Audit Ready Access Control

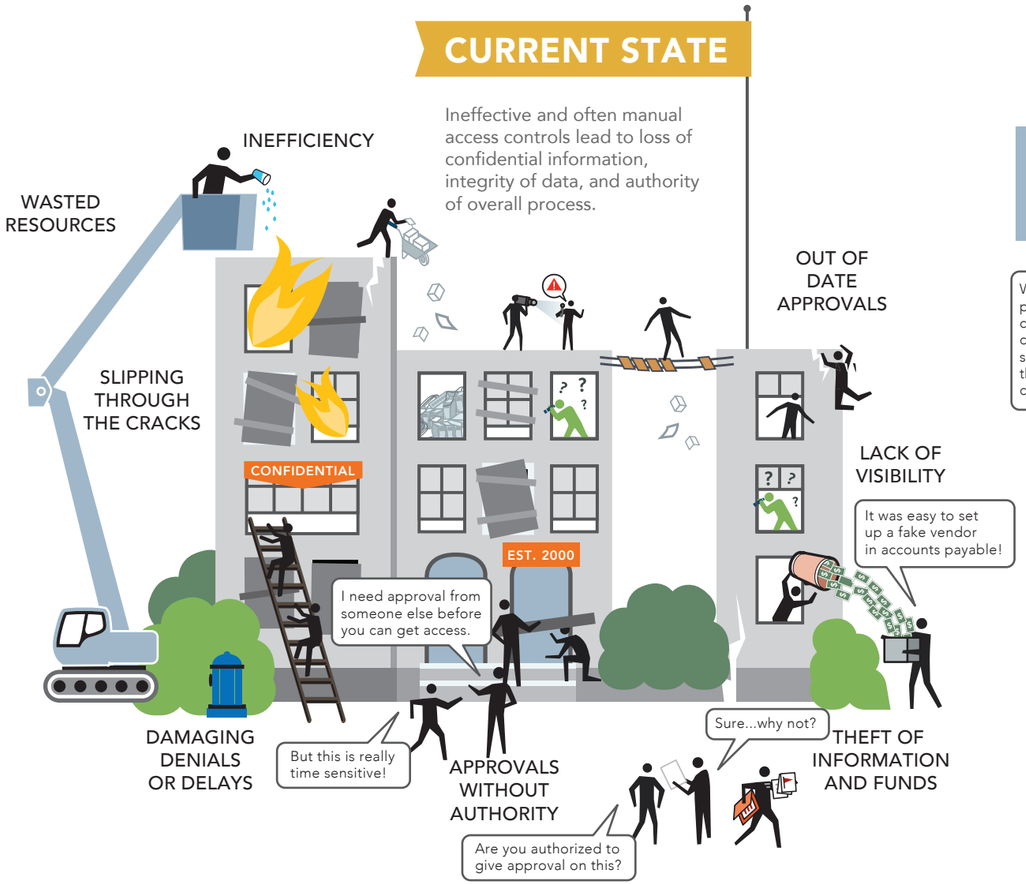
Organizations must protect information and assets by controlling access to critical systems. If an unauthorized person receives access, it can result in misappropriation of information, theft of funds and intellectual property, or damage to operations. If someone who should have access is denied it, consequences can be equally dire. In too many organizations, access control is managed manually or in disparate systems and there simply is no efficient and reliable way to provide assurance that the right controls are in place. In this illustration, we look at the benefits found in an automated audit ready control framework.

