

Propagation Overview

IT infrastructures are usually complex, with many interconnected systems and components. Propagation allows you to reflect these inter-dependencies by disseminating control results and risks from one entity and/or entity collection down to multiple other entities or entity collections. Generally, with propagation, you are spreading the results from one to many entities or entity collections, as opposed to doing it from many entities or entity collections to a single entity or entity collection. In order for propagation to occur, there must be a relationship between entities or between the entity and entity collection. Also, propagation must be enabled for the relationship. This allows the entities or entity collection to inherit the results from the related entities or entity collections within a program

RiskVision utilizes a publish - auto-subscribe - revocation model for propagation. Before any control results can be propagated, they first have to be published by a related entity or an entity within the same program for a relationship for which propagation has been enabled. All related entities or entity collections will automatically inherit the results but can then revoke those results if they decide to meet the control(s) on their own.

RiskVision application has the following types of propagation:

- Inter system
- Intra system

Inter system: This type of propagation happens between entities and other entities, between entity collections and other entity collections, or between entities and entity collections. An example of this type of propagation would be propagating results for authentication and authorization-related controls from Active Directory to the SAP financial system.

Intra system: This type of propagation happens between entity collection and its members and is meant to capture controls that apply only to the specific system in question and not other systems or components. For example, Active Directory may provide authentication and authorization-related services to other systems, but for internal Active Directory components, may need to propagate results for other controls, such as whether there is a system security plan in place or whether risk management processes are being followed for the system.