# Assessment Evidence: Enterprise-Wide Management

Assessor’s Note:

* Enterprise-wide requirements are PSP-PCTF only and are not specified in CAN/CIOSC 103-1

| **ID** | **Qualifier(s)** | ***Conformance Criteria***  **Evidence** |
| --- | --- | --- |
| EWMG |  | *General requirements for enterprise-wide management that are applicable to all atomic and compound processes identified in the PCTF* |
| EWMG.01 | GEN | *The entity under assessment MUST ensure that policies and plans are developed, documented, and disseminated within the organization that address, at an enterprise level:*   * *Risk assessment;* * *Audit and accountability;* * *Security assessment;* * *Disaster or contingency planning;* * *Identification and authorization;* * *Systems and communication protection;* * *Incident response;* * *System and information integrity;* * *Information management and privacy protection;* * *System maintenance;* * *Technical access control (e.g. lockdown of operating systems, intrusion detection, password management, encryption, and network access management); and* * *Physical access to technology assets.* |
| EWMG.02 | GEN | *The entity under assessment MUST ensure that the formal operational policy and procedures, identified in EWMG.01, are reviewed and updated regularly on a fixed schedule appropriate to the context of the program/service being delivered.*  *Policies/plans may also require update on an ad hoc basis based on operational events or extraordinary need.* |
| EWMG.03 | GEN | *The entity under assessment MUST have active procedures that reflect the operational policy requirements for:*   * *provision of notice,* * *activity audit,* * *information maintenance* * *information protection* * *information archiving and destruction, and* * *provision of redress or dispute resolution.* |
| EWMG.04 | GEN | *The entity under assessment MUST ensure that automated procedures fulfilling service delivery comply with the relevant policy as identified in EWMG.01.* |
| EWMG.05 | GEN | *The entity under assessment MUST specify its mandate and authority as these relate to the identification of entities and to the relationships between entities.* |
| EWMG.06 | GEN | *The entity under assessment MUST provide a description of the program or service, including:*  *1. The type and nature of the program or service;*  *2. The intended clients of the program or service; AND*  *3. The approximate size, characteristics, and composition of the client population.* |
| EWMG.07 | GEN | *The entity under assessment MUST ensure that personal information, organizational information, and relationship information are collected and managed under relevant law, regulation, and policy.* |
| EWMG.08 | GEN | *For all PCTF governed activities, the entity under assessment MUST identify the authorized operational roles, access management processes, and modification processes pertaining to the collection and management of information.* |
| EWMG.09 | GEN | *For all PCTF governed activities, the entity under assessment MUST have quality assurance processes (e.g., monitoring, measurement) in place to ensure consistent execution of operational tasks.*    *Specifically, this pertains to operational activities such as:*   * *front counter activities;* * *back office activities such as information processing and adjudication; and,* * *information maintenance and modification activities.* |
| EWMG.10 | GEN | *The entity under assessment MUST have clearly communicated dispute resolution processes in place to allow affected parties (i.e., Subjects, Agents, Verifiers, Issuers) to challenge decisions taken during ongoing service provision.* |
| EWMG.11 | GEN | *The entity under assessment MUST provide notice to entities providing identity evidence or relationship evidence that false or misleading statements may result in violation of the terms and conditions of the program or service.* |
| EWMG.12 | GEN | *The entity under assessment MAY rely on another entity to carry out program or service activities that are subject to these conformance criteria. In such cases, the entity under assessment MUST:*  *1. Provide documentation of the written agreement for the arrangement in effect; AND*  *2. Provide documentation of the agreed upon conformance criteria.* |
| EWMG.13 | GEN | *The entity under assessment MUST ensure that service providers to whom they have delegated service provision tasks adhere to applicable identity management controls, standards, and guidelines.* |
| EWMG.14 | GEN | *The entity under assessment MUST manage system components using its defined system development life cycle that incorporates security concerns.* |
| EWMG.15 | GEN | *The entity under assessment MUST have formal technology change management processes in place to evaluate and manage risk associated with technology evolution.* |
| EWMG.16 | GEN | *The entity under assessment MUST ensure that its personnel responsible for operations affecting personal information, organizational information, and relationship information have received privacy and security training.* |
| EWMG.17 | GEN | *The entity under assessment MUST ensure the confidentiality and integrity of program/service information at rest and in transit, within the boundaries of their security and information protection context.* |
| EWMG.18 | GEN | *The entity under assessment MUST ensure that system boundary protection tools, devices, and techniques are employed.* |
| EWMG.19 | GEN | *The entity under assessment MUST uniquely identify and authenticate nonorganizational personnel or users, or processes acting on behalf of non-organizational personnnel or users, where authentication is appropriate.* |
| EWMG.20 | GEN | *The entity under assessment MUST adhere the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks for the management of secure or privacy-protected information.* |
| EWMG.21 | GEN | *The entity under assessment MUST enforce access controls to ensure that only authorized personnel can update identity information or relationship information.* |
| EWMG.22 | GEN | *The entity under assessment MUST employ tools and techniques to protect against or limit the effects of common external system attacks (e.g., network based attacks such as denial of service attacks, network access based attacks such as authentication replay*  *and secret guessing).* |
| EWMG.23 | GEN | *The entity under assessment MUST have automated intrusion detection and alerting technology in place.* |
| EWMG.24 | GEN | *The entity under assessment MUST have a program of continuous vulnerability testing of system and software components leveraged in the delivery of services.* |
| EWMG.25 | GEN | *The entity under assessment MUST conduct regular penetration testing of all components leveraged in the delivery of services.* |
| EWMG.26 | GEN | *The entity under assessment MUST test, evaluate, and update the contingency plan (i.e., disaster recovery) on a regular basis.* |
| EWMG.27 | GEN | *The entity under assessment MUST have comprehensive automated backup procedures in place addressing backup of operational data, user level information, system level information, and system and security documentation.* |
| EWMG .28 | GEN | *The entity under assessment MUST ensure the integrity of backups of operational data, user level information, system level information, and system and security documentation.* |
| EWMG.29 | GEN | *The entity under assessment SHOULD store backups of critical system software and operational data in a facility that is physically separate from the operational system.* |
| EWMG.30 | GEN | *The entity under assessment MUST have formal information retention and disposition schedules, appropriate to their program/service delivery context.* |