FEATURE

Effective User Access Reviews

User access review is a control to periodically verify that only legitimate users have access to applications or infrastructure. During a user access review, an application business or IT owner may discover that users who left the enterprise or transferred to another team in the enterprise continue to have access to applications or infrastructure after their access credentials or privileges should have been removed. This vulnerability can be exploited, resulting in financial and/or reputational loss to the enterprise. However, following some best practices that allow full transparency and ensure that unauthorized users do not have access to an application or system can help mitigate this risk.

Sundaresan Ramaseshan, CISM, ITIL Foundation, ITIL Service Operation
Is an IT supervisor supporting security tools at Ford Motor Private Ltd. in Chennai, India. He has more than 27 years of experience in various IT software development life cycle roles. Ramaseshan continues to enhance his depth of knowledge in the security domain and share some of the successes he observes in day-to-day operations in the hopes that they may benefit the IT security community.

User Types

A user is a person who uses an application or tool to achieve a desired business outcome. In the IT world, users can be classified into two broad groups:

- **Business users**—They use an application or tool as part of achieving their defined business outcome. Some examples are finance application users who use an application for enterprise finance activity and product development application users who use an application for a product development process.
- **IT users**—They have access to an application, tool or system for their assigned application delivery responsibilities, such as application development, testing, deployment or operations support. This user type is usually given access based on IT team type, such as development, support or general.

Common User Access Risk Scenarios

The following are some common user access risk scenarios that result in users who can access applications or systems to which they should not have access:

- Users leave a team but still have one or more of their previous team access privileges.
- Users change roles but still have one or more of their previous role access privileges.
- Users leave the enterprise but still have one or more access privileges.
- A user's reporting manager is involved in approving user continued access attestation. The risk occurs when a current reporting manager moves to a different team/assignment, but the extract used for attestation communication is not appropriately changed and such communication is sent to the user's previous reporting manager.

User Access Review Best Practices

Implementing user access review best practices can help to eliminate or avoid the mentioned risk scenarios.

Business User Access Review Best Practices
The application business owner is responsible for the effectiveness of the user access review control for business users. The owner can assign a delegate to assist with this activity, but the application business owner remains accountable for this control and any violations.

Best practices that application business owners can implement to help ensure effective user access reviews include:

- When a new business user joins the team, the application business owner attests and provides relevant roles and access levels for the business user.
- When a business user leaves the team or changes roles, the application business owner validates the user and the user's access level for any updates or removal.
- At predetermined intervals (prescheduled part of calendar of activity), a business user access review is automatically triggered or manually initiated. The application business owner receives a list of existing business users, roles and access privileges. The application business owner then takes action to remove or change any incorrect privileges.
- Any change to the application business owner and/or delegate is to be updated as part of transition from current contact to new contact.

IT User Access Review Best Practices
IT users need to have access to the application back end to execute their responsibilities. IT users' access privileges are dependent on their team and role.

The application's IT owner is responsible for the effectiveness of the user access review control for IT users. The owner can assign a delegate to assist with this activity, but the application's IT owner remains accountable for this control and any violations. The IT owner is the custodian of the business data. Therefore, after the IT owner completes the access review, he or she must get approval from the application business owner to complete the user access review cycle.

If the application business owner is not an IT expert, the application IT owner can set up a clarification session with the business owner to explain the application and the IT responsibilities. This effort can increase trust between the business team and the IT team and result in a more productive workplace, as improved trust enhances speed and reduces cost.

> "THE SOD ASSIGNS RESPONSIBILITIES AND PRIVILEGES FOR IT TEAM MEMBERS SO THAT NO SINGLE PERSON CAN INTRODUCE FRAUDULENT OR MALICIOUS CODE WITHOUT DETECTION."

Best practices that an application's IT owners can implement to help ensure effective user access reviews include:

- Developing an onboarding template (**figure 1**) that provides the user roles, the tasks for each role and the required access for each task. The onboarding template role responsibilities are based on the segregation of duties (SoD) control (**figure 2**). The SoD assigns responsibilities and privileges for IT team members so that no single person can introduce fraudulent or malicious code without detection. No user can have access that can potentially compromise the control. For example, for change management, a developer

Figure 1—Segregation of Duties (SoD)

