BEST PRACTICES

A scalable approach to access control in RSA Archer

In most organizations, separation of duties is a common internal control to prevent fraud and error in IT systems. Data and information in GRC (Governance, Risk Management & Compliance) solutions is integral to an organization's Risk Intelligence strategy and should be well-protected. To achieve separation of duty, RSA Archer establishes three lines of defence: Business stakeholders, the corporate program team, and the internal audit group.

How is Access Control modeled in RSA Archer?

Role-based access control is an approach that's often used to restrict system access to certain authorized users, and is adopted by most enterprises and implemented for IT and business systems. With the proper implementation of a role-based access control permission model in Archer, we can achieve the following objectives:

- Restrict access to data only to authorized resources.
- Better reporting and a holistic understanding of the organization's risk and its impact to business processes and operations.

There are three levels of access control available within RSA Archer:

- **Access Roles:** define which module can be accessed by a user.
- **Group / Record Permissions:** define which records can be accessed by a user within a specific module.
- **Sections / Tabs / Fields:** define which elements can be seen or edited by a user

In this document, I'll focus on **Group / Record Permissions.**

Aligning the permission model with business hierarchy

Access control is usually aligned closely with the organization's business hierarchy, allowing authorized users in various business groups access to the required data depending on their role and responsibilities. A simple example would be a Vancouver-region regulation compliance report, which should only be accessed by authorized people in Canada, while people from China in the same organization should not have access this report.

One challenge occurs if an organization has a very complex business hierarchy. It's not uncommon for large companies to have hundreds of business units across the world, with overlapping responsibilities. In Archer, while it's technically possible to create several hundred groups to accommodate each business unit, I don't recommend it! Archer group assignment access is usually only given to the system administrator and the effort to maintain the group structure / user assignment is huge for one administrator to manage.

By Zhao Tian
GRC Solution Designer
icebergnetworks.com

Typically, an organization will want to implement multiple business hierarchies for different parts of their GRC program, for example:

- Legal View of Business Hierarchy for Compliance
- Finance View of Business Hierarchy for Operational Risk
- Technology View of Business Hierarchy for Application Risk

I recommend a more reliable and scalable option for implementing an enterprise-wide access control model to meet this complex requirement and keep the effort to maintain it as low as possible.

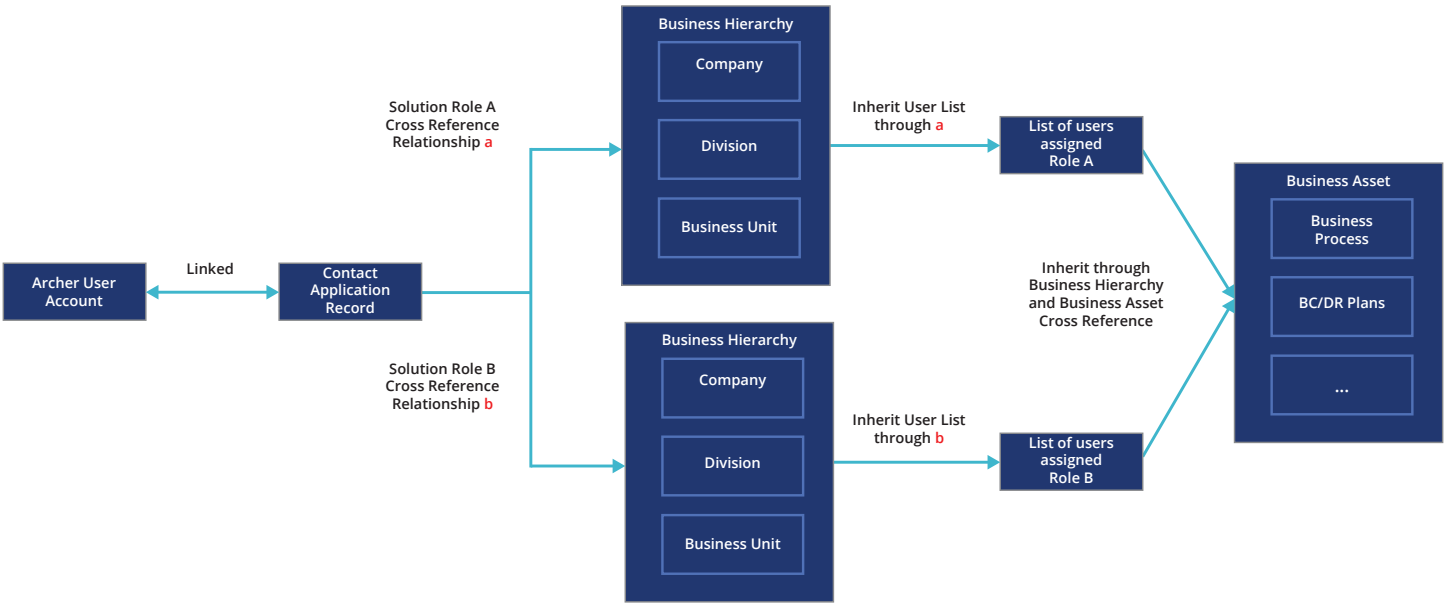
Implementing an enterprise-wide access control model meets complex access requirements, while minimizing maintenance for your Archer administrator.

