Dass eine solche Mission immer so viel Papierkram bedeuten muss! Immerhin sorgt er dafür, dass du bereits einen guten Überblick besitzt. Aber wahrscheinlich merkst du an dieser Stelle, dass noch zwei wichtige Punkte fehlen:

- Du brauchst eine aktuelle Inventarliste mit allen rechteführenden Systemen oder Anwendungen.
- Jedes rechteführende System – praktisch ist jede einzelne Applikation betroffen – benötigt ein Berechtigungskonzept.

Die klare Schlussfolgerung: Ein IAM-Tool darf nur solche Berechtigungen und Rollen enthalten, die in einem übergeordneten Berechtigungskonzept dokumentiert sind. Außerdem müssen die Berechtigungskonzepte auch nach der IAM-Einführung regelmäßig auf Aktualität geprüft werden. Dazu gehört etwa, sie bei Aufnahme oder Wegfall von Berechtigungen oder Rollen entsprechend anzupassen.

Durch deine akribische Vorarbeit liegen bereits die Mindestangaben für IAM-relevante Dokumente vor. Sie finden sich im Kapitel »Aufbau des Regelwerks« und gelten natürlich auch für Berechtigungskonzepte. Fehlen also nur noch die spezifischen Eckpunkte für die Berechtigungskonzepte.

Eckpunkte für ein Berechtigungskonzept

Ein Berechtigungskonzept deckt alle wichtigen Aspekte ab, die mit dem Zugriff auf Daten und IT-Systeme zusammenhängen. Dazu gehören die Prozesse, Accounts, Berechtigungssystematik sowie Kontrollen und Überwachung. Für deine Mission kommt es auf jeden einzelnen dieser Aspekte an.

Prozesse

- **Einbindung in IAM-Prozesse**
  Beschreibung, ob und wie diese Anwendung an ein IAM-Tool oder ein PAM-Tool angebunden ist.
- **Erstellung von Berechtigungen**
  Beschreibung, wer Berechtigungen für die Anwendung erstellt
- **Änderung von Berechtigungen**
  Beschreibung, wer Berechtigungen für die Anwendung ändert
- **Löschung von Berechtigungen**
  Beschreibung, wer Berechtigungen für die Anwendung löscht
- **Vergabe und Entzug von Berechtigungen**
  Beschreibung, wer Berechtigungen vergibt und entzieht. Wenn die Anwendung über das IAM-Tool läuft, kann ein Standardtext genutzt werden.

- **Genehmigungsstrukturen**
  Beschreibung, wer Berechtigungen genehmigt. Dabei können unterschiedliche Personen je nach Kritikalität einbezogen werden.
- **Provisionierung und Deprovisionierung von Accounts und Berechtigungen**
  Beschreibung, wer genau die Accounts und Berechtigungen zuweist und entzieht.

Accounts

- **Personal Accounts**
  Beschreibung, welche Arten persönlicher Accounts es in der Anwendung gibt, inklusive Nomenklatur, wenn vorhanden.
- **Non Personal Accounts**
  Beschreibung, welche Arten nicht-persönlicher Accounts es in der Anwendung gibt, inklusive Nomenklatur, wenn vorhanden. Die in Task 16 erstellte Tabelle sollte hier eingepflegt werden.

Berechtigungssystematik

- **Authentifizierung/Autorisierung**
  Beschreibung, wie auf die Anwendung zugegriffen werden kann.
- **Berechtigungsstruktur**
- **Beantragbare Rollen und Berechtigungen**
  Beschreibung, welche Rollen und Berechtigungen bestellt werden dürfen. Hier sollte eine Tabelle mit den notwendigen Attributen, wie Name, Beschreibung, enthaltene Berechtigungen, Zielgruppe, Kritikalität, Accounttyp, SoD-Kennzeichen eingepflegt werden.
- **Weitere Berechtigungsstrukturen bzw. Stufen in der Anwendung**
  Beschreibung, ob es eventuell weitere Berechtigungsstrukturen gibt.
- **Automatische Berechtigungsvergabe**
  Beschreibung, ob Berechtigungen automatisiert vergeben werden.

Kontrollen & Überwachung

- **Segregation of Duties (SoD)**
  Beschreibung, ob die Anwendung SoD-relevant ist und wenn ja, in welcher Form. Das Resultat wird dann in die Tabelle mit den beantragbaren Rollen/Gruppen/Profile/Berechtigungen eingetragen.
- **Nachvollziehbarkeit**
  Beschreibung, wie vergebene Rechte dokumentiert und nachvollzogen werden können.
- **Kontrolle kritischer Berechtigungen**
  Beschreibung, wenn vorhanden, wie kritische Rechte zusätzlich überwacht werden müssen.

- **Rezertifizierung von Berechtigungsstrukturen**
  Beschreibung, wie dieses Berechtigungskonzept überprüft wird.
- **Rezertifizierung von zugewiesenen Berechtigungen**
  Beschreibung, wie die Berechtigungen rezertifiziert werden und damit auch die Einhaltung des Berechtigungskonzepts sichergestellt wird. Für die Detaillierung der Rezertifizierung hat Matthias Finder die Task 09 erstellt. Dort wird erläutert, wie Rezertifizierungen durchgeführt werden.

Zum Schluss nochmal ganz Wichtig: Man muss es fast gebetsmühlenartig wiederholen: Kein IAM ohne gültiges Berechtigungskonzept – nur die Rechte und Rollen, die im Berechtigungskonzept abgebildet sind, dürfen ins IAM.