C5 Fact Sheet

- **Preise**
  - C5 Implementierung und Testierung
    - Typ 1
      - Implementierung
        - 29.950 EUR
      - Lizenzen
        - 8.090 EUR
      - Testierung durch WP
        - Design
          - 17.550 EUR
        - Preis Paket:
          - 55.590 EUR
      - gefordert seit 01.07.2024
    - Typ 2
      - >50 Mitarbeiter
        - Typ 2
          - Implementierung
            - 10.250 EUR
          - Testierung
            - auf Wirksamkeit
              - 29.250 EUR
          - Preis Paket:
            - 39.500 EUR
          - gefordert ab 01.07.2025
      - <50 Mitarbeiter
        - Implementierung
          - 9.300 EUR
        - Testierung durch WP
          - auf Wirksamkeit
            - 20.700 EUR
        - Preis Paket:
          - 30.000 EUR
        - gefordert ab 01.07.2025
- **Kundenerfahrungen**
  - schnelle und präzise Umsetzung
  - strukturiertes Vorgehen
  - SECaaS kommt mit einem klaren Plan
  - strukturierte Prozesse
- **Testierung**
  - durch einen unabhängigen Wirtschaftsprüfer
  - Abgestimmte Verfahren, weswegen wir schneller und präziser sind
  - Erfahrungen aus vielen Projekten
  - Arbeit mit unserer KI, damit haben wir die Vorteile auch die Anforderungen des WPs zu kennen
- **C5 Implementierung**
  - Phase 1 - Analyse und Plannung
    - GAP Analyse
    - Status Aufnahme
      - Nutzung und Inklusion aller existierenden Dokumentationen des Kunden
    - Scope Definition
    - Projekt Planung
  - Phase 2 - Implementierung der Anforderungen
    - Dokumentation der Richtlinien
    - Dokumentation der Prozesse
    - Training und Awareness Maßnahmen
    - Aufsetzen eines ISMS Frameworks beim Kunden
    - Anpassung und Customizing der Control Ausprägungen
    - Implementierung der technischen und organisatorischen Maßnahmen
    - Design des IKS
  - Phase 3 - Internal Audit und Zertifizierung
    - Durchführung des Internal Audits
    - Auswahl des Zertifizierers
      - Im Paket ist dies die BFMT
    - Durchführung der Zertifizierungsprüfung und Ausstellung des Zertifikats
- **C5 Kriterienkatalog**
  - Ziel:
    - Definition der Mindestanforderungen an die IT-Sicherheit von Cloud-Dienstleistern
  - Herausgeber:
    - Bundesamt für Sicherheit in der Informationstechnik (BSI)
  - Versionen:
    - Aktuellste Fassung beachten (C5:2020)
  - Relevanz:
    - Erhöhte Transparenz und Nachvollziehbarkeit für Kunden und Regulierungsbehörden
  - wesentliche Inhalte
    - Organisatorische Anforderungen:
      - Richtlinien, Schulungen, Verantwortlichkeiten
    - Betriebliche Sicherheit:
      - Incident Management, Change Management, Logging
    - Physische Sicherheit:
      - Rechenzentrumsstandorte, Zutrittskontrollen, Redundanzen
    - Technische Sicherheitsmaßnahmen:
      - Netzwerksicherheit, Zugriffskontrollen, Verschlüsselung
    - Notfallmanagement & Business Continuity:
      - Backup-Strategien, DRP, Notfallübungen
    - Datenschutz & Compliance:
      - DSGVO, branchenspezifische Regularien, Rechtskonformität
- **gesetzliche Anforderungen für die Testierung**
  - Pflicht für bestimmte Branchen:
    - Kritische Infrastrukturen (KRITIS) gemäß BSI-Gesetz
    - Finanz- und Versicherungsbranche (BaFin, MaRisk, VAIT, DORA)
    - Gesundheitswesen (NIS2, DSGVO, B3S für Krankenhäuser)
      - § 393 SGB V
        - (1) Leistungserbringer im Sinne des Vierten Kapitels und Kranken- und Pflegekassen sowie ihre jeweiligen Auftragsdatenverarbeiter dürfen Sozialdaten und Gesundheitsdaten auch im Wege des Cloud-Computing-Dienstes verarbeiten, sofern die Voraussetzungen der Absätze 2 bis 4 erfüllt sind.
        - (2) Die Verarbeitung von Sozial- und Gesundheitsdaten im Wege des Cloud-Computing-Dienstes darf nur
          - 1. im Inland,
          - 2. in einem Mitgliedstaat der Europäischen Union oder
          - 3. in einem diesem nach § 35 Absatz 7 des Ersten Buches gleichgestellten Staat oder, sofern ein Angemessenheitsbeschluss gemäß Artikel 45 der Verordnung (EU) 2016/679 vorliegt, in einem Drittstaat
        - (3) Eine Verarbeitung nach Absatz 1 ist nur zulässig, wenn zusätzlich zu den Anforderungen des Absatzes 2
          - 1. nach dem Stand der Technik angemessene technische und organisatorische Maßnahmen zur Gewährleistung der Informationssicherheit ergriffen worden sind,
          - 2. ein aktuelles C5-Testat der datenverarbeitenden Stelle im Hinblick auf die C5-Basiskriterien für die im Rahmen des Cloud-Computing-Dienstes eingesetzten Cloud-Systeme und die eingesetzte Technik vorliegt und
          - 3. die im Prüfbericht des Testats enthaltenen, korrespondierenden Kriterien für Kunden umgesetzt sind.
    - Öffentliche Auftraggeber (Vergaberecht, IT-Sicherheitsvorgaben)
  - C5 als Nachweis für regulatorische Anforderungen:
    - BaFin (Deutschland) → Anforderungen an IT-Sicherheit bei Finanzdienstleistern
    - EU-NIS2-Richtlinie → Stärkung der Cybersicherheit in kritischen Sektoren
    - ISO 27001 und C5 → Kann als ergänzender Nachweis für ISMS verwendet werden
    - Vergaberecht → In Ausschreibungen zunehmend als Mindestanforderung
  - Alternativen oder Kombinationen zu C5:
    - ISAE 3402 / SOC 2 (internationale Audits für Cloud-Sicherheit)
    - TISAX (Automobilindustrie)
    - B3S (Branchenstandards für kritische Infrastrukturen)

Presented with xmind