Kurzübersicht
Kulturreferat
Prozess Berechtigungsvergabe

Überblick zum Prüfungsgegenstand
Das Kulturreferat hat mit seinen unterschiedlichen Aufgabenstellungen eine komplexe IT-Umgebung und hohe Sicherheitsanforderungen an die Vergabe von Berechtigungen und Zugriffen auf die IT-Systeme. Neben dem dezentralen Informations-, Kommunikations- und Anforderungsmanagement (KULT-GL-dIKA) wurden in verschiedenen Fachdienststellen des Kulturreferats stichprobenartig deren Prozesse im Rahmen der Berechtigungsvergabe geprüft.

Zielsetzung der Prüfung
Ziel dieser Prüfung war es, einen Beitrag zu leisten, die Ordnungsmäßigkeit der Prozesse und die Sicherheitsanforderungen an die Berechtigungsvergabe zu gewährleisten.

Prüfungsergebnisse (Zusammenfassung)
- Der Prozess der Berechtigungsvergabe wird in Teilen nicht durchgängig angewandt und ist nicht schriftlich geregelt.
- Aus den Anträgen geht teilweise nicht hervor, wer diese genehmigt hat und die Mitzeichnungsverpflichtung durch die Geschäftsstellen wurde nicht konsequent eingefordert.
- Die Rechtevergabe und deren Dokumentation ist nicht transparent genug und somit fehleranfällig.
- WDA-Admins der Fachdienststellen verfügen über ein Rollenprofil, das ihnen mehr Rechte zuweist, als sie für Ihre Aufgabenerfüllung benötigen.
- Es ist kein klarer Prozess für die Generierung von Abwesenheitsmeldungen bei personenbezogenen E-Mail-Postfächern bei einer Abwesenheit ab drei Arbeitstagen erkennbar
- Es sind keine verbindlichen Aussagen oder Regelungen zur Deaktivierung von Accounts bei längeren Abwesenheiten vorhanden.
- Bei der telefonischen Übermittlung von Passworten besteht die Gefahr, dass unberechtigte Dritte diese erlangen könnten.

Empfehlungen auf der Basis der Prüfungsergebnisse (Zusammenfassung)
- Der Prozess der Berechtigungsvergabe ist schriftlich und nachvollziehbar zu regeln. In KULT-GL-dIKA ist zu dokumentieren, wer in den jeweiligen Fachdienststellen des Kulturreferats Antragsberechtigter ist.
- Es ist darauf zu achten, dass die Berechtigungen und Zugriffskennungen durch die Fachabteilungen nachvollziehbar beantragt und verantwortet werden und ob die Unterschriften der Geschäftsstellenleitungen tatsächlich erforderlich sind.
- Die Fachdienststellen benennen künftig auf welche Daten und Systeme die User tatsächlich Zugriff benötigen. Es ist zu überprüfen, in wie weit ein Berechtigungskonzept durch Festlegung und Definition von Benutzergruppen und -rollen eingeführt werden kann.
- Die Zugriffsberechtigungen der Mitarbeiterinnen und Mitarbeiter sind abhängig von deren jeweiligen Aufgaben zu bereinigen.
- Es ist referatsweit kritisch zu hinterfragen, ob Abwesenheitsmeldungen bei mehr als drei Tagen Abwesenheit dienstlich erforderlich sind. Entsprechend sind die Ergebnisse und neuen Prozesse zu dokumentieren.
- Im Rahmen des Risikomanagements ist zu überprüfen, ob und ab wann im Kulturreferat Accounts bei längeren Abwesenheiten zu deaktivieren sind. Die Ergebnisse sind zu dokumentieren. Ein daraus resultierender Prozess ist festzulegen und zu kommunizieren.
- Bei der Übermittlung von Passworten sind sichere Vorgehensweisen zu treffen, die das Risiko reduzieren, dass unberechtigte Dritte deren Kenntnis erlangen. Dies ist schriftlich, verbindlich zu regeln.

Schlussgespräch am 18.06.2014:

Die Dienststelle erklärte, dass die Zugriffsberechtigungen der WDA-Admins inzwischen bereinigt wurden.

Stellungnahme der geprüften Organisationseinheit (Zusammenfassung)

- Seit das KULT-GL-dIKA am 01.01.2012 die Zuständigkeit für alle Institute übernommen hat, ist der Prozess der Berechtigungsvergabe nachvollziehbar geregelt und wird derzeit schriftlich dokumentiert. Es wurden keine Berechtigungen mehr ohne Unterschriften vergeben. In den Fachdienststellen sind Verantwortliche benannt. Auf die Unterschrift der Geschäftsstellen kann nicht verzichtet werden, da nur diese den Berechtigungsstatus der Antragsteller kennen und mit der Unterschrift bestätigen.
- In Zukunft wird auf den Anträgen explizit vermerkt, auf welche Verzeichnisse die Benutzer Zugriff erhalten sollen. Auf ein Rollenkonzept wird verzichtet. Im Kulturreferat gibt es über 350 verschiedene Gruppenberechtigungen und die wenigsten können zu Rollen zusammengefasst werden. Der Aufwand wäre enorm und der Nutzen sehr gering. Das Berechtigungskonzept wird gerade schriftlich dokumentiert.
- Es ist mittlerweile referatsweit geregelt und kommuniziert, dass bei einer Abwesenheit von mehr als drei Tagen auf Antrag der Geschäftsstellen eine Abwesenheitsnachricht eingestellt wird.
- Das Vorgehen und die Regelungen zur Deaktivierung von Accounts bei längeren Abwesenheiten sind noch in Arbeit. Nach der Abstimmung werden diese den Geschäftsstellen analog der Information über die Abwesenheitsmeldungen bei personenbezogenen E-Mail-Postfächern kommuniziert.
- Der Prozess der Passwortvergabe ist einheitlich geregelt und wird derzeit schriftlich fixiert. Im WDA-Stammdatensatz der Mitarbeiterinnen und Mitarbeiter ist grundsätzlich die Personalstammnummer hinterlegt. Diese Nummer kennen außer den Mitarbeiterinnen und Mitarbeitern nur die Personalstellen. Beim Zurücksetzen des Passworts erfolgt die Authentifizierung daher über die Personalstammnummer.
  Neue Kolleginnen und Kollegen erhalten bei Dienstantritt einen verschlossenen Umschlag mit ihrer Personalstammnummer, mit der sie sich anschließend bei der EDV-Hotline für die Erstanmeldung verifizieren können.

Der Rechnungsprüfungsausschuss übernimmt die Prüfungsergebnisse und trägt die Empfehlungen des Revisionsamts mit.