C5 Fact Sheet

Pricing

- C5 Implementation and Certification
  - Type 1
    - Implementation:
      - 29.950 EUR
    - Licenses
      - 8.090 EUR
    - Testing by auditor
      - Design
        - 17.550 EUR
    - Total Package:
      - 55.590 EUR
    - since 01.07.2024
  - Type 2
    - >50 Employees
      - Type 2
        - Implementation
          - 10.250 EUR
        - Testing:
          - Effectiveness
            - 29.250 EUR
        - Total Package:
          - 39.500 EUR
        - from 01.07.2025
    - <50 Employees
      - Implementation
        - 9.300 EUR
      - Testing by auditor:
        - Effectiveness
          - 20.700 EUR
      - Total Package:
        - 30.000 EUR
      - from 01.07.2025

Customer Experiences

- Fast and precise implementation.
- Structured approach
- SECaaS comes with a clear plan.
- Well-organized processes.

Testing

- Conducted by an independent auditor.
- Harmonized procedures enable faster and more precise implementation.
- Drawing on experience from numerous projects.
- Leveraging our AI to understand auditor requirements.

C5 Implementation

- Phase 1: Analysis and Planning
  - Gap analysis.
  - status assessment.
    - Utilization and inclusion of all existing customer documentation.
  - Scope definition.
  - Project planning.
- Phase 2: Implementation of Requirements
  - Documentation of policies.
  - Documentation of processes.
  - Training and awareness measures.
  - Setting up an ISMS framework at the customer.
  - Customization and adjustment of control attributes.
  - Implementation of technical and organizational measures.
  - Designing the internal control system (ICS).
- Phase 3: Internal Audit and Certification
  - Conducting internal audits.
  - Selecting the certification body (e.g., BFMT Audit GmbH).
  - Performing the certification audit and issuing the certificate.

C5 Criteria Catalog

- Objective:
  - Definition of minimum requirements for IT security of cloud service providers.
- Publisher:
  - Federal Office for Information Security (BSI), Germany.
- Versions:
  - Always observe the latest version (C5:2020).
- Relevance:
  - Increased transparency and traceability for customers and regulatory authorities.
- Key Contents
  - Organizational Requirements:
    - Policies, training, responsibilities
  - Operational Security:
    - Incident Management, Change Management, Logging
  - Physical Security:
    - Data center locations, access controls, redundancies
  - Technical Security Measures:
    - Network security, access controls, encryption
  - Emergency Management & Business Continuity:
    - Backup strategies, Disaster Recovery Plans (DRP), emergency exercises
  - Data Protection & Compliance:
    - GDPR, sector-specific regulations, legal compliance

Legal Requirements for Certification

- Mandatory for Specific Industries:
  - Critical Infrastructures (KRITIS) under BSI Law
  - Finance and Insurance Sector (BaFin, MaRisk, VAIT, DORA)
  - Healthcare Sector (NIS2, DSGVO, B3S for hospitals)
    - § 393 SGB V
      - (1) Service providers as defined in the Fourth Chapter and health and nursing care insurance funds, as well as their respective data processors, are permitted to process social data and health data through cloud computing services, provided that the conditions of paragraphs 2 to 4 are met.
      - (2) The processing of social and health data through cloud computing services is only permitted if:
        - 1. In the country,
        - 2. In a member state of the European Union, or
        - 3. In a state equated according to § 35 paragraph 7 of the First Book or, if an adequacy decision according to Article 45 of Regulation (EU) 2016/679 is present, in a third country.
      - (3) Processing according to paragraph 1 is only permissible if, in addition to the requirements of paragraph 2:
        - 1. Technical and organizational measures appropriate to the state of the art to ensure information security have been taken.
        - 2. A current C5 certificate of the data processing entity regarding the C5 basic criteria for the cloud computing services used and the technology employed is available, and
        - 3. The criteria corresponding to the test report of the certificate have been implemented for customers.
  - Public Contracting Authorities (Procurement Law, IT Security Requirements)
- C5 as Proof for Regulatory Requirements
  - BaFin (Germany) → IT Security Requirements for Financial Service Providers
  - EU NIS2 Directive → Strengthening Cybersecurity in Critical Sectors
  - ISO 27001 and C5 → Can be used as supplementary proof for ISMS
  - Procurement Law → Increasingly required as a minimum standard in tenders
- Alternatives or Combinations to C5:
  - ISAE 3402 / SOC 2 (International Audits for Cloud Security)
  - TISAX (Automotive Industry)
  - B3S (Industry Standards for Critical Infrastructures)

Presented with xmind