

4.1 Human Actors

[Go to 4. Actors and Responsibilities](#)

Human Actors direct, govern, operate, assess, authorize, maintain, or consume [Crucible](#) capabilities.

The actor names used on this page describe functional responsibilities rather than mandatory organizational titles. One person can perform several roles, and an organization can divide one role among several people.

Program and Product Leadership

Executives and **Organizational Leaders** establish organizational priorities, allocate resources, approve shared capabilities, and evaluate the operational and financial effects of adopting Crucible across multiple products or programs.

Program Managers and **Product Managers** coordinate delivery priorities, resource needs, implementation status, operational risks, provider support, and roadmap decisions.

These roles do not define technical configuration or independently approve an environment for operation unless the organization assigns them those responsibilities.

System Ownership and Governance

System Owners define the mission, operational, security, compliance, and lifecycle expectations applicable to a system or [Infrastructure Environment](#).

Governance Authorities establish organizational policies, controls, approval criteria, technical direction, and responsibility assignments.

Authorizing Authorities evaluate risk, assessment results, and supporting [Evidence](#) when making authorization or [Operational Approval](#) decisions.

Crucible supports these decisions by producing and preserving relevant information. Crucible does not grant [Accreditation](#), Operational Approval, or an [Authority to Operate \(ATO\)](#).

Architecture and Engineering

Enterprise Architects, **System Architects**, and **Solution Architects** define architectural boundaries, shared responsibilities, interfaces, provider contracts, and lifecycle relationships.

Platform Engineers construct and maintain reusable [Platforms](#), deployment environments, provider integrations, and automation services.

Infrastructure Engineers define and deploy infrastructure through [Infrastructure as Code \(IaC\)](#) and

related provider implementations.

DevSecOps Engineers integrate construction, deployment, assessment, dependency management, and Evidence generation into controlled operational workflows.

Software Factory Engineers establish and operate [Software Factories](#) that use Crucible capabilities.

Image Engineers construct, harden, verify, and maintain [Machine Images](#) and other supported image forms.

Developers and **Maintainers** create or modify Crucible components, provider implementations, plugins, integrations, and supporting tools.

Security, Compliance, and Assessment

Cybersecurity Engineers apply security criteria, review configurations, evaluate controls, assess results, and support remediation activities.

Compliance Officers evaluate compliance criteria, assessment results, exceptions, claims, [Compliance Findings](#), and supporting Evidence.

Assessors perform or review assessments using the applicable criteria, methods, and organizational procedures.

Auditors examine [Traceability](#), [Provenance](#), assessment results, lifecycle records, and [Auditability](#).

These roles can overlap, but organizations should preserve any separation of duties required by applicable policies, controls, or authorization processes.

Operations

Environment Operators deploy, operate, monitor, maintain, validate, and retire managed Infrastructure Environments within the authority granted to them.

Enclave Operators import, deploy, operate, and maintain approved content within [Disconnected Environments](#) or [Air-Gapped Environments](#).

Transfer Personnel prepare, review, move, receive, or import authorized content across a [Transfer Boundary](#) according to the applicable handling and approval procedures.

An organization can assign these responsibilities to separate people when security controls, information-handling rules, or separation-of-duty requirements require independent actions.

Consumers

Application Teams and **Product Teams** consume approved images, infrastructure resources, platform services, [Baselines](#), and deployment environments.

These teams can provide product-specific configuration and mission software while relying on shared Crucible capabilities for common lifecycle activities.

Responsibility Boundaries

Human Actors remain responsible for decisions requiring organizational authority, professional judgment, or risk acceptance.

Automated Crucible activities can construct, assess, validate, record, and report results, but automation does not replace the people or authorities responsible for:

- Establishing applicable policies and criteria
- Approving access to environments and resources
- Authorizing transfers across controlled boundaries
- Accepting risk
- Approving deployment or operational use
- Granting Accreditation, Operational Approval, or an ATO

The applicable leaf requirements in [Annex C: Requirements](#) define the required actions and controls. This page groups the Human Actors associated with those actions and does not create additional roles or responsibilities.

© 2026 Dido Solutions, Inc. and Jackrabbit Consulting, Inc.

From:
<https://wiki.didosolutions.com/> - **Dido Solutions, Inc Wiki**

Permanent link:
<https://wiki.didosolutions.com/dido/02-crusible/04-actors-and-responsibilities/04-01-human-actors?rev=1785588982>

Last update: **2026/08/01 05:56**

