# Evidence Collection and Assessment

The evidence templates can be used as one of the collection and discovery methods

Generalized criteria that can be applied to all the requirements.

**Evidence** comprises records, statements of fact or other information relevant to the audit criteria and which are verifiable. Audit evidence may be qualitative or quantitative.

A typical audit process should consist of the following:

* Identification of sources of information
* Collecting the information by appropriate sampling and verifying
* Establishing audit evidence from the information
* Evaluating the information and evidence against audit criteria
* Identifying audit findings
* Reviewing the audit findings and evidence
* Audit conclusion

**Evaluation Criteria** are used as a reference against which conformity is determined and may include:

* applicable policies, procedures, standards,
* laws and regulations,
* management system requirements,
* contractual requirements or
* industry/business sector codes of conduct

## Recommended approach

This approach is consistent with what is recommend for conformity assessment schemes and systems as recommended by ISO/CASCO

|  |  |
| --- | --- |
| 4.1.2.1 Top management shall demonstrate their commitment to the cyber security program by:  **Level 1 requirements**  Top management shall demonstrate their commitment to the cyber security program by:   1. ensuring the cyber security policy and objectives are established and are aligned with the strategic direction of the organization. 2. ensuring that the resources needed for the cyber security program are available and are aligned with the cyber security policy and objectives. 3. communicating the importance of effective cyber security and of conforming to the cyber security program requirements. 4. establishing cybersecurity program metrics and tracking progress; and supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility. 5. supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility | |
| **The Client may provide as evidence:**   * Any specific documentation that supports **Level 1 a) thru e)** including:   + Applicable policies, procedures and guidelines   + Approval processes by management including, where possible, management approval of specific documents.   + Plans that specify cyber security program resources (human or financial), including internal or contracted resources.   + Internal communications (emails, memos, etc.) relating to the importance of cyber security and conforming to program requirements.   + Program metrics and tracking progress, including reports, or as part of a management system. * Any related documentation that illustrates management commitment * A completed copy of questionnaire that has been provide by the auditor. * Records of interviews conducted with senior level management and employees | **The Auditor may use as evaluation criteria**   * Documentation has sufficient level of detail that is appropriate to the size of the organization. * Levels of resourcing are reasonable and commensurate with the size of the organization. * Communication products that have been reviewed with consideration and, if necessary, tailored to the client’s context. * Program and metrics are suitable for the client’s context, business risk and business activities. * Senior management and their employee’s overall knowledge and commitment to the cyber security program. |
| **Additional guidance:**   * Depending on the size and maturity of the organization, the relevant evidence may be embedded or acknowledged in more generalized business policy and technical documents. * The auditor may need to document what exists as tacit knowledge or informal processes that exist with the organization. Documentation may come in the form of surveys, interviews, records. The client should have an opportunity to review and provide comment before it is finalized as evidence. | |

## Additional Notes: Generalized Criteria