	Web Server (Backend Access)			Application Server (Backend Access)			Database Server (Backend Access)			GUI Access		
Team	**Dev**	**QA**	**PROD**	**Dev**	**QA**	**PROD**	**Dev**	**QA**	**PROD**	**Dev**	**QA**	**PROD**
Operations Team												
Analyst	None	Read/ Write	Read/ Write	None	Limited Access (non-sudo access)	Limited Access (non-sudo access)	None	Limited Access (non-sudo access)	Limited Access (non-sudo access)	None	Read/ Write	Read/ Write (limited access)
Project Manager/ Lead	None	Read/ Write	Read/ Write	None	Limited Access (non-sudo access)	Limited Access (non-sudo access)	None	Limited Access (non-sudo access)	Limited Access (non-sudo access)	None	Read/ Write	Read/ Write (limited access)
Supervisor	None	None	None	None	None	None	None	None	None	None	None	Admin Access
Development Team												
Analyst	Read/ Write	None	None	Full Access	None	None	Full Access	None	None	Admin Access	Read/ Write	Read/ Write (limited access)
Project Manager/ Lead	Full Access	None	None	Full Access	None	None	Full Access	None	None	Admin Access	Read/ Write	Read/ Write (limited access)
Supervisor	None	None	None	None	None	None	None	None	None	Admin Access	None	None
Business Users Team												
Analyst	None	None	None	None	None	None	None	None	None	None	Admin Access	Admin Access
Project Manager/ Lead	None	None	None	None	None	None	None	None	None	None	Admin Access	Admin Access
Supervisor	None	None	None	None	None	None	None	None	None	None	Admin Access	Admin Access
Server Team												
Server Operations Analysis Technician	None	Sudo Access	Sudo Access	None	Sudo Access	Sudo Access	None	None	None	None	None	None
Server Operations Lead	None	Sudo Access	Sudo Access	None	Sudo Access	Sudo Access	None	None	None	None	None	None
Server Operations Supervisor	None	None	Sudo Access	None	Sudo Access	Sudo Access	None	None	None	None	None	None

Figure 2—Onboarding Document

Operations Team Analyst Onboard Checklist

Task	Assigned/ Requested	Approver	Status	Comments
Add Access to QA Webserver—Read/Write	Requested	Application IT approval/ delegate	In-progress	03/18/2018: Raised request 34596 in ticketing tool
Add Access to PROD Webserver—Read/Write	Requested	Application IT approval/ delegate	In-progress	03/21/2018: Raised request 34586 in ticketing tool
Add Access to QA App server—Limited	Requested	Application IT approval/ delegate	In-progress	03/18/2018: Raised request 34123 in ticketing tool
Add Access to PROD App server—Limited	Requested	Application IT approval/ delegate	In-progress	03/21/2018: Raised request 34763 in ticketing tool
Add Access to QA DB server—Limited	Requested	Application IT approval/ delegate	In-progress	03/18/2018: Raised request 34898 in ticketing tool
Add Access to PROD DB server—Limited	Requested	Application IT approval/ delegate	In-progress	03/21/2018: Raised request 34444 in ticketing tool
Add Application QA front end access—Read/Write	Requested	Application business approval/ delegate	Completed	03/19/2018: Business owner approved and provided access 03/16/2018: Raised request 26467 with business owner
Add Application PROD front end access—Limited	Requested	Application business approval/ delegate	Completed	03/19/2018: Business owner approved and provided access 03/16/2018: Raised request 26788 with business owner

Development Team Supervisor Onboard Checklist

Task	Assigned/ Requested	Approver	Status	Comments
Add Application Dev front end admin access	Requested	Application business approval/ delegate	Completed	03/19/2018: Business owner approved and provided access 03/16/2018: Raised request 26888 with business owner

produces code and performs unit testing. A lead then verifies the code and test results and moves the code to a higher environment. The developer cannot move the code to a higher environment, and the lead does not have the ability to develop code.

- Making it mandatory to use an onboarding document when providing access privileges to a user
- Using a calendar of activity (**figure 3**) to mark and initiate periodic user access reviews as part of the enterprise audit and assurance program. Determine the frequency of user access reviews based on the criticality of the asset, the associated risk and user movement dynamics.
- Based on the calendar of activity, automatically triggering or manually initiating IT user access review activity
- Using an offboarding document (**figure 4**) when a user moves out of a role, team or enterprise to remove user access to tools and applications. The review should be scheduled as close as