DEVELOPED BY OCEG®

WITH CONTRIBUTIONS FROM ControlPanel GRC

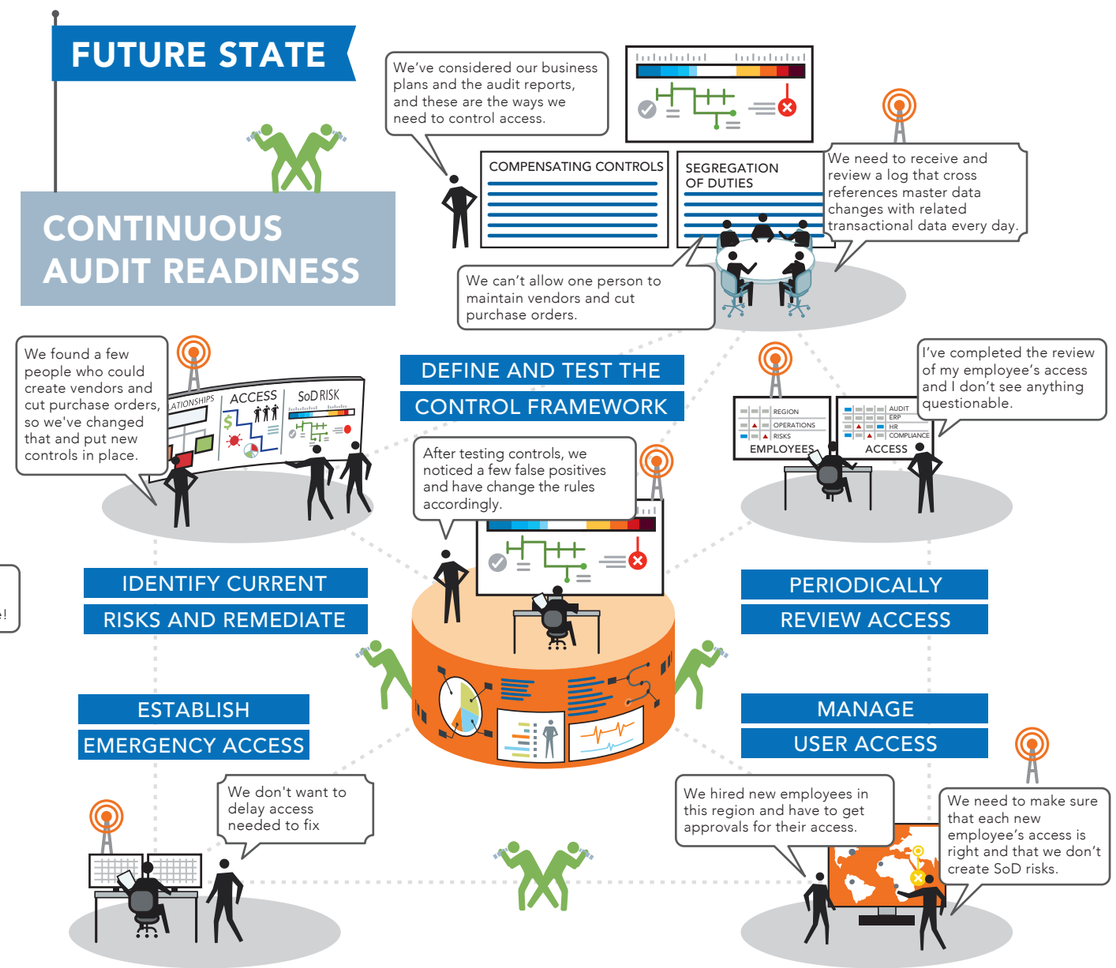
CURRENT STATE

Ineffective and often manual access controls lead to loss of confidential information, integrity of data, and authority of overall process.



FUTURE STATE

CONTINUOUS AUDIT READINESS



BENEFITS

- **VISIBILITY** enhances audit accuracy
- **EFFICIENCY** reduces manual tasks
- **AGILITY** enables quick change
- **ACCURACY** builds confidence
- **RELIABILITY** supports strategy
- **COVERAGE** addresses all aspects of the business
- **RESPONSIVENESS** drives timely action

MAKING THE CASE FOR CHANGE

CONTROL FRAMEWORK DESIGN

- Determine environment - business operations, roles, responsibilities
- Consider external and internal audit findings and legal requirements
- Establish Segregation of Duties (SoD) requirements
- Define compensating controls to apply when SoD isn't possible
- Install automated system to reduce time and errors

RISKS / REMEDIATION

- Evaluate current access relative to defined need
- Analyze current SoD risks
- Identify improper access and remove rights from users
- Manage SoD ensuring future improper access is denied
- Re-evaluate as changes arise in roles, users and needs

EMERGENCY ACCESS

- Define emergency situations and approval process
- Identify approvers and pre-approved users
- Determine elevated access rights for each need
- Gather transaction executions and data changes from emergency sessions and forward for review/ sign off
- Store approvals/sign offs for emergency access sessions for future audits

COMPENSATING CONTROLS

- Manage compensating controls through automated system that addresses each step
- Apply compensating control when segregating is appropriate but not possible
- Monitor actions that trigger controls
- Push compensating control reporting to appropriate business owners for review and sign off
- Prepare filtered reports on triggered controls

USER MANAGEMENT

- Manage requests for new users
- Manage requests and triggers for changes in existing user rights
- Check SoD risks based on access request changes
- Review and compile information on changes in roles and rights
- Obtain approvals from supervisors/business owners for access request changes

PERIODIC ACCESS REVIEW

- Schedule periodic reviews of access levels
- Schedule periodic reports with outliers identified
- Push user access data to supervisors or business owners
- Assess usage data and confirm access is appropriate or revise
- Process requested and automatically triggered changes from review

ASSESS THE OPERATION OF CONTROLS

- Identify areas of the organization (by location, business unit or type of users) where operation is not effective
- Adjust methods for ensuring controls operate as designed
- Revisit the control framework design and modify compensating controls as necessary from review