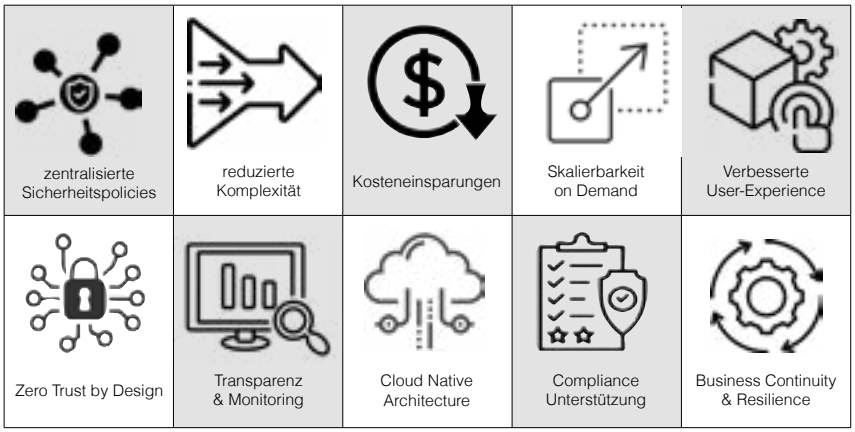
SASE Umsetzungscheckliste

Dies ist ein praxisorientierter Umsetzungsleitfaden für die Einführung von SASE.
Der Fokus liegt auf strategischer Planung, technischer Umsetzung und organisatorischer Verankerung.

10 messbare Mehrwerte von SASE



Projektphasen

1 STRATEGISCHE VORBEREITUNG

- Ist-Analysen & Zieldefinitionen
- Stakeholder & Governance

2 TECHN. PLANUNG & ANBIETERAUSWAHL

- Anforderungen festlegen
- Anbieterauswahl & PoC

3 ROLLOUT & MIGRATION

- Schrittweiser Rollout
- Policies & Monitoring

4 BETRIEB & KONT. OPTIMIERUNG

- Betriebsmodell etablieren
- Change-Management & Schulung
- Reviews & Audits

5 SKALIERUNG & INNOVATION

- Zukunftsstrategien

Telonic GmbH | Albin-Köbis-Str. 2 | 51147 Köln
Phone +49 2203 9648 0 | E-Mail: kontakt@telonic.de
www.telonic.de

Über Telonic

Die Telonic GmbH mit Hauptsitz in Köln zählt zu den etablierten IT-Systemhäusern in Deutschland. Seit 1979 in Familienbesitz, unterstützt die Telonic Unternehmen und Organisationen aus nahezu allen Branchen bei der Planung, Absicherung und Optimierung komplexer IT-Infrastrukturen – mit Fokus auf Netzwerkdesign, IT-Security und Analyse.

Das Portfolio reicht von Netzwerksegmentierung, Next-Generation Firewalls, Secure Access und SIEM/SOC-Anbindung bis hin zu Traffic-Analyse, Performance Monitoring und automatisiertem Incident Handling.

Die Telonic steht für technische Exzellenz, langfristige Partnerschaften und einen praxisnahen, lösungsorientierten Ansatz – deutschlandweit und international.

Wir verfügen über langjährige Erfahrung im SD-WAN- und SSE-Umfeld mit verschiedenen Produkten.

Gerne unterstützen wir Sie gerne bei Ihrem Projekt: vom Design, über den PoC, die Implementierung, bis hin zum operativen Betrieb.

Ihr Ansprechpartner
Christian Gruhlke
Network & Security Ambassador

TELONIC

1. STRATEGISCHE VORBEREITUNG

Ist-Analyse & Ziele

Architektur prüfen → Cloud Nutzung bewerten → Ziele definieren

- ☐ **Netzwerk- und Sicherheitsarchitektur** analysieren
  Welche **Lösungen** (z. B. VPN, Firewall, SD-WAN) sind aktuell im Einsatz?
- ☐ **Cloud-Nutzung bewerten**: Wo befinden sich die Daten und Anwendungen (On-Prem, Hybrid, Multi-Cloud)?
- ☐ **Ziele definieren**: Performance verbessern, Sicherheitsniveau erhöhen, Kosten senken, Zero Trust umsetzen etc.