First things first

This type of access control model requires that you've already implemented your business hierarchy in Archer, and that you have a solid understanding of business asset access control. Large organizations usually have a massive asset management system. The challenge is how to map all the asset access to the proper business hierarchy. That's something you'll need to consider and plan for in advance before implementing this kind of access control.

Implementing an Archer Access Control Model

The architecture diagram below illustrates how an Archer User Account (shown at the left) is linked to information from the Contact Application Record.

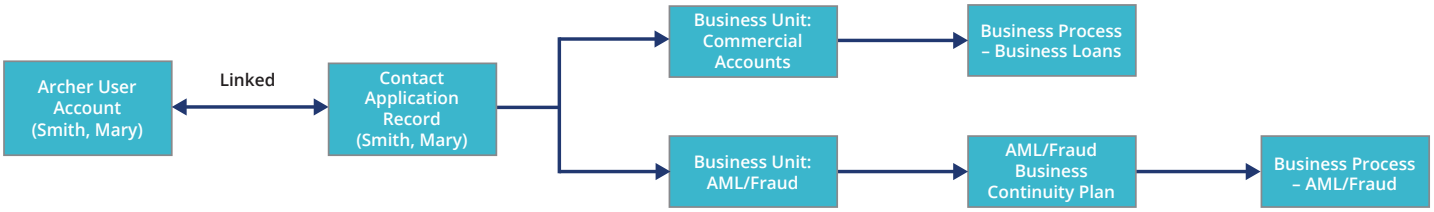


In Archer, the Contacts Application can be used to capture personal information, which can include employees inside the organization or external vendors. Then we can assign the contact record to the business unit / division that the employee belongs to.

The individual Contact Application record can be linked to an Archer user account, and we can leverage an option called "Inherited Record Permission with restricted mode" to link the user access from the Contact application record all the way down to the GRC Asset/Assessment information which is associated with the Business Hierarchy.

Even if there are multiple versions of the business hierarchy residing within Archer, we can use cross-reference fields to differentiate between them. Then we can link user access from each associated business hierarchy to GRC Asset/Assessment information.

This chart shows how this might look for an individual user, Mary Smith, who has access to information from multiple business units.



More ways to simplify and streamline

As mentioned above, this approach simplifies the management of complex access control requirements by transferring control from the system administrator (IT) to the solution administrator (Business), by linking user access to roles that are already established as part of business hierarchies. By the way, the hierarchies that are established within Archer can also be integrated via data feeds or API to external HR systems and business tools, which can further simplify user governance.

Access control is a key to success

To deliver an effective Risk Intelligence Program, your GRC solution must be able to provide trusted, transparent and aggregated information to a broad range of stakeholders in your organization. The more people who can access reports and useful information from the tool, the more effective you'll be at breaking down silos and achieving a true enterprise-wide view of risk. That's only possible with a robust and scalable approach to access control, that gives everyone confidence that sensitive company data is being properly protected.