen, oder eine nicht genehmigte Cloud-Anwendung könnte zu unbemerkten Datenabflüssen führen. Besteht ein Bedarf an Assets, dann können die festgelegten Meldewege genutzt werden. Bei der Beschaffung von Assets sind die Verfahren und Regelungen des Assetmanagements zu beachten.

Related Links (2)

REQUIRED ASST.3.11

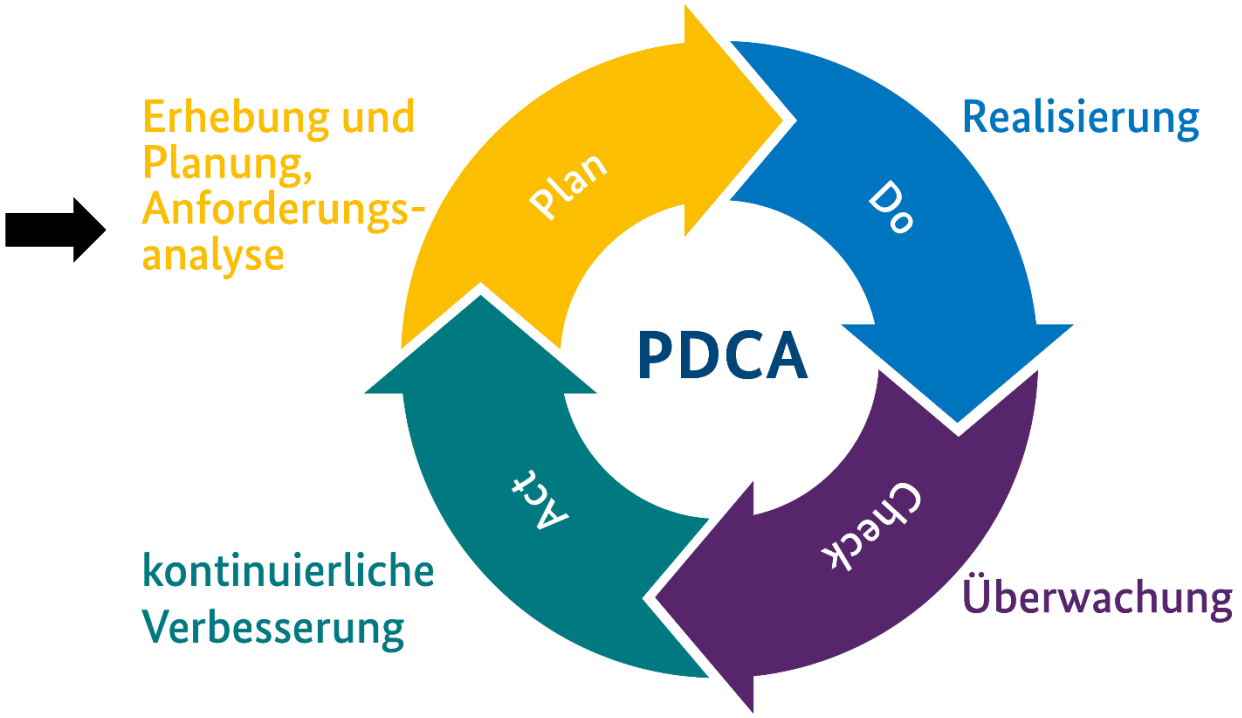
RELATED KONF.3.7

SENS.2.4.1 **Verbindung unautorisierter IT-Sys...** NORMAL-SDT AUFWAND 3

Methodik Grundschutz++

Anforderungsanalyse

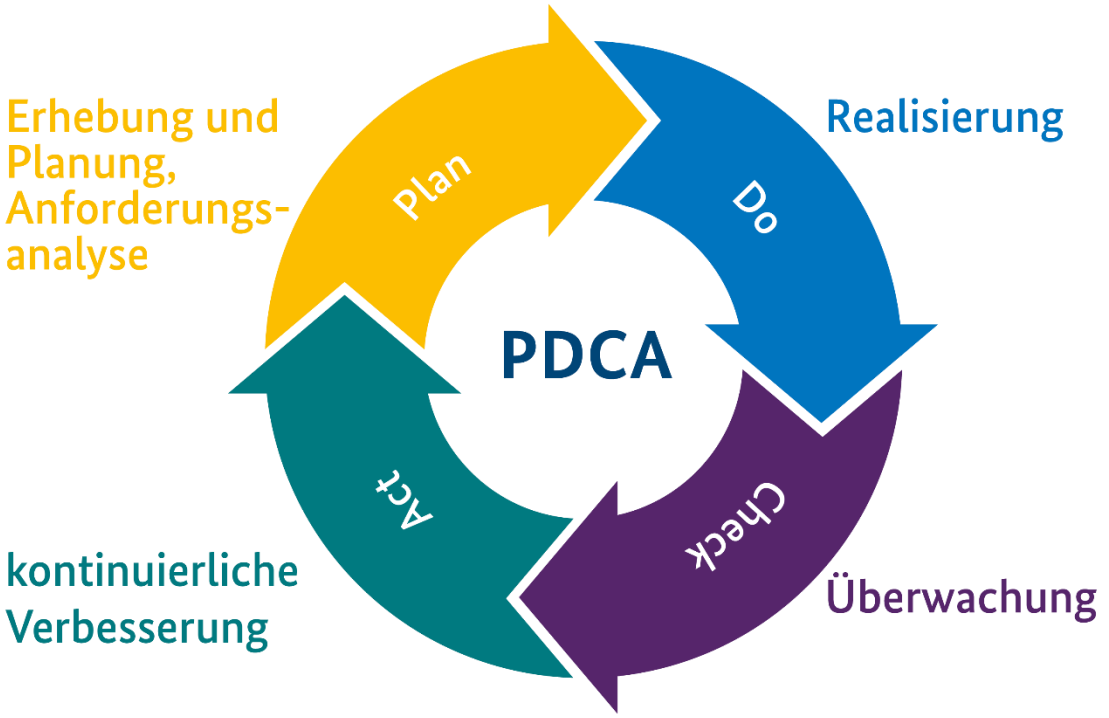
- Definition und Abgrenzung des Informationsverbunds
