Glossary of Terms - Security Risk Management

Last Modified on 02/10/2023 11:33 am EST

TERM	*DEFINITION*
Activity	Part of an application where users can create, edit, and view data.
Announcement	A generic broadcast message from an administrator to Portal Users.
Application	Holds activities where users complete tasks (actions) and view information (views).
Asset	Defined-value library asset information referenced as material to a negative event; used as fixed or moving corporate assets, or items with large value and impacts to the business.
Business Unit	Primary organizational hierarchy providing security and ownership to key data objects including Incidents, Risks, Controls and Incident Types. Some standard reports are anchored at the Business Unit (BU) level. All Business Units link to a Company object.
Control	The method an organization uses to manage risk, including policies, procedures, guidelines, practices, or organization structure, which can be of administrative, technical, management or legal nature. For Security Risk Management, controls are visible and linked to Locations only if Compliance Management or Incident Management are also used. GS: Should we include this?
Corrective Action	An improvement in the organization to eliminate a gap or problem and prevent reoccurrence.
End users	The non-administrative users who work with Security Risk Management and its applications.
Field	A component on a form where a user can input data. Fields can include plain text, numeric, date and time formats, as well as select lists (dropdown menus), and attachments.

TERM	DEFINITION
Finding	Finding record specific to a requirement to document multiple photos, attachments and comments for the specific assessment cycle. Allows historical findings for continuous assessment.
Incident	An event that is deemed worthy of being recorded, tracked, assessed and analyzed.
Incident Type	A category that describes an incident and can be used to group it with similar incidents.
Issue	A gap or a problem in the organization.
Library	Contains all object types and their data that can be added to incidents.
Location	A fixed location with physical mailing address and/or geographical coordinates. Further classification includes internal corporate locations with asset impacts versus material external reference points on negative events.
Object	A record saved to an object type (the record category). For example, Incident is the object type, while Accident, which outlines the details of an on-site incident, is the object.
Object Type	The category of the data collected (e.g. Incident, Employee Record, Witnesses, Vehicles, etc.). Once a record is saved to an object type, it becomes an object.
Organization	Master Organization record with key operations info and hierarchy, representing perpetuity but referenced temporally on Incidents as external entities. Children records include locations and related personnel.
Person	Master Person record with key Vital Statistics, representing perpetuity but referenced temporally on Incidents. Children records include employment and student details, locations, social media accounts and trespass orders. For Security Risk Management, persons are used for tracking key employees at a location. GS: I don't believe we mentioned this in the guide. Should we mention it here?

TERM	DEFINITION
Process	A set of interdependent actions or operations taken to achieve a result. For Security Risk Management, processes are visible and linked to locations only if Compliance Management or Risk Management are also used. GS: Should we include this?
Risk	Risks are potential that events, unexpected or unanticipated, may have adverse effect of the organization.
Requirement	Requirements are, but not limited to, all applicable laws, regulations, orders, requirements, guidelines, and advisories required by a regulatory authority. For Security Risk Management, requirements are used to store checklist items and can be weighted and scored.
Security Framework Audit	The Security Framework Audit allows the security audit team to evaluate all relevant requirements across the organization and specific locations.
Security Risk Framework	A set comprehensive set of regulatory obligations that an organization is required to comply with. For Security Risk Management, it is used to house the set of requirements or checklists for site and security audits. GS: Or is it called Compliance framework?
States	The various stages of the data collection process (e.g. Create, Triage, Review, Investigate, Close) for an object type workflow.
Task	Actions attached to an incident that must be completed before the incident can be closed.
Triage	Incidents submitted to the Portal go to the Triage, where the Incident Screener vets potential incidents for their validity.
User Groups	A collection of users saved to a group (e.g. Employees or Managers). The user group they are assigned to will determine their rights within the app.
Value	Data entered or selected in a field. For example, Name is the field, but the data entered in that field, John Doe, is the value.

TERM	*DEFINITION*
Workflow	Controls the flow of data as well as defines what data is displayed, where it’s displayed, and to whom it’s displayed through applications, activities, search results, reports, and assignments. Each object type has a workflow.