# Information Security Certification Processes

## 1 Application Process

Our application process is designed to be straightforward and transparent. Organizations interested in CMMC, ISO or SSAE certification can apply through our website or by contacting our office. The application form requires basic information about the organization, the scope of certification, and any relevant documentation.

## 2 Audit and Certification Procedures

Our audit and certification procedures are conducted in accordance with the appropriate governing body. ISO certifications procedures align with ISO/IEC 17021-1 standards. The process includes a Stage 1 audit to review documentation and a Stage 2 audit to assess the implementation of the management system. Upon successful completion, a certification decision is made, and a certificate is issued.

Certification audits typically follow a structured, multi-phase process to assess whether an organization's Information Security Management System (ISMS) meets the standard's requirements.

### 1. Preparation and Application

• Define the scope (e.g., departments, locations, systems).

• Select an accredited certification body.

• Submit an application and complete a pre-assessment questionnaire.

### 2. Stage 1 Audit – Documentation Review

- The auditor reviews:
    - ISMS policies and procedures
    - Risk assessment and treatment plans
    - Statement of Applicability (SoA)
    - Internal audit and management review records
- Purpose: Ensure the ISMS is formally documented and ready for implementation review.

### 3. Stage 2 Audit – Implementation & Effectiveness

- On-site or remote audit of the ISMS in action.
- Includes:
    - Interviews with staff
    - Observation of processes
    - Review of records and controls
- Focus: Verify the ISMS is effectively implemented and operational.

4. Audit Report and Nonconformities
- Auditor issues a report detailing:
    - Findings
    - Nonconformities (major or minor)
    - Opportunities for improvement
- Organization must address nonconformities with corrective actions.

5. Certification Decision

- The certification body reviews the audit report and corrective actions.
- If compliant, the organization is issued an ISO/IEC 27001 certificate (valid for 3 years).

6. Surveillance Audits (Years 2 & 3)
- Annual audits to ensure continued compliance.
- Focus on:
    - Key controls
    - Internal audits
    - Management reviews
    - Corrective actions

7. Recertification Audit (Year 4)

- A full audit similar to Stage 2 to renew the certification for another 3-year cycle.

## 3 Use of Certification Marks

Certified clients are granted the right to use our certification marks in accordance with our guidelines. These marks can be used on marketing materials, websites, and other promotional content to demonstrate compliance with ISO or CMMC standards. Misuse of certification marks may result in suspension or withdrawal of certification.

## 4 Rights and Duties of Certified Clients

Certified clients have the right to receive impartial and competent certification services. They are also responsible for maintaining compliance with the relevant ISO standards, informing us of any significant changes, and cooperating during surveillance audits.

## 5 Appeals and Complaints Process

We have established a fair and transparent process for handling appeals and complaints. Clients can submit appeals or complaints through our website or by contacting our office. All submissions are reviewed by an independent committee, and decisions are communicated promptly.

During the appeal process, the following steps are required to be followed, at a minimum:

- The compliance team will log the appeal and record the date received, by whom it was received, and who the appellant is.
- Once the appeal is received, the compliance team is required to contact the appellant to confirm the appeal and direct the appellant to the publicly accessible appeals handling process.
- The compliance team will oversee the due diligence process to validate or dismiss the appeal.
- All documentation and evidence gathered during the appeal handling process will be provided to the compliance team, independent from the audit team and certification decision maker. This team will be responsible for deciding what actions should be taken in response to the appeal.
- The appeal, once closed, is filed, and will include all supporting documentation and evidence utilized in making the decision.

## 6 Fees and Charges

Our fees and charges are competitive and reflect the scope and complexity of the certification process. A detailed fee schedule is available on our website or upon request. We ensure transparency in all financial transactions and provide clear invoices for all services rendered.

The pricing of certification is influenced by several factors, including the type of assessment, scope and complexity of the organization, executive support, customer readiness, and timing.

- Scope and Complexity: A broader and more complex management system typically requires more extensive auditing, which can increase certification costs. This includes the size of the organization, the number of processes, and the geographical locations involved.
- Executive Support: Strong support from top management can streamline certification procedures, potentially reducing costs by ensuring timely and effective implementation of required standards.
- Customer Readiness: The readiness of the organization to meet ISO standards can impact costs. Organizations well-prepared for audits often incur lower costs than those needing significant improvements.

Timing: The timing of certification activities, including the scheduling of audits and the availability of necessary documentation, can affect pricing. Flexibility and efficient scheduling may lead to cost savings.