  - ➢ Assetanalyse
- Erstellung eines Anforderungspakets
  - ➢ Assetmodellierung auf die Zielobjektkategorien
- Ergänzung von Anforderungen
- Durchführung der Risikobetrachtung
  - ➢ Einstieg in die Risikobetrachtung
  - ➢ Ergebnisse fließen in das Anforderungspaket
- Gestaltungsentscheidung



Methodik Grundschutz++

Realisierung

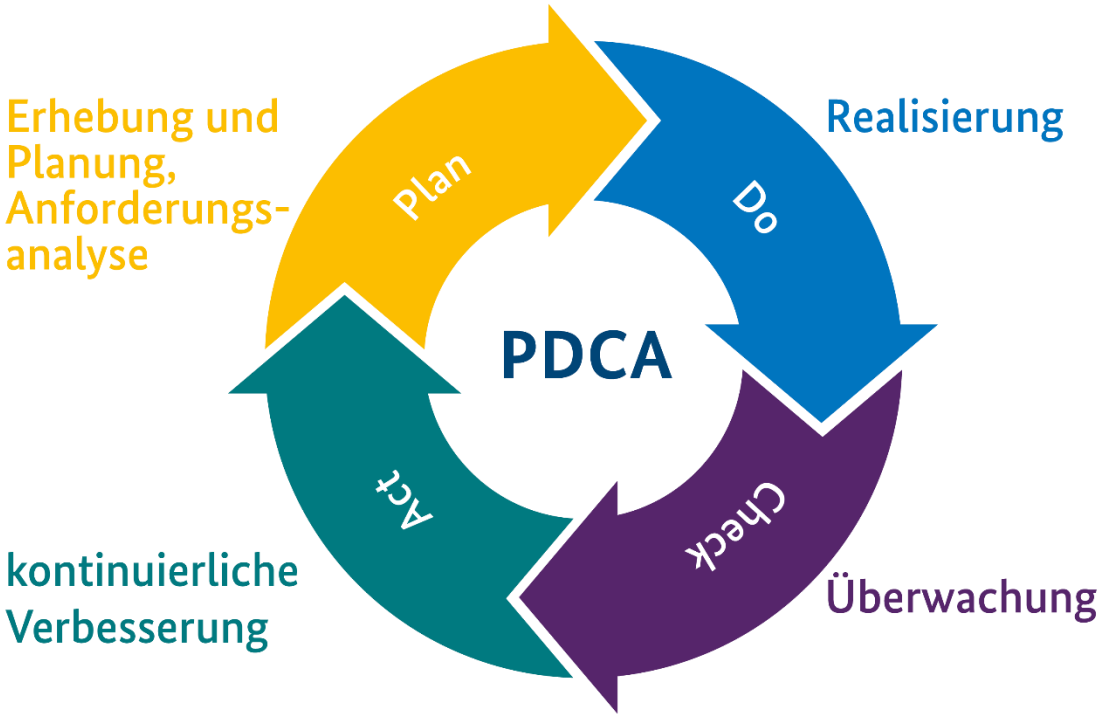
- Ermittlung des Umsetzungsstatus
- Bewertung fehlender Umsetzungen
- Umsetzungsplanung und Priorisierung
- Festlegung von Zuständigkeiten und Umsetzungsfristen
- Fortschrittsverfolgung