Figure 3—Calendar of Activity		
Control calendar:		
Jan-2019:	**Feb-2019** 02/15: IT User Quarterly Access Review	**Mar-2019**
Apr-2019 04/15: Business User Half-Yearly Access Review	**May-2019** 05/15: IT User Quarterly Access Review	**Jun-2019**
Jul-2019	**Aug-2019** 08/15: IT User Quarterly Access Review	**Sep-2019**
Oct-2019 10/15: Business User Half-Yearly Access Review	**Nov-2019** 11/15: IT User Quarterly Access Review	**Dec-2019**

Figure 4—Offboarding Document

Operations Team Analyst Offboard Checklist

Task	Assigned/ Requested	Approver	Status	Comments
Remove Access to QA Webserver—Read/Write	Requested	Application IT approval/ delegate	In-progress	09/18/2018: Raised request 83456 in ticketing tool
Remove Access to PROD Webserver—Read/Write	Requested	Application IT approval/ delegate	In-progress	09/21/2018: Raised request 83777 in ticketing tool
Remove Access to QA App server—Limited	Requested	Application IT approval/ delegate	In-progress	09/18/2018: Raised request 83245 in ticketing tool
Remove Access to PROD App server—Limited	Requested	Application IT approval/ delegate	In-progress	09/21/2018: Raised request 83100 in ticketing tool
Remove Access to QA DB server—Limited	Requested	Application IT approval/ delegate	In-progress	09/18/2018: Raised request 83909 in ticketing tool
Remove Access to PROD DB server—Limited	Requested	Application IT approval/ delegate	In-progress	09/21/2018: Raised request 83196 in ticketing tool
Remove Application QA front end access—Read/Write	Requested	Application business approval/ delegate	Completed	09/19/2018: Business owner removed access 09/16/2018: Raised request 95434 with business owner
Remove Application PROD front end access—Limited	Requested	Application business approval/ delegate	Completed	09/19/2018: Business owner removed access 09/16/2018: Raised request 95333 with business owner

Development Team Supervisor Offboard Checklist

Task	Assigned/ Requested	Approver	Status	Comments
Remove Application Dev front end Admin access	Requested	Application business approval/ delegate	Completed	09/19/2018: Business owner removed access 09/16/2018: Raised request 95346 with business owner

possible to the actual time of the offboarding. Ensuring accurate offboarding means eliminating risk due to unauthorized users.

- Developing automated processes for onboarding and offboarding. For example, an onboarding script processes access requests or adds access for various systems and tools based on the SoD. An offboarding script processes access removal requests or access removal from various systems and tools (see **figures 5** and **6**).
- If collaborative tools, such as SharePoint or Webex, are being used and access is requested for users outside of the team(s), assigning an administrator to validate access requests. As part of this assurance, a periodic automatic workflow of access verification and action retention or removal that is based on the request response of yes or no should be configured.
- Reflecting reporting changes holistically. If the user's reporting manager is involved in user attestation and this communication is received by the user's previous reporting manager, manual intervention, including follow-ups, is necessary.

Conclusion

During this time of rapid transformation of how IT and business teams work, enterprises expect security to not be compromised for the speed of delivery. The new DevSecOps culture promises secure, high-quality software faster and implies that security is the underlying core consideration through the IT process. Enterprises need to challenge themselves to improve access review by using automation tools and techniques. By adhering to the disciplines discussed previously, enterprises can assure concerned stakeholders that all is well with respect to user access.

Figure 5—Automating Onboarding

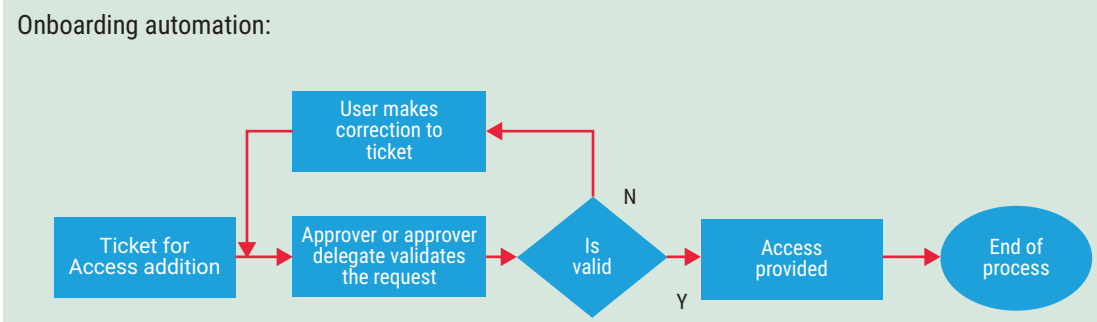

Figure 6—Automating Offboarding