ℹ Dokumentieren Sie Schwachstellen
(z. B. Performance-Einbußen im Homeoffice, uneinheitliche Sicherheitsrichtlinien).

Stakeholder & Governance

Teams einbinden → Rollen klären → RACI nutzen

- ☐ **Relevante Teams** identifizieren und einbinden**:** IT-Security, Netzwerk, Compliance, Datenschutz, Einkauf
- ☐ **Projektteam und Lenkungsausschuss** definieren
- ☐ **Verantwortlichkeiten klären**
- ☐ Mögliche externe Partner oder Berater einbeziehen

ℹ Nutzen Sie ein RACI-Modell zur Rollenverteilung (Responsible, Accountable, Consulted, Informed).

2. TECHNISCHE PLANUNG UND ANBIETERAUSWAHL

Anforderungen festlegen

Funktionen → Integration → Compliance

- ☐ **Kritische Funktionen** (z.B. ZTNA, CASB, SWG, FWaaS)
- ☐ **Relevante Integrationen** (Identity Provider (IdP), SIEM, Endpoint Management, Cloud Dienste)
- ☐ Anforderungen an **Skalierbarkeit, Latenz, Datenschutz, Compliance**

ℹ Orientieren Sie sich an den für sie relevanten Use Cases, nicht nur an Funktionen.

Anbieterauswahl & PoC

Pilot-Standorte → SaaS- / Remote Access

- ☐ **Zugriff auf SaaS Anwendungen**
- ☐ **Remote Zugriff**
- ☐ **Policy Enforcement**
- ☐ **Netzwerkperformance**

ℹ *SASE vereint Netzwerkfunktionen (SD-WAN) und Sicherheitsdienste (SSE – Secure Service Edge) in einer integrierten Architektur. Dabei müssen SD-WAN und SSE nicht zwingend vom selben Anbieter stammen.*
Ein wesentlicher Vorteil einer herstellerübergreifenden Komplettlösung liegt jedoch in der zentralen, vereinfachten Verwaltung über ein einziges Webportal. Beispielsweise bietet Palo Alto Networks genau das mit dem Strata Cloud Manager (SCM) – einer zentralen Management-Plattform für Prisma SD-WAN in Kombination mit der Prisma Access SSE-Lösung.

3. ROLLOUT UND MIGRATION

Schrittweiser Rollout (Phasenmodell)

Nebenstandorte → Hauptstandorte → VPN ablösen

- ☐ **Integration Benutzeridentität**
- ☐ **Alt-VPN ablösen**
- ☐ **Einführung SD-WAN**
- ☐ **Migration On-Prem Sicherheitslösungen**

Policies & Monitoring

Richtlinien → SIEM / XDR → Tests

- ☐ **Festlegen zentraler Richtlinie**
- ☐ **Integration mit SIEM, UEBA oder XDR**
- ☐ **Test der Alterting und Reaktionsmechanismen**

> Realisieren Sie die “Easy Wins” zuerst,
> z. B. ZTNA für Remote-Zugriff oder einheitlicher Web-Zugriffsschutz.

4. BETRIEB UND OPTIMIERUNG

Anforderungen

Betriebsmodell → Schulungen → Reviews / Audit

- ☐ Klärung von **Zuständigkeiten, SLAs** und **KPIs**
- ☐ **Information und Schulung** der Mitarbeiter, **Awareness** schaffen
- ☐ **Jährliche Prüfung** und Anpassung gemäß veränderter Anforderungen, **Change Management**

> Policy-as-Code für Automatisierung.

4. SKALIERUNG & INNOVATION

Zukunftsstrategien

Next Steps

- ☐ Integration mit KI-basierten Sicherheitstools
- ☐ Verbindung mit IoT/OT-Infrastrukturen
- ☐ Ausbau in Richtung SSE (Security Service Edge) und Digital Experience Monitoring (DEM)

> **SASE als Basis für Zero Trust nutzen.**

Mit dieser Checkliste haben Sie den roten Faden für eine erfolgreiche SASE-Einführung in der Hand. Wenn Sie Ihr Projekt praxisnah und effizient umsetzen möchten, begleiten wir Sie gerne – von der Planung bis zum Betrieb. Sprechen Sie uns an! Ihr Team Telonic ✉