SoCal Privacy Consultants

Lean. Sustainable. Legally Defensible.

Roles Based Access Controls (RBAC) Explained

What is RBAC?

Roles-based access controls ensure that access to Resources that store or control access to personal information you want to protect can be well designed, easy to implement, and easy to review for errors.

This explanation focuses on System RBAC. Policy and procedures should address the following:

Resources refers to information storage and access control systems, including both electronic storage systems (e.g. electronic file shares on a server), firewalls and VPN services (managed by "System RBAC") and hard paper storage (e.g. physical file cabinets). Resources may also include contracted third parties such as cloud service providers, email list servers, and data analytics vendors.

RBAC Governance

1. Designate a Resource Owner, preferably a single individual, to design appropriate RBAC rights for various roles having access to a specific Resource. Identified roles should have enough granularity to ensure minimum necessary access rights.
    - As an example, Tier 1 customer service may have read only access. Tier 2 may have read and update capability. CS Management may have the same as Tier 2 but also the ability to delete information.
    - The design should take into account company needs for the next 2-3 years. This may mean that certain roles will temporarily be unassigned.
2. Designate a Resource Custodian responsible for the implementation of properly authorized RBAC rights. The Resource Custodian should be a technical individual with privileged access to the Resource, who can create a role or group with the rights defined by the Resource Owner. Generally, there should be a primary and a back-up Resource Custodian.

Minimum necessary access (also known as "least privilege" or "need to know") is the minimum level of access necessary for an individual, or group of individuals, within an RBAC role to meet their regular job duties. The level of access is determined by job *need,* not convenience. Those in job roles requiring infrequent access should defer to individuals who have RBAC rights to that information based on their regular job duties.

Implementing RBAC

1. Resource Owners must authorize RBAC assignment of rights.
    - Once roles have been defined, the Resource Owner can assign roles by specific user or by job title. If formal job titles are in place, the latter option may be easier to implement, as new hires are automatically assigned RBAC roles to Resources during on-boarding.
    - Authorization or change control is made for new users, users changing job functions, and user terminations.
2. Resource Custodians assign users to authorized RBAC roles.
    - Assignment should occur when authorization is documented. The documentation must be producible upon request to ensure custodians are not assigning rights to users without authorization.

RBAC Responsibilities

1. Resource Owners periodically review RBAC rights.
   - The Resource Owner must periodically review both the roles definitions created for accessing a Resource, and who has been granted the rights to each RBAC role. This review should be documented.
     - RBAC role rights may change infrequently, such as for a cloud service provider, or may change often, such as for an application being actively developed in-house or a rapidly growing company. Resource Owners should appropriately adjust how frequently they review role rights and whether new roles need to be created, based on factors such as findings and company growth or changes.
     - Review of users (not just job titles) assigned to RBAC roles is important to catch issues such as missed assignment during hiring, missed disabling of access during termination or a user's job change, or implementation error by the Resource Custodian.
     - Resource Owner may also consider requesting a list of terminations from HR since the last RBAC review to ensure that all terminated users have had access removed.
2. Resource Custodians should provide Resource Owners a report of all RBAC roles and what rights each role has, and the user(s) assigned to each role. Typical review frequency is every 3 or 6 months which should be established in policy.
   - When possible, this should be done in an automated, consistent fashion.
   - Changes from the most recent review should be highlighted (which users gained / lost access), as most access rights are likely similar between reviews.
3. Management/HR must inform Resource Owners and Custodians of new and terminated users, and when a user's role changes.
   - This is especially important during user terminations when the Resource is not integrated with centralized account management systems such as Microsoft Active Directory. These "external" Resources (Wordpress, Box.com, etc.) can easily be overlooked allowing continued, inappropriate access.

Types of Rights to Consider During RBAC Design

1. **User Rights** are general user rights. Most RBAC roles are defined around different user rights.
2. **Special User Rights** means infrequently granting access to a RBAC role for a limited period of time, such as to perform QA. Resource Owners should make this determination and notify the Resource Custodian to properly manage deactivation after a specified time period.
3. **Privileged User Rights**, a.k.a. "super user", have increased RBAC rights. Privileged users should also require dual authentication to protect from unauthorized access. Resource Custodians generally have these rights.

   It is important to note that while they have the *rights* to manage access to a Resource, privileged users may not be *authorized* to access the underlying data. There should be adequate oversight of privileged users by the Resource Owners and actions taken to ensure theses rights are not being misused. If an individual is a custodian of a Resource and is also a user, these should be two different accounts for that individual and used appropriately.
4. **Emergency Root Access User Rights** are rarely used privileged user rights that should be locked in a safe under dual control including a senior non-privileged user. These rights may be needed during an emergency or when the Resource Custodian is unavailable.

Feel free to reach out to us if you have any questions. SoCal Privacy Consultants perform gap assessments and help organizations build lean, sustainable, and legally defensible privacy and security programs.

Michael Cox, CIPP/US | President and Founder
SoCal Privacy Consultants | www.socalprivacy.com
mcox@socalprivacy.com | m: 619.318.1263