Methodik Grundschutz++

Überwachung

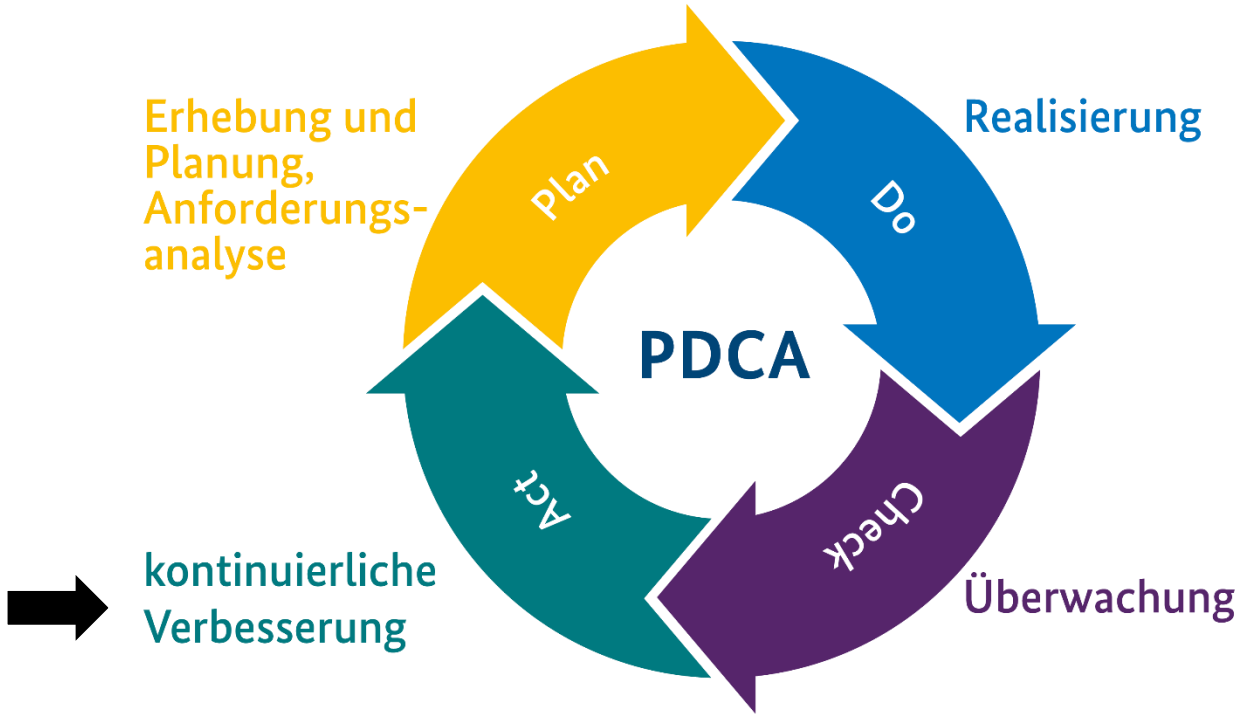
- Leistungsbewertung des ISMS
- Internes Auditprogramm und -durchführung
- Bewertungsschemata und Auditberichte
- Managementbewertungen
- Monitoring-Methoden und -tools
- Validierung der Anforderungen



Methodik Grundschutz++

kontinuierliche Verbesserung

- Umgang mit Nicht-Konformitäten
- Identifikation von Verbesserungspotenzialen
- Korrektur- und Verbesserungsplan
- Evaluation



Ausblick

Wie geht es weiter?

Bisher	• Vorbereitungsphase für Pilotierung • Pilotierungsfassung der Methodik-Grundschutz++
April 2026	• Start der Pilotierung der Methodik Grundschutz++
September 2026	• Konsolidierungsphase des Methodik-Dokuments • Ende der Pilotierungsphase
Oktober 2026	• Veröffentlichung der Methodik Grundschutz++ (it-sa)
November 2026	• Schulungskonzepte
Januar 2027	• Anmeldungen für Personenzertifizierung
Oktober 2031	• Ende der Zertifizierbarkeit IT-Grundschutz (GS++ Veröffentlichung +5 Jahre)

Vielen Dank für Ihre Aufmerksamkeit!

Johannes Oppelt

Johannes.Oppelt@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 87
53175 Bonn

www.bsi.bund.de

Bundesamt
für Sicherheit in der
Informationstechnik

Follow us: