



المدرسة الوطنية لعلوم التكنولوجيا
École Nationale des Sciences Appliquées d'Oujda



جامعة محمد الأول وجدة
UNIVERSITE MOHAMMED PREMIER OUJDA

UNIVERSITÉ MOHAMMED PREMIER ÉCOLE NATIONALE DES SCIENCES APPLIQUÉES D'OUJDA

Fillière Sécurité Informatique et Cyber-Sécurité (SICS)

PROJET DE FIN D'ÉTUDES - PFE

RÉALISÉ PAR : MOKADDEM MOUSTAPHA

**Étude du paysage normatif lié à la gestion des identités
et comparaison des solutions IGA**

Encadré par :

M. SEFRAOUI Omar : Encadrant (ENSAO)
Mme. GHARNATEI Imane : Encadrante (Deloitte)

Membres du jury :

M. SEFRAOUI Omar : Encadrant (ENSAO)
M. KERKRI Abdelmounaim : Examinateur
M. MADANI Mohamed Amine : Examinateur

Année académique 2022/2023

Note de confidentialité

Certaines données et informations contenues dans ce rapport, qu'elles soient explicites, implicites ou masquées, sont strictement confidentielles. Dès lors toute reproduction, sous quelque forme que ce soit, est strictement interdite, sauf accord préalable de la société.

Dédicaces



A MES TRÈS CHERS PARENTS

C'est grâce à votre amour, votre immense affection, vos encouragements, vos dévouements, ainsi que vos innombrables sacrifices que j'arrive aujourd'hui au terme de ce travail. Que Dieu vous comble de santé et de prospérité, et vous garde longtemps pour que je puisse vous combler à mon tour. J'espère que vous trouverez dans ce travail le témoignage de ma profonde reconnaissance et mon éternel attachement.

A MES SOEURS ET LA TRÈS CHÈRE FAMILLE

Nul mot ne pourra exprimer ma gratitude envers vous. Je vous dédié ce travail en témoignage de ma reconnaissance infinie et mes remerciements pour vos conseils et vos encouragements. Je vous souhaite une vie pleine de bonheur et de succès.

A MES CHERS AMIS ET COLLÈGUES

En souvenir de notre sincère et profonde amitié et des moments agréables que nous avons passés ensemble et qui seront sans doute gravés dans nos mémoires. Veuillez trouver l'expression de mon profond respect et de mon affection la plus sincère.

A TOUS MES CHERS PROFESSEURS

Avec tous mon respect et mon éternelle reconnaissance.

A TOUTES LES PERSONNES

Qui ont participé à l'élaboration de ce travail, à tous ceux que j'ai omis de citer, à tous ceux qui m'aiment.

Remerciements



Je voudrais tout d'abord adresser toute ma gratitude à M. Ayoub ASSAID, manager de l'équipe IAM, ainsi que Mme. Imane GHARNATEI, mon encadrante au sein de l'entreprise, qui ont veillé à ce que je reçois le maximum possible de connaissances pendant la période du Knowledge Transfer surtout, leurs conseils m'ont été d'une grande utilité et d'un appui considérable dans ma méthodologie de travail. Je les remercie également pour leur accueil chaleureux, pour leur orientation, patience et pédagogie malgré la charge de leur emploi de temps, et surtout pour cette opportunité pour bien maîtriser les bases de l'IGA

Je remercie Pr. Omar SEFRAOUI, mon encadrant à l'ENSAO, qui m'a guidée, conseillée et supervisée tout au long de mon stage afin de m'aider à aboutir à l'objectif de mon stage de fin d'études.

Un grand merci à toute l'équipe IAM à DELOITTE MOROCCO CYBER CENTER, spécialement M. Younes AITIFALI , M. Issam SEBTI,M. Oussama BELLAGNAOUI et toute l'équipe de travail sans exception, auprès de laquelle il a été très agréable de travailler et d'apprendre.

Je profite également de cette occasion pour exprimer ma gratitude envers l'ensemble du corps professoral de l'ENSAO, pour leur enseignement tout au long de ces trois années. Je remercie également les membres du jury d'avoir accepté de juger mon travail avec bienveillance. Enfin, je suis reconnaissant envers toutes les personnes qui m'ont soutenue de près ou de loin dans la réalisation de ce projet.



Résumé

Le présent rapport s'inscrit dans le cadre de notre projet de fin d'études où on a effectué une analyse approfondie du paysage normatif lié à la gestion de l'identité, en se concentrant sur la comparaison des solutions de gouvernance et d'administration de l'identité (IGA). L'objectif est d'évaluer comment les solutions IGA aident à atteindre la conformité avec les normes pertinentes pour un client potentiel de l'entreprise, Deloitte Morocco Cyber Center.

Dans ce rapport, on a exploré les concepts fondamentaux de la gestion des identités et des accès (IAM) et de l'IGA, en soulignant leurs distinctions. En outre, on a approfondi les aspects clés de l'IGA, notamment les politiques, les systèmes de demande d'accès, les certifications, et la séparation des tâches (SoD), etc. De plus, on a mené une étude normative détaillée des normes internationales ISO 27001 et NIST CSF. Cette étude nous a permis d'examiner les normes et d'identifier les contrôles spécifiquement applicables aux solutions de gouvernance et d'administration des identités (IGA). En analysant et en extrayant ces contrôles, on a assuré une base solide pour évaluer les capacités de conformité des solutions IGA sélectionnées.

Pour garantir une évaluation complète, on a utilisé une étude comparative indépendante, en s'appuyant sur des sources réputées telles que Gartner et Forrester. Cette étude a permis de sélectionner les deux meilleures solutions IGA disponibles sur le marché, notons les solutions Saviynt et SailPoint. Ensuite, on s'est concentré sur la mise en œuvre des contrôles dérivés des normes ISO 27001 et NIST CSF dans ces solutions. En analysant chaque solution individuellement, on a documenté les actions et configurations spécifiques requises pour réaliser les contrôles identifiés. Cette évaluation a fourni des informations précieuses sur la manière dont les solutions répondent aux exigences de contrôle.

Le rapport a abouti à une évaluation concluante, offrant une analyse comparative des deux solutions. Cette évaluation vise à déterminer leur efficacité à répondre aux exigences de conformité et à aider les organisations dans leurs initiatives de gestion de l'identité.

Abstract

This report is part of our end-of-study project where we conducted an in-depth analysis of the normative landscape related to identity management, focusing on the comparison of Identity Governance and Administration (IGA) solutions. The objective is to assess how IGA solutions help achieve compliance with relevant standards for a potential client of the company, Deloitte Morocco Cyber Center.

In this report, we explored the fundamental concepts of identity and access management (IAM) and IGA, highlighting their distinctions. In addition, we delved into the key aspects of IGA, including policies, access request systems, certifications, and separation of duties (SoD), etc. Also, we conducted a detailed normative study of the international ISO 27000 and NIST CSF standards. This study enabled us to examine the standards and identify controls specifically applicable to Identity Governance and Administration (IGA) solutions. By analyzing and extracting these controls, we ensured a solid basis for assessing the compliance capabilities of selected IGA solutions.

To ensure a comprehensive assessment, we used an independent benchmarking study, drawing on reputable sources such as Gartner and Forrester. This study enabled us to select the two best IGA solutions available on the market. We then focused on the implementation of controls derived from ISO 27000 and NIST CSF standards in the selected solutions, namely Saviynt and SailPoint. Analyzing each solution individually, we documented the specific actions and configurations required to realize the identified controls. This assessment provided valuable information on how the solutions meet the control requirements.

The report resulted in a conclusive assessment, offering a comparative analysis of both solutions. The aim of the evaluation is to determine their effectiveness in meeting compliance requirements and helping organizations with their identity management initiatives.

Acronymes

API Application Programming Interface. 33, 36, 37

ARS Access Request System. 14

AWS Amazon Web Services. 34

CSV comma-separated values. 43

DMCC Deloitte Morocco Cyber Center. 4, 5

EIC Entreprise Identity Cloud. 33

GRC Gouvernance, risque et conformité. 16

IAM Identity Access Management. 1, 5, 7, 8, 12

IGA Identity Governance and Administration. 12

IIQ IdentityIQ. 36, 37

ISO International Organization for Standardization. 17–19, 39, 42, 43, XI

MSSP Managed Security Service Provider. 1, 7, 8

NIST National Institute of Standards and Technology. 22, 39

NIST CSF National Institute of Standards and Technology Cybersecurity Framework. 22, 39, 42, 43, VIII

REST Representational State Transfer. 33, 36, 37

SCIM System for Cross-domain Identity Management. 36

SMSI Système de Management de la Sécurité de l'Information. 17

SOD Segregation Of Duties. 16

Liste des tableaux

2.1	Les contrôles liés à la gestion d'identités dans ISO 27001	21
2.2	Les contrôles liés à la gestion d'identités dans NIST CSF	28
3.1	Les solutions comparées	31
3.2	Benchmarking des solutions IGA	32

Table des figures

1.1	Les services de Risk Advisory	4
1.2	Où sommes-nous situés ?	5
1.3	Les 9 piliers Cyber	5
1.4	Diagramme de Gantt	9
2.1	Gestion des risques dans ISO 27001	18
2.2	Niveaux de maturité NIST CSF	22
3.1	Architecture Saviynt EIC	34
3.2	Architecture Saviynt EIC	35
3.3	Architecture SailPoint IdentityIQ	36
4.1	Affectation d'un propriétaire à un droits d'accès	39
4.2	Règle de génération des noms d'utilisateurs	40
4.3	Importation des utilisateurs	40
4.4	Suppression immédiate des identifiants	41
4.5	Système de demande d'accès	42
4.6	Groupes d'applications	43
4.7	Affectation d'un propriétaire à un droit d'accès	43
4.8	Importation des utilisateurs	44
4.9	Suppression immédiate des identifiants	44
4.10	Système de demande d'accès	44
4.11	Définition des applications	45
4.12	La granularité fine	46
4.13	L'architecture du "SOD RULESET"	46
4.14	Exemples de "SOD RULESET"	47
4.15	Analyse SOD détective	47
4.16	Analyse SOD préventive	48
4.17	Contrôles d'atténuation	49
4.18	Politiques de séparation des tâches	49
4.19	Entitlement Sets	50
4.20	SOD détective	50

4.21 SOD préventive	51
4.22 SOD simulation	51
4.23 Règles techniques	52
4.24 Règles de mise à jour des utilisateurs	52
4.25 Joiner configuration	54
4.26 Architecture de la campagne de Saviynt	55
4.27 Création de la campagne dans Saviynt	55
4.28 Processus de certification	56
4.29 Création de la certification	57
4.30 La certification de SailPoint	57
4.31 Dashboard de certification	58
4.32 Flux de travail d'une double approbation	59
4.33 Flux de travail d'une double approbation	59
4.34 Radar d'évaluation de Saviynt et Sailpoint IIQ	61
4.35 Pourcentage des contrôles utilisés des familles choisies	61

Table des matières

Dédicaces	3
Remerciements	4
Résumé	5
Abstract	6
Liste des Acronymes	7
Liste des tableaux	8
Table des figures	9
Introduction générale	1
1 Chapitre 1 : Contexte général	2
1.1 Présentation de l'organisme d'accueil	3
1.1.1 Présentation générale de Deloitte	3
1.1.2 Risk Advisory	3
1.1.3 Deloitte Morocco Cyber Center	4
1.1.4 Les piliers Cyber de Deloitte	5
1.2 Concepts préliminaires	6
1.2.1 Identités numériques	6
1.2.2 Gestion du cycle de vie des identités numériques	6
1.2.3 Solution de sécurité de l'identité	7
1.3 Cadre du projet	7
1.3.1 Contexte du projet	7
1.3.2 Problématique	8
1.3.3 Objectif du projet	8
1.3.4 Conduite et planification du projet	9
2 Chapitre 2 :État de l'art	11
2.1 Principes fondamentaux liés à la gestion d'identité	12
2.1.1 La gestion de l'identité et de l'accès	12

2.1.2	La Gouvernance et l'administration des identités	12
2.1.3	Relation entre IAM et IGA	13
2.1.4	Système de demande d'accès	13
2.1.5	Les connecteurs	14
2.1.6	Politiques	15
2.1.7	Certification	15
2.1.8	Gouvernance, risque et conformité, et séparation des tâches	16
2.2	Cadre normatif	16
2.2.1	La norme ISO 27001	17
2.2.1.1	Système de gestion de la sécurité de l'information	17
2.2.1.2	Gestion des risques dans ISO 27001 :2013	18
2.2.1.3	La gestion des identités dans ISO 27001	19
2.2.2	NIST CSF	22
2.2.2.1	Niveaux de maturité :	22
2.2.2.2	Fonctions :	23
2.2.2.3	Profils :	24
2.2.2.4	La Famille Contrôle d'Accès (Access Control (AC)) :	24
3	Chapitre 3 :Comparaison des solutions de sécurité de l'identité	29
3.1	Spécification des fonctionnalités	30
3.2	Les produits Comparés	31
3.3	Benchmark des solutions	31
3.4	Présentation des solutions choisies	33
3.4.1	Saviynt	33
3.4.1.1	Architecture Saviynt :	33
3.4.2	SailPoint IdentityIQ	34
3.4.2.1	Architecture SailPoint	35
4	Chapitre 4 : Implémentation des contrôles sur les solutions IGA	38
4.1	Identity Warehouse et système de demande d'accès	39
4.1.1	Saviynt EIC	39
4.1.2	SailPoint IdentityIQ	43
4.2	Séparation des tâches	45
4.2.1	Saviynt EIC	45

4.2.2	SailPoint IdentityIQ	49
4.3	Politiques	51
4.3.1	Saviynt EIC	51
4.3.2	SailPoint IdentityIQ	53
4.4	Certifications	54
4.4.1	Saviynt EIC	54
4.4.2	SailPoint IdentityIQ	56
4.5	Flux de Travail	58
4.5.1	Saviynt EIC	58
4.5.2	Sailpoint IdnetityIQ	59
	Conclusion générale	62

Introduction générale

L'évolution rapide dans notre monde interconnecté a révolutionné notre façon de mener notre vie, de travailler et d'interagir. Cependant, ce progrès a également donné lieu à une évolution parallèle des cybermenaces, les acteurs malveillants adaptent constamment leurs tactiques pour exploiter les vulnérabilités de notre écosystème numérique.

L'une de ces vulnérabilités critiques réside dans la mauvaise gestion des identités, qui a des conséquences considérables pour les individus. En effet, selon le rapport Verizon de 2022 sur les violations de données, 82% de ces violations impliquent un "élément humain". En mettant en place une solution d'IAM robuste, les organisations peuvent gérer de manière centralisée les identités et les droits d'accès des utilisateurs. Cela permet de limiter les risques liés aux erreurs humaines, en contrôlant l'accès aux ressources sensibles et aux données confidentielles et en attribuant des droits d'accès appropriés aux utilisateurs.

C'est là où le rôle des Identity Access Management (IAM) Managed Security Service Provider (MSSP) devient indispensable, proposant un service IAM managé pour gérer l'infrastructure de gestion des identités et des accès des clients avec une présence géographique et un nombre d'employés important. Appliquer les disciplines IAM de manière conforme aux normes liées à la gestion de l'identité est essentiel pour garantir une approche cohérente et sécurisée de la gestion des identités au sein des systèmes informatiques.

C'est dans ce cadre que s'inscrit notre projet, qui vise à faire une étude du paysage normatif relative à la gestion des identités, et essayer de déduire les contrôles qui régissent la gestion d'identité, pour ensuite appliquer et implémenter ces exigences dans les meilleures solutions de gestion d'identité choisies après la mise en place d'une étude Benchmarking. Pour étayer davantage le bienfondé de ces propos, ce rapport retrace les différentes étapes suivies pour atteindre ces objectifs, ces étapes peuvent être résumées en 4 chapitres :

- Un premier chapitre où on présente l'organisme d'accueil, les concepts préliminaires en relation avec l'environnement technique du projet, puis le cadre du projet et la méthodologie de travail.
- Le second chapitre est consacré à la définition des principes fondamentaux liés à l'IAM, puis une étude du cadre normatif du projet sous les normes ISO 27001 et NIST CSF.
- Le troisième chapitre concerne le Benchmark des solutions de sécurité de l'identité.
- Finalement, le dernier chapitre traite l'implémentation des contrôles extraits de l'étude normative pour les solutions SailPoint et Saviynt.

Chapitre 1

CONTEXTE GÉNÉRAL

Introduction

Ce chapitre met le point sur le contexte générale du projet, en présentant l'organisme d'accueil, les concepts préliminaires et ainsi le cadre du projet.

1.1 Présentation de l'organisme d'accueil

1.1.1 Présentation générale de Deloitte

Deloitte est un acteur mondial de référence en Audit & Assurance, Consulting, Financial Advisory, Risk Advisory, et Juridique et Fiscal. Avec plus de 175 ans d'expérience, elle fournit à ses clients de toutes tailles et de tous secteurs des services d'excellence et de proximité[1]. Avec un réseau de firmes membres dans plus de 150 pays, Deloitte associe une expertise de niveau internationale à un service d'excellence pour aider ses clients à trouver des solutions à leurs problèmes les plus difficiles.

Les différents services offerts par Deloitte sont :

- Audit & Assurance
- Consulting
- Financial Advisory
- Tax and Legal
- Risk Advisory

1.1.2 Risk Advisory

Il est crucial, pour une entreprise, de connaître les risques, de les évaluer, les modéliser, afin de prendre des décisions éclairées. Le rôle de Deloitte est d'accompagner les entreprises dans la gestion des risques d'entreprise, la sécurité de l'information et la vie privée, la qualité et l'intégrité des données, le risque stratégique et de réputation, le risque réglementaire, le risque de projet et la Cyber Risk et d'autres activités.

Le service Risk Advisory est organisé autour de cinq grandes catégories de risques :risques stratégiques et de réputation, risques réglementaires, risques financiers, risques opérationnels et risques cyber.

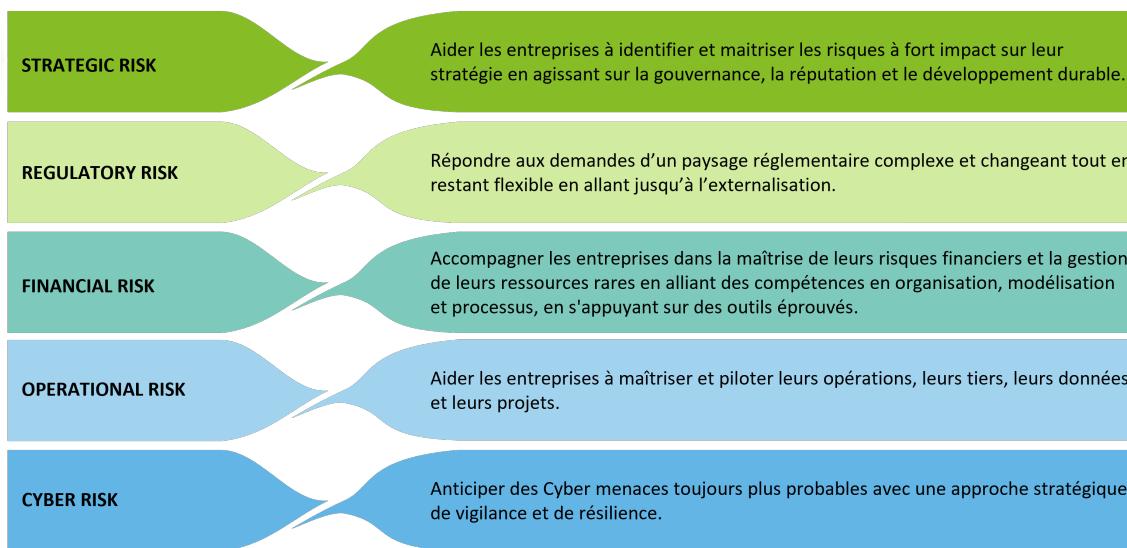


FIGURE 1.1 – Les services de Risk Advisory

1.1.3 Deloitte Morocco Cyber Center

C'est une réalité nécessaire que toutes les organisations doivent reconnaître et intégrer aujourd'hui, car elle est devenue en quelques années un indicateur clé de notre époque : le risque cybersécurité est partout.

Le MCC est le premier centre cyber en Afrique à offrir des services cyber en conformité avec les meilleures pratiques en matière de cybersécurité.

Le MCC dispose d'un pool de spécialistes cybersécurité, de technologies et de services pour répondre au besoin croissant d'expertise cyber, et pour élargir l'offre de services de Deloitte Global. La figure suivante montre où se situe Deloitte Morocco Cyber Center (DMCC) par rapport à Deloitte

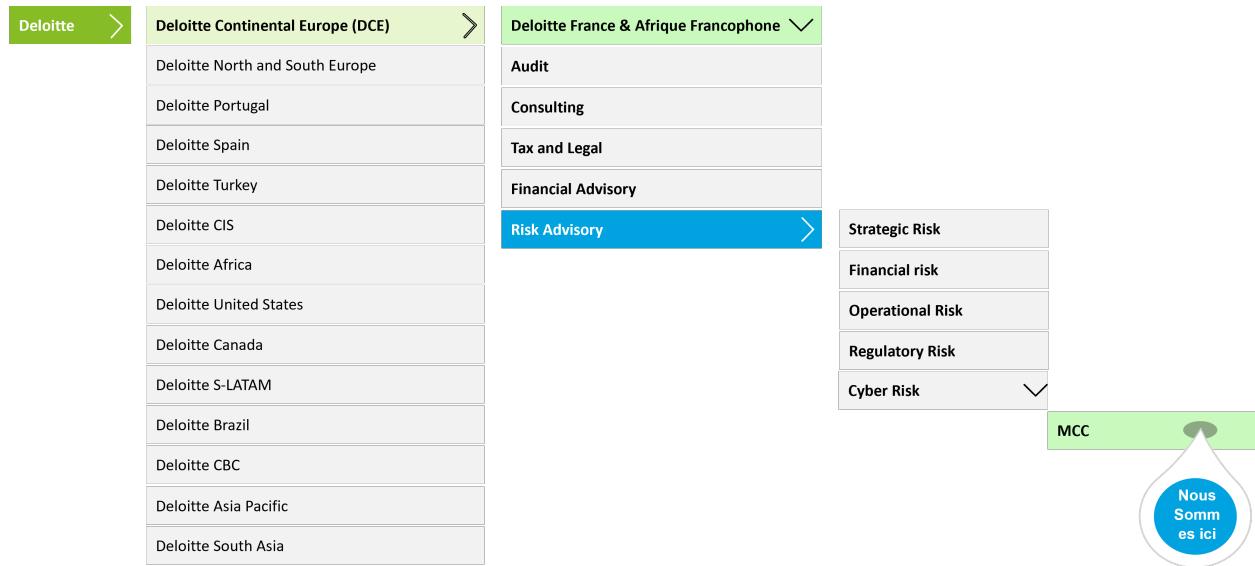


FIGURE 1.2 – Où sommes-nous situés ?

1.1.4 Les piliers Cyber de Deloitte

Deloitte Cyber apporte son soutien aux entreprises pour améliorer leurs performances en résolvant des problèmes complexes, afin qu’elles puissent construire un avenir plus sûr et confiant. Grâce au réseau diversifié de collaborateurs à travers le monde, Deloitte couvre tous les aspects du cyber-risque.

Voici une description de chaque domaine d’expertise :

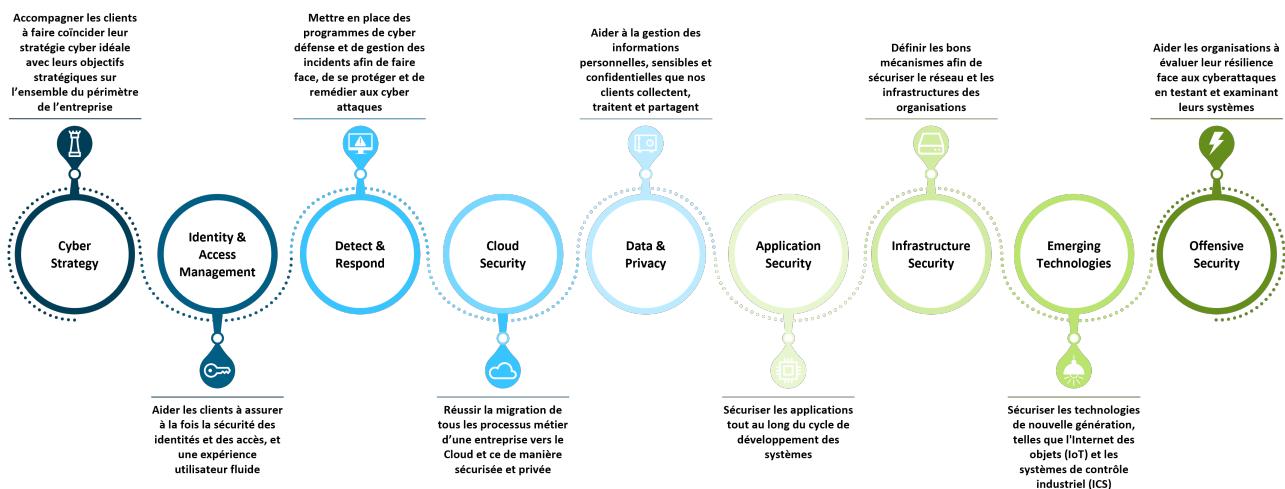


FIGURE 1.3 – Les 9 piliers Cyber

Dans le cadre de mon stage, j’ai eu l’opportunité de travailler sur la partie IAM au sein du Deloitte Morocco Cyber Center (DMCC). Mes missions entraient dans le cadre de la gestion,

la gouvernance et l'administration des identités.

1.2 Concepts préliminaires

1.2.1 Identités numériques

Les identités regroupent tous les utilisateurs qui interagissent avec les systèmes et les données de l'entreprise[9]. Elles comprennent toute personne ou tout objet ayant accès aux systèmes de votre entreprise, y compris les employés, les sous-traitants, les partenaires, et même les entités non humaines telles que des machines, des applications et d'autres composants logiciels. Chaque identité est un ensemble d'informations propres qu'on appelle attributs qui sont souvent à l'origine des processus IGA. Par exemple, la localisation d'un utilisateur peut être utilisée pour lui donner accès à une application. Une identité peut regrouper plusieurs droits qui sont des types d'accès dont dispose un utilisateur lorsqu'il se connecte à une application. Également connue sous le nom de permissions [5].

1.2.2 Gestion du cycle de vie des identités numériques

Chaque fois qu'une organisation recrute un nouvel employé, celle-ci emploie un nouveau contractant ou collabore avec un tiers, celui-ci doit avoir accès aux informations, applications et processus essentiels qui lui permettent d'accomplir les tâches qui lui sont confiées. Toute identité peut avoir accès à diverses ressources et applications de ce type tout au long de sa présence dans l'organisation. Les anciennes ressources peuvent être révoquées et de nouvelles attribuées au fur et à mesure que l'identité change de rôle au sein de l'entreprise. Et au final, lorsque l'identité quitte l'organisation, tous les accès aux ressources sont révoqués. Cela englobe le cycle de vie de l'identité : Rejoindre, Déplacer et Quitter. Lors de la planification de la gestion du cycle de vie des identités pour les employés ou d'autres personnes ayant des relations avec l'organisation, telles que les sous-traitants ou les étudiants, de nombreuses organisations modélisent le processus d'adhésion, de déplacement et de départ. Examinons plus en détail ces processus :

- Rejoindre : lorsqu'une personne a besoin d'un accès, une identité est nécessaire pour ces applications, donc une nouvelle identité numérique doit être créée si elle n'est pas déjà disponible.
- Déplacer : lorsqu'une personne se déplace d'un périmètre à l'autre, des autorisations d'accès supplémentaires doivent être ajoutées ou supprimées à son identité numérique.

- Quitter : lorsqu'une personne quitte le champ d'application de l'accès, il peut être nécessaire de supprimer l'accès et, par la suite, l'identité peut ne plus être requise par les applications, sauf à des fins d'audit et forensics par exemple.

1.2.3 Solution de sécurité de l'identité

Les employés doivent avoir le bon accès à la bonne application et aux bonnes données à tout moment. Puisque l'identité est un élément clé de l'accès aux ressources, les identités doivent être sécurisées. Les organisations détiennent de nombreux types d'identités (représentant les utilisateurs), ces identités ont également besoin d'accéder aux applications, aux données et aux systèmes d'entreprise et les équipes IT doivent maintenir ces applications à jour : les organisations sont en changement permanent. De même avec l'augmentation des exigences réglementaires et des failles de sécurité, les organisations ont plus que jamais besoin de protéger qui a accès aux applications et aux données. Les solutions de sécurité de l'identité répondent à ce besoin, elles permettent de gérer les identités au sein de l'organisation, les comptes auxquels les identités peuvent accéder, les droits associés à chaque compte et les rôles qui permettent une gestion efficace. Aussi, elles aident les organisations à renforcer la sécurité et réduire les risques grâce à une visibilité centralisée de l'identité (détecte les accès inappropriés et les violations des politiques), améliorer la conformité et la performance de l'audit, fournir un accès rapide et efficace, réduire les coûts d'exploitation.

1.3 Cadre du projet

1.3.1 Contexte du projet

Le IAM MSSP propose aux entreprises clientes un service IAM managé pour gérer leur infrastructure de gestion des identités et des accès. Deloitte offre une gamme de services comprenant la gouvernance des identités, la gestion des accès, l'authentification. Ces services sont conçus pour aider les organisations à gérer la sécurité de leurs utilisateurs et de leurs données, à assurer la conformité aux exigences réglementaires et à réduire le risque de cyberattaques. En externalisant la sécurité IAM à un IAM MSSP, les organisations peuvent bénéficier d'une connaissance et d'une expérience des experts dans la gestion d'environnements IAM complexes. C'est dans ce cadre que s'intègre notre projet qui vise à faire une étude du paysage normatif et légal relative à la gestion des identités pour ensuite challenger et vérifier la conformité des solutions de sécurité de l'identité que propose Deloitte avec ces normes.

1.3.2 Problématique

Alors que le paysage des menaces évolue et que les exigences réglementaires deviennent de plus en plus strictes, le choix de la bonne solution IGA est devenu un aspect de plus en plus important de la stratégie de cybersécurité. Cette étude est conçue pour fournir des informations détaillées à Deloitte en tant que fournisseurs de services de sécurité gérés (MSSP) de gestion des identités et des accès (IAM) et à ses clients potentiels dans le choix de la solution de sécurité des identités la plus efficace.

En analysant et en comparant diverses solutions IGA, ce rapport vise à une compréhension complète du paysage normatif lié à la gestion de l'identité, y compris les exigences légales et réglementaires. En outre, cette étude permettra d'identifier la ou les solutions IGA les plus efficaces en termes de conformité à ces normes, de réduction des risques et de protection contre les attaques basées sur l'identité.

Enfin, notre étude facilitera le processus de sélection de Deloitte et de ses clients potentiels, en fournissant une référence précieuse pour aider à choisir la solution de sécurité de l'identité la plus appropriée. En s'appuyant sur les informations fournies dans ce rapport, ils peuvent prendre des décisions éclairées sur leurs stratégies de cybersécurité, en réduisant le risque de failles de sécurité et en garantissant la conformité avec les normes réglementaires.

1.3.3 Objectif du projet

Afin de répondre aux besoins de l'entreprise, ce stage vise à atteindre plusieurs objectifs clés :

- Faire une étude du paysage normatif relative à la gestion des identités : identifier et comprendre les différentes normes et réglementations qui régissent la gestion des identités dans les entreprises et déterminer les exigences en matière de sécurité des identités, de respect de la vie privée et de conformité réglementaire.
- Benchmarking des solutions IGA sur le marché : comparer les différentes solutions IGA et comprendre les fonctionnalités de chaque solution, les exigences techniques et les coûts associés à chaque solution (identifier les forces et les faiblesses) pour finir par sélectionner les solutions IGA les plus appropriées pour répondre aux besoins du client.
- Appliquer les exigences sur les solutions de sécurité de l'identité et challenger ces solutions : Appliquer les exigences identifiées lors de l'étude normative et du benchmarking des solutions IGA sur les deux solutions sélectionnées : Saviynt EIC et SailPoint IIQ. Cette analyse permettra d'identifier les avantages et les inconvénients de chaque solution

en termes de sécurité, de conformité et d'expérience utilisateur.

1.3.4 Conduite et planification du projet

Pour mener à bien un projet et atteindre ses objectifs prédéterminés tout en relevant des défis inattendus, la phase de planification est d'une importance cruciale. Sans elle, le projet manquerait de direction et serait exposé à diverses formes de difficultés et incertitudes. Il est donc impératif que cette phase soit menée avec beaucoup de soin et d'attention aux détails.

En règle générale, la planification d'un projet consiste à décomposer le projet en plusieurs étapes, à estimer le temps nécessaire à chacune d'entre elles et à déterminer leur ordre. Pour faciliter ce processus, nous avons choisi d'utiliser un diagramme de Gantt, qui représente visuellement l'avancement du projet.

Dans le cas de ce projet particulier, nous avons d'abord suivi un programme de formation générale offert par Deloitte avant de commencer notre activité de conseil. Cela nous a permis d'acquérir une compréhension globale de l'écosystème.

Deloitte a mis en place une politique de télétravail autorisant un à deux jours de travail à distance par semaine. En organisant une réunion hebdomadaire avec mon encadrant à Deloitte et une réunion mensuelle avec mon encadrant à l'ENSAO nous avons pu maintenir une collaboration constante, ce qui a permis au projet de progresser sans retard significatif.

Le diagramme de Gantt suivant illustre les différentes étapes du projet :

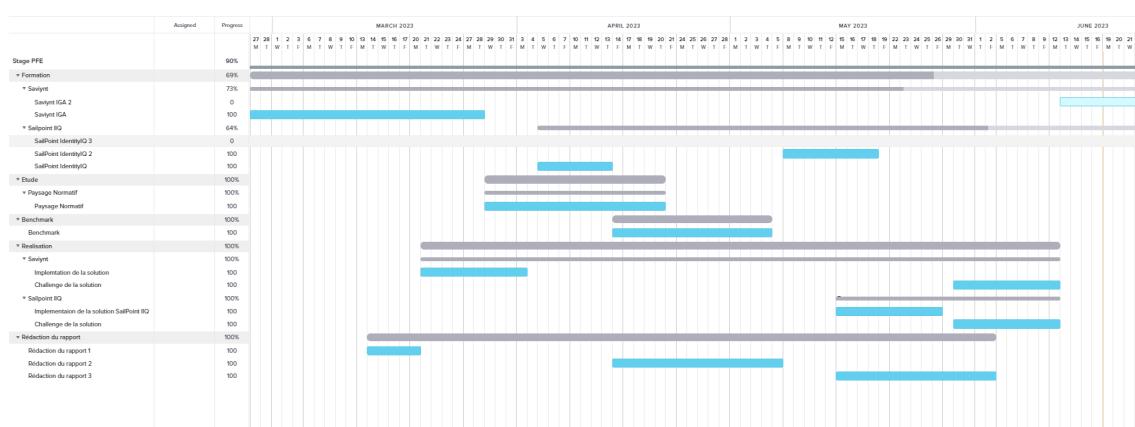


FIGURE 1.4 – Diagramme de Gantt

Conclusion

Dans ce chapitre nous avons circonscrit le périmètre, la problématique, les objectifs et le déroulement de ce projet ainsi que la présentation de l'organisme d'accueil et des concepts

préliminaires.

Chapitre 2

ÉTAT DE L'ART

Introduction

Ce chapitre est consacré à la définition des principes fondamentaux liés à l'IAM, puis fera l'objet d'une étude du cadre normatif du projet sous les normes ISO 27001 et NIST CSF

2.1 Principes fondamentaux liés à la gestion d'identité

2.1.1 La gestion de l'identité et de l'accès

Identity Access Management (IAM) est l'ensemble des processus et politiques liés à la gestion et le contrôle des identités numériques, des priviléges d'accès des utilisateurs dans leurs réseaux et systèmes. L'IAM regroupe le cycle de vie entier des identités qui inclue leur création, modification, surveillance et suppression.

L'IAM incorpore 3 concepts majeurs :

- Identification : c'est la possibilité d'identifier un utilisateur ou une application qui fonctionne sur les systèmes de manière unique. Ceci peut être accompli avec un nom d'utilisateur, ID, ou autre identifiant qui pourrait identifier d'une manière unique.
- Authentification : c'est le pouvoir de prouver qu'un utilisateur ou une application est légitime.
- Autorisation : l'allocation ou la délégation des permissions à un individu spécifique ou un type d'utilisateur. L'autorisation mène à bien les processus IAM au-delà de l'authentification. Les utilisateurs se voient s'accorder des permissions selon leur rôle dans l'organisation.

2.1.2 La Gouvernance et l'administration des identités

Identity Governance and Administration (IGA) fait référence aux processus qui permettent aux organisations de contrôler et de garantir que les identités et les droits de sécurité des personnes restent correctement gérés, sécurisés et suivis. C'est un concept qui offre à l'équipe de sécurité informatique d'avoir une visibilité sur toutes les autorisations de vos utilisateurs et les autorise à les modifier. Aussi il permet d'automatiser les processus d'intégration et de dés intégration, et ainsi économiser du temps et des ressources et de s'assurer que les employés disposent des bonnes autorisations. Les avantages de l'IGA vont au-delà de la sécurité et permettent aussi d'optimiser les flux de travail.

L'IGA est généralement considérée comme faisant partie de l'IAM, et non l'inverse. L'IAM est

un terme plus complet qui englobe tous les aspects de la gestion des identités numériques et de leur accès aux ressources, y compris le provisionnement des identités, l'authentification, l'autorisation et la gestion des accès. L'IGA est un sous-ensemble de l'IAM qui traite des politiques, des procédures et des technologies utilisées pour gérer et contrôler l'accès aux systèmes et aux données au sein d'une organisation.

2.1.3 Relation entre IAM et IGA

La gestion des identités et des accès (IAM) et la gouvernance et l'administration des identités (IGA) sont deux composantes essentielles du cadre de sécurité d'une organisation. Bien que l'IAM et l'IGA soient tous deux essentiels au maintien de la sécurité des données, ils diffèrent par leur champ d'application et leurs fonctionnalités.

L'IAM désigne l'ensemble des politiques, des technologies et des procédures qui permettent à une organisation de gérer et de contrôler l'accès à ses ressources. Les solutions IAM sont principalement axées sur l'authentification, l'autorisation et le contrôle d'accès afin de garantir que seules les personnes autorisées ont accès aux données et aux systèmes.

En revanche, l'IGA se concentre sur la gestion des identités des utilisateurs et de leurs priviléges d'accès. Il fournit une plateforme centralisée pour gérer les identités au sein d'une organisation. Les solutions IGA offrent des fonctionnalités telles que la gestion du cycle de vie des identités, les certifications d'accès et les contrôles de séparation des tâches (SoD) pour aider les organisations à gérer les risques liés aux identités.

2.1.4 Système de demande d'accès

Le système de demande d'accès offre une gestion centralisée des identités et des capacités de gouvernance avec une meilleure visibilité sur qui a accès à quoi. Il met en place un processus permettant au demandeur d'introduire efficacement une demande d'accès et à l'approbateur d'examiner et d'approuver la demande.^[10] L'approbateur désigné reçoit la demande sur la page d'approbation pour examiner les demandes. Il analyse la criticité ou le risque d'accorder des permissions d'accès et prend la bonne décision d'accorder ou de refuser l'accès. Il est également possible que l'organisation dispose d'un système automatisé qui traite les demandes sans approbation individuelle. La gestion des demandes d'accès ne se limite pas à l'approbation ou au refus des demandes d'accès en fonction de l'identité du demandeur ; il s'agit de trouver un équilibre entre la sécurité de l'organisation et l'efficacité opérationnelle.

Un utilisateur peut demander différents types de ressources, comme les applications : Vous

pouvez demander l'accès à un compte d'utilisateur, à des droits, à des priviléges, à des rôles d'application d'une application. L'ARS répertorie toutes les applications configurées par l'administrateur.

Le flux typique d'une demande d'accès peut être divisé en trois étapes :

- L'utilisateur soumet un formulaire de demande.
- Approbation de la demande d'accès.
- Exécution de la demande d'accès.

L'exécution est réalisée en fonction des applications connectées ou déconnectées

- Déconnectées : il n'y a pas de connexion active entre l'application et la solution IGA et par conséquent ils ne peuvent pas communiquer avec et les données ne peuvent pas être échangées automatiquement entre les deux systèmes.
- Applications connectées : Automatiquement provisionnées / exécutées par le biais du connecteur qu'on va détailler dans la partie suivante.

2.1.5 Les connecteurs

Les connecteurs se réfèrent à la configuration pour connecter les solutions IGA aux applications cibles. Lorsqu'une application est déconnectée, cela signifie que les demandes et les approbations sont créées et complétées dans la solution IGA. Une fois les approbations terminées, une tâche est créée et les tickets correspondants peuvent être créés. Les professionnels techniques accomplissent manuellement les tâches de provisionnement dans les applications cibles.

Pour établir une connexion entre la solution IGA et une application cible, il faut configurer un connecteur avec les paramètres de connexion appropriés. Une fois le connecteur configuré, la solution IGA peut établir une connexion avec l'application cible et commencer à échanger des données.

Les paramètres de connexion varient pour chaque connexion. Ces paramètres peuvent être classés en trois grandes catégories : les paramètres de connexion, les paramètres d'importation et les paramètres de provisionnement. Avant de créer une connexion, vous devez examiner les paramètres de connexion requis pour votre connexion dans la documentation du connecteur.

La solution IGA supporte un certain nombre de connecteurs prêts à l'emploi qui permettent de se connecter à différentes applications cibles, notamment AWS, Azure, Box, Salesforce, etc. Ces connecteurs sont préconfigurés avec les paramètres de connexion nécessaires, ce qui facilite l'établissement d'une connexion entre la solution IGA et l'application cible. Cela permet aux organisations d'intégrer rapidement et facilement leurs processus de gouvernance et d'adminis-

tration des identités à leur infrastructure informatique existante, améliorant ainsi l'efficacité et la sécurité.

2.1.6 Politiques

Comme évoqué dans la section 1.2.2 le cycle de vie des identités comporte le processus d'intégration, de déplacement, et de départ d'un employé d'une entreprise. Les politiques permettent de configurer des règles pertinentes pour gérer les divers événements du cycle de vie de l'identité. Il existe différents types de règles pour attribuer ou révoquer automatiquement l'accès en fonction de certaines conditions. Parmi ces types on peut trouver les règles qui donnent des accès de naissance lorsqu'un nouveau employé rejoint l'entreprise, et également des règles pour gérer tous ce qui est mis à jour sur les utilisateurs ou sur les attributs d'une permission, aussi il existe des règles pour gérer toutes les demandes des accès sur le système et des règles pour scanner s'il existe des données et informations confidentielles.

Voici quelques scénarios courants de risques liés à l'accès des utilisateurs, où les politiques jouent un rôle important en automatisant l'attribution et la révocation des permissions aux utilisateurs :

- Les utilisateurs dont le rôle a été modifié mais qui conservent un ou plusieurs privilèges d'accès à leur ancien rôle.
- Les utilisateurs qui ont quitté l'organisation mais qui disposent toujours d'un ou plusieurs privilèges d'accès.

2.1.7 Certification

Un examen périodique des droits des utilisateurs et des privilèges d'accès (comptes, rôles et applications) au sein d'une entreprise est essentiel pour garantir que le privilège d'accès correct est fourni à l'utilisateur. Cela se fait par le biais de la certification, qui implique la vérification par l'utilisateur de son emploi, de la propriété de l'accès . La certification est un processus par lequel une partie responsable s'assure que les personnes et les ressources n'ont accès qu'en cas d'absolue nécessité pour l'exécution d'une fonction. La certification implique également l'approbation (certification) ou le rejet (révocation) de chaque privilège d'accès. Les certifications peuvent être programmées pour être exécutées régulièrement afin de répondre aux exigences de conformité.

2.1.8 Gouvernance, risque et conformité, et séparation des tâches

Gouvernance, risque et conformité (GRC) traditionnellement était utilisé pour classer les applications utilisées pour gérer le risque et la conformité dans une entreprise, ils mettaient en œuvre les technologies GRC pour répondre aux exigences de conformité uniquement pour les applications financières critiques. Par conséquent, toutes les applications utilisées dans l'entreprise n'étaient pas soumises à la gouvernance. Aujourd'hui, GRC couvre de multiples disciplines, y compris la gestion du risque de l'entreprise, la conformité, la gestion du risque des applications tiers, l'audit interne, etc. La GRC se compose de trois éléments principaux :

- La gouvernance : Aligner les processus et les actions sur les objectifs de l'entreprise. La gouvernance est nécessaire pour définir les orientations (par le biais de la stratégie et de la politique), surveiller les performances et les contrôles, et évaluer les résultats.
- Le risque : Identifier et traiter tous les risques de l'organisation.
- La conformité : S'assurer que toutes les activités répondent aux exigences légales et réglementaires.

La séparation des tâches (SOD) est un ensemble de contrôles internes préventifs dans la politique de conformité d'une entreprise qui atténue le risque d'erreur et de fraude dans la comptabilité et les états financiers en exigeant que plus d'une personne effectue une tâche liée à une transaction. Le SOD contribue à protéger l'entreprise contre la fraude en garantissant qu'un même utilisateur n'a pas accès à des applications susceptibles d'être utilisées pour contourner un processus d'approbation. Par exemple : Prenons un scénario dans lequel un utilisateur final a accès à la création d'une facture. En outre, si le même utilisateur a accès à l'approbation de la même facture, il peut en résulter un problème financier qui peut être préjudiciable à l'entreprise. Il s'agit d'une violation du SOD.

Les solutions de sécurité de l'identité fournissent un ensemble de règles prêtes à l'emploi qui peuvent être utilisées facilement pour analyser les risques et les SODs. Il fournit également une analyse des tendances des risques, une analyse de l'impact de la remédiation et une remédiation automatisée.

2.2 Cadre normatif

ISO 27001 et NIST CSF sont deux cadres populaires que les organisations utilisent pour améliorer leur posture de cybersécurité et gérer les risques liés à la sécurité de l'information. Bien qu'ils aient des objectifs similaires, ils proviennent de sources différentes et présentent des

caractéristiques distinctes. C'est deux normes ont été choisies pour les points suivants :

Points forts de la norme ISO 27001 :

- Reconnaissance internationale : est une norme internationalement reconnue, ce qui signifie que les organisations certifiées peuvent démontrer leur conformité aux normes mondiales d'information et de sécurité.
- Amélioration continue : Le cadre ISO 27001 encourage les organisations à adopter une approche d'amélioration continue de la sécurité de l'information, en les obligeant à évaluer régulièrement les risques, à mettre en place des mesures de sécurité appropriées et à surveiller leur efficacité.
- Cadre complet : ISO 27001 fournit un cadre complet pour la gestion de la sécurité de l'information.

Points forts de la norme NIST CSF :

- Flexibilité : Le NIST CSF est un cadre flexible qui peut être adapté aux besoins et aux risques spécifiques de chaque organisation.
- Alignement avec les réglementations et les normes : Le NIST CSF est élaboré par le National Institute of Standards and Technology (NIST), une institution gouvernementale américaine. Par conséquent, il est souvent aligné sur les réglementations et les normes de cybersécurité.
- Langage commun et collaboration : Le NIST CSF fournit un langage commun et une structure de communication pour discuter de la cybersécurité au sein de l'organisation et avec les parties prenantes externes.

2.2.1 La norme ISO 27001

2.2.1.1 Système de gestion de la sécurité de l'information

Système de Management de la Sécurité de l'Information (SMSI) s'agit d'un cadre de politiques, de procédures et de processus conçus pour gérer les risques liés à la sécurité de l'information d'un organisme et protéger les informations sensibles. La norme International Organization for Standardization (ISO) 27001 propose une approche structurée de la mise en œuvre d'un SMSI et de la gestion efficace des risques liés à la sécurité de l'information. [?]

Le SMSI de la norme ISO 27001 est basé sur le cycle Planifier-Faire-Vérifier-Agir (PDCA), qui est un processus d'amélioration continue conçu pour garantir que le SMSI est efficace et aligné sur les objectifs de l'organisation. Le cycle PDCA se compose de quatre phases :

- Plan : Dans cette phase, l'organisation établit les objectifs et les processus nécessaires pour gérer les risques liés à la sécurité de l'information. Il s'agit d'identifier les risques pour la sécurité de l'information, de déterminer le champ d'application du SMSI et d'élaborer un plan de gestion des risques.
- Do : Au cours de cette phase, l'organisation met en œuvre les processus et les contrôles nécessaires pour gérer les risques liés à la sécurité de l'information. Il s'agit notamment de mettre en œuvre les contrôles de gestion des identités dont nous avons parlé précédemment, ainsi que d'autres contrôles de sécurité visant à protéger les informations sensibles.
- Check : Au cours de cette phase, l'organisation surveille et évalue l'efficacité du SMSI. Il s'agit d'effectuer des audits et des examens réguliers afin d'identifier les problèmes et les possibilités d'amélioration.
- Act : Au cours de cette phase, l'organisation prend des mesures pour améliorer le SMSI sur la base des résultats du suivi et de l'évaluation de la phase de contrôle. Il s'agit de modifier les processus et les contrôles afin de résoudre les problèmes identifiés et d'améliorer l'efficacité globale du SMSI.

2.2.1.2 Gestion des risques dans ISO 27001 :2013

Lorsqu'elle conçoit son système de management de la sécurité de l'information, l'organisation doit tenir compte des enjeux et des exigences, et doit déterminer les risques et opportunités qui nécessitent d'être abordés pour empêcher ou limiter l'impact d'un incident. La figure suivante montre l'organisation des risques dans ISO 27001 :

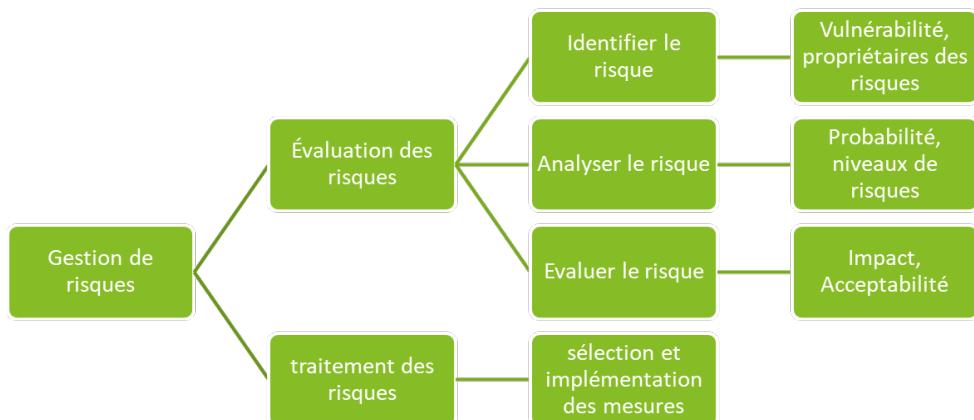


FIGURE 2.1 – Gestion des risques dans ISO 27001

2.2.1.3 La gestion des identités dans ISO 27001

La gestion des identités est un aspect important de la gestion de la sécurité de l'information, et elle est abordée dans la norme ISO 27001 dans le cadre du système de management de la sécurité de l'information (SMSI). La norme ISO 27001 exige que les organisations identifient et gèrent les risques associés à l'utilisation des identités, à la fois au sein de l'organisation et avec des parties externes. Il s'agit notamment de s'assurer que les identités des utilisateurs, des appareils et des systèmes sont correctement gérées et contrôlées afin d'empêcher l'accès non autorisé à des informations sensibles. Plus précisément, les contrôles suivants sont pertinents pour la gestion des identités dans la norme ISO 27001 :

A.9 Contrôle d'accès		
A.9.1 Exigences métier en matière de contrôle d'accès		
Objectif : Limiter l'accès à l'information et aux moyens de traitement de l'information.		
A.9.1.1	Politique de contrôle d'accès	Une politique de contrôle d'accès doit être établie, documentée et revue sur la base des exigences métier et de sécurité de l'information
A.9.2 Gestion de l'accès utilisateur		
Objectif : Maîtriser l'accès utilisateur par le biais d'autorisations et empêcher les accès non autorisés aux systèmes et services d'information.		
A.9.2.1	Enregistrement et désinscription des utilisateurs	Un processus formel d'enregistrement et de désinscription des utilisateurs doit être mis en œuvre pour permettre l'attribution des droits d'accès.

A.9.2.2	Distribution des accès aux utilisateurs	Un processus formel de distribution des accès aux utilisateurs doit être mis en œuvre pour attribuer et retirer des droits d'accès à tous types d'utilisateurs sur l'ensemble des services et des systèmes.
A.9.2.3	Gestion des droits d'accès à priviléges	L'allocation et l'utilisation des droits d'accès à priviléges doivent être restreintes et contrôlées.
A.9.2.4	Gestion des informations secrètes d'authentification des utilisateurs	L'attribution des informations secrètes d'authentification doit être réalisée dans le cadre d'un processus de gestion formel.
A.9.2.5	Revue des droits d'accès utilisateurs	Les propriétaires d'actifs doivent vérifier les droits d'accès des utilisateurs à intervalles réguliers.
A.9.2.6	Suppression ou adaptation des droits d'accès	Les droits d'accès aux informations et aux moyens de traitement des informations de l'ensemble des salariés et utilisateurs tiers doivent être supprimés à la fin de leur période d'emploi, ou adaptés en cas de modification du contrat ou de l'accord.

A.9.4 Contrôle de l'accès au système et à l'information

Objectif : Empêcher les accès non autorisés aux systèmes et aux applications.

A.9.4.1	Restriction d'accès à l'information	L'accès à l'information et aux fonctions d'application système doit être restreint conformément à la politique de contrôle d'accès.
A.9.4.3	Système de gestion des mots de passe	Les systèmes qui gèrent les mots de passe doivent être interactifs et doivent garantir la qualité des mots de passe.

A.9.4.4	Utilisation de programmes utilitaires à priviléges	L'utilisation des programmes utilitaires permettant de contourner les mesures de sécurité d'un système ou d'une application doit être limitée et étroitement contrôlée.
A.6 Organisation de la sécurité de l'information		
A.6.1 Organisation interne		
Objectif : Établir un cadre de management pour lancer et vérifier la mise en place et le fonctionnement opérationnel de la sécurité de l'information au sein de l'organisation.		
A.6.1.1	Fonctions et responsabilités liées à la sécurité de l'information	Toutes les responsabilités en matière de sécurité de l'information doivent être définies et attribuées.
A.6.1.2	Séparation des tâches	Les tâches et les domaines de responsabilité incompatibles doivent être cloisonnés pour limiter les possibilités de modification ou de mauvais usage, non autorisé(e) ou involontaire, des actifs de l'organisation.
A.12 Sécurité liée à l'exploitation		
A.12.4 Journalisation et surveillance		
Objectif : Enregistrer les événements et générer des preuves.		
A.12.4.1	Journalisation des événements	Des journaux d'événements enregistrant les activités de l'utilisateur, les exceptions, les défaillances et les événements liés à la sécurité de l'information doivent être créés, tenus à jour et vérifiés régulièrement.

TABLE 2.1 – Les contrôles liés à la gestion d'identités dans ISO 27001

2.2.2 NIST CSF

Le National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), est un ensemble de lignes directrices et de pratiques robustes et multiformes développé par le très estimé NIST. Introduit en 2014, il vise essentiellement à offrir aux organisations un cadre souple et adaptable leur permettant d'évaluer, de gérer et de renforcer leurs capacités en matière de cybersécurité de manière exhaustive. En s'appuyant sur les normes et les meilleures pratiques de l'industrie, il rassemble les contributions des secteurs public et privé, aboutissant à un cadre complet et inclusif.

Le NIST CSF comprend trois composantes principales qui participent de manière synergique à son efficacité :

2.2.2.1 Niveaux de maturité :

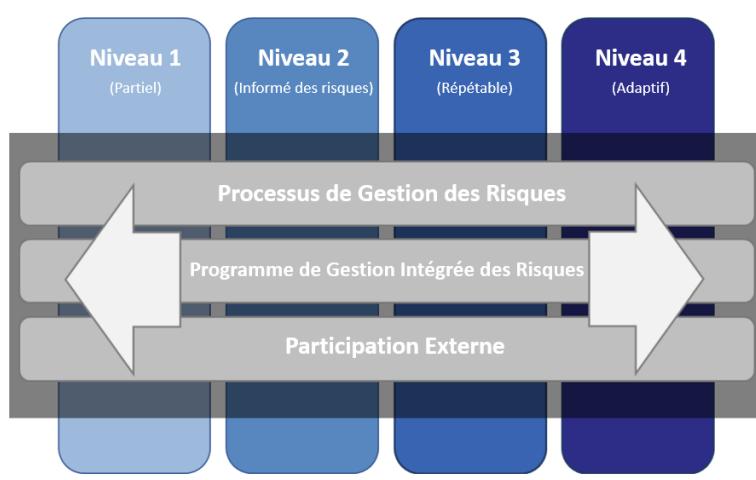


FIGURE 2.2 – Niveaux de maturité NIST CSF

- Niveau 1 - Partiel : Les organisations de niveau 1 ont une connaissance limitée des risques liés à la cybersécurité et ne disposent pas de processus formels pour y faire face. Elles ont une approche ad hoc de la cybersécurité et réagissent souvent aux incidents au cas par cas. Les activités de cybersécurité ne sont pas bien définies ni coordonnées au sein de l'organisation.
- Niveau 2 - Informées des risques : Les organisations de niveau 2 ont une compréhension de base de leurs risques en matière de cybersécurité et ont commencé à mettre en œuvre certains processus de gestion des risques. Elles ont commencé à élaborer un programme de cybersécurité formalisé, mais celui-ci n'est peut-être pas totalement intégré dans les processus généraux de gestion des risques de l'organisation.

- Niveau 3 - Répétable : Les organisations de niveau 3 ont mis en place un programme de cybersécurité structuré et reproductible. Elles ont mis en place des processus et des procédures documentés qu'elles mettent à jour et améliorent régulièrement. Elles ont une bonne compréhension des risques liés à la cybersécurité et ont mis en œuvre des stratégies d'atténuation des risques. Les activités de cybersécurité font régulièrement d'objet d'un suivi et d'un examen de leur efficacité.
- Niveau 4 - Adaptation : Les organisations de niveau 4 disposent d'un programme de cybersécurité mature et adaptable qui est continuellement contrôlé, évalué et amélioré. Elles ont une connaissance approfondie des risques liés à la cybersécurité et adaptent de manière proactive leurs stratégies et leurs pratiques pour faire face aux risques émergents. La culture de la cybersécurité est bien implantée dans l'ensemble de l'organisation et la cybersécurité est intégrée dans tous les aspects des processus opérationnels.

2.2.2.2 Fonctions :

- Identifier : La fonction "Identifier" consiste à comprendre et à gérer de manière globale les risques liés à la cybersécurité. Il s'agit notamment d'identifier et d'inventorier les actifs, d'évaluer les vulnérabilités, de déterminer les impacts potentiels et d'établir des processus de gouvernance pour gérer efficacement la cybersécurité au sein de l'organisation.
- Protéger : La fonction "Protéger" est essentiellement axée sur la mise en œuvre de mesures de protection contre les menaces liées à la cybersécurité. Il s'agit d'élaborer et de mettre en œuvre des politiques, des procédures et des contrôles afin de garantir la confidentialité, l'intégrité et la disponibilité des systèmes, des biens et des données critiques.
- Déetecter : La fonction "Déetecter" met l'accent sur la mise en place de capacités permettant d'identifier rapidement les incidents de cybersécurité. Il s'agit de mettre en place des systèmes et des processus de surveillance pour détecter et analyser les activités anormales, les indicateurs de compromission ou les accès non autorisés. L'objectif est de permettre une réaction rapide et d'atténuer les dégâts ou les dysfonctionnements potentiels.
- Réagir : La fonction "Réagir" implique l'élaboration et la mise en œuvre de stratégies de réaction efficaces pour faire face aux incidents de cybersécurité détectés. Il s'agit notamment d'établir un plan de réponse aux incidents, de définir les rôles et les responsabilités, de coordonner la communication et la collaboration, et d'exécuter les actions appropriées

pour contenir et atténuer l'impact des incidents.

- Récupérer : La fonction "Récupération" est centrée sur l'élaboration et la mise en œuvre de plans et de processus visant à restaurer les capacités ou les services qui ont été affectés par des incidents de cybersécurité. Il s'agit de mener les activités adéquates pour restaurer les données, les systèmes et les fonctionnalités. Il s'agit également d'effectuer une analyse post-incident, d'évaluer les enseignements tirés et de mettre à jour les plans afin d'améliorer la résilience et de prévenir de futurs incidents.

2.2.2.3 Profils :

Les profils représentent l'alignement unique des exigences et des objectifs d'une organisation, de sa propension au risque et de ses ressources sur les résultats souhaités du noyau du cadre de référence. Les profils peuvent être utilisés pour identifier les opportunités d'amélioration de la posture de cybersécurité en comparant un profil "actuel" à un profil "cible".[10]

2.2.2.4 La Famille Contrôle d'Accès (Access Control (AC)) :

Le contrôle d'accès englobe un ensemble sophistiqué de mécanismes, de politiques et de procédures qui permettent aux organisations d'établir et d'appliquer des limites et des restrictions convenables concernant les personnes qui peuvent accéder à des ressources spécifiques, le moment où l'accès est autorisé et les actions qui peuvent être effectuées une fois l'accès accordé. Il vise à empêcher les accès non autorisés, à préserver la confidentialité et l'intégrité des informations sensibles et à garantir que seules les personnes ou entités autorisées sont en mesure d'interagir avec les systèmes et les données critiques.

Contrôle d'accès (Access Control AC)		
AC-2 : Gestion des comptes		
Ce contrôle couvre des activités telles que la création de comptes d'utilisateurs, leur maintien tout au long de leur cycle de vie et la désactivation des comptes lorsqu'ils ne sont plus nécessaires.		
AC-2(1)	Gestion des comptes automatisé	Prendre en charge la gestion des comptes système à l'aide de mécanismes automatisés définis par l'organisation.

AC-2(3)	Désactiver les comptes	Désactiver les comptes dans un délai défini par l'organisation lorsque les comptes : (a) ont expiré ; (b) ne sont plus associés à un utilisateur ou à une personne ; (c) sont en violation de la politique de l'organisation ; ou (d) sont inactifs depuis une période définie par l'organisation.
AC-2(4)	Actions d'audit automatisées	Auditer automatiquement les actions de création, de modification, d'activation, de désactivation et de suppression des comptes.
AC-2(7)	Comptes d'utilisateurs privilégiés	a) Établir et gérer les comptes d'utilisateurs privilégiés conformément à un système d'accès basé sur les rôles et un système d'accès basé sur les attributs ; (b) Contrôler les attributions de rôles ou d'attributs privilégiés. (c) surveiller les modifications apportées aux rôles ou aux attributs ; et (d) révoquer l'accès lorsque l'attribution de rôles ou d'attributs privilégiés n'est plus appropriée
AC-2(8)	Gestion dynamique des comptes	Créer, activer, gérer et désactiver dynamiquement les comptes système définis par l'organisation
AC-3 : mise en vigueur des contrôles d'accès		Ce contrôle vise à renforcer la mise en œuvre et l'application des contrôles d'accès. Il s'agit de rendre les contrôles d'accès plus robustes et plus efficaces en mettant en œuvre des mesures telles que des méthodes d'authentification plus solides, des règles d'autorisation plus strictes, des contrôles d'accès réguliers et la surveillance des utilisations non autorisées

AC-3(2)	Double autorisation	Appliquer la double autorisation pour commandes et actions privilégiées définies par l'organisation
AC-3(3)	Contrôle d'accès mandataire	Les politiques de contrôle d'accès mandataires limitent les actions que les sujets peuvent entreprendre en ce qui concerne la propagation des priviléges, c'est-à-dire qu'un sujet disposant d'un privilège ne peut pas transmettre ce privilège à d'autres sujets.
AC-3(4)	Contrôle d'accès discrétionnaire	Les sujets ne sont pas limités dans les actions qu'ils peuvent entreprendre avec les priviléges auxquelles ils ont déjà eu accès. Ainsi, les sujets auxquels l'accès aux priviléges a été accordé ne sont pas empêchés de transmettre ces priviléges à d'autres sujets
AC-3(7)	Contrôle d'accès basé sur les rôles	Appliquer une politique de contrôle d'accès basée sur les rôles à des sujets et des objets définis et contrôler l'accès en fonction de rôles définis par l'organisation et utilisateurs autorisés à assumer ces rôles.
AC-3(8)	Révocation des autorisations d'accès	Appliquer la révocation des autorisations d'accès résultant de modifications des attributs des sujets et des objets sur la base de règles définies par l'organisation.
AC-3(13)	Contrôle d'accès basé sur les attributs	Appliquer une politique de contrôle d'accès basée sur les attributs aux sujets et objets définis et contrôler l'accès sur la base d'attributs définis par l'organisation pour assumer les autorisations d'accès.

AC-3(15)	Contrôle d'accès discrétionnaire et mandataire	(a) Appliquer la politique de contrôle d'accès obligatoire définie par l'organisation à l'ensemble des sujets et objets couverts spécifiés dans la politique; et (b) Appliquer la politique de contrôle d'accès discrétionnaire définie par l'organisation à l'ensemble des sujets et objets couverts spécifiés dans la politique.
AC-4 : Contrôle du flux d'informations		
Ce contrôle est axé sur la mise en œuvre et l'application de mesures visant à contrôler le flux d'informations au sein des systèmes et des réseaux d'une organisation, afin d'empêcher les flux d'informations non autorisés ou involontaires.		
AC-4(9)	Revue Humaines	Renforcer l'utilisation de revues humaines dans les conditions définies par l'organisation.
AC-5 : Séparation des tâches		
L'objectif de ce contrôle est de s'assurer qu'aucune personne ne contrôle ou n'a accès à des fonctions critiques ou à des informations sensibles au sein d'une organisation, en attribuant des responsabilités différentes à des personnes différentes.		
<ul style="list-style-type: none"> a. Identifier et documenter les fonctions définies par l'organisation devant être séparées. b. Définir les autorisations d'accès au système pour soutenir la séparation des fonctions. 		
AC-6 : Privilège Minimum		
Ce contrôle se concentre sur le principe de l'octroi aux utilisateurs du niveau minimum de priviléges nécessaires à l'exercice de leurs fonctions.		
AC-6(5)	Comptes privilégiés	Restreindre les comptes privilégiés sur le système à personnel ou rôles définis par l'organisation.

AC-6(7)	Revue des privilèges des utilisateurs	a) examiner les privilèges attribués aux rôles ou catégories d'utilisateurs définis par l'organisation afin de valider la nécessité de ces privilèges ; et(b) réattribuer ou supprimer les privilèges, si nécessaire, afin de refléter correctement la mission de l'organisation et ses besoins opérationnels.
---------	---------------------------------------	--

TABLE 2.2 – Les contrôles liés à la gestion d'identités dans NIST CSF

Conclusion

En conclusion, ce chapitre a permis de définir les principes fondamentaux de la gestion des identités et des accès (IAM) à savoir les politiques, les certifications, le SOD, etc... et à examiner le cadre normatif du projet en se référant aux normes ISO 27001 et NIST CSF pour en extraire les contrôles liés à la gestion d'identité.

COMPARAISON DES SOLUTIONS DE SÉCURITÉ DE L'IDENTITÉ

Introduction

Dans ce chapitre, on détaillera les spécifications fonctionnelles puis on passera vers le Benchmarking des solutions IGA pour enfin définir la solution choisie.

3.1 Spécification des fonctionnalités

Les solutions d'administration et de gouvernance des identités existent depuis plusieurs décennies et s'articulent toujours autour du provisionnement des utilisateurs, de l'approbation des accès/demandes, de la recertification des accès, de la gestion des rôles et de la séparation des tâches (SoD). Cependant, les fournisseurs de solutions IGA continuent d'innover, stimulés par les changements importants survenus dans les environnements informatiques et par les efforts de transformation numérique de leurs clients. Ainsi, la plupart des grands fournisseurs proposent désormais des options de livraison SaaS viables, ainsi que des solutions de gouvernance cloud/SaaS en plein essor[2]. Les clients et les prospects de l'IGA sont également confrontés à des structures d'entreprise étendues, des exigences de conformité en constante évolution et d'une diversité croissante d'applications cibles et de droits à travers une variété de comptes d'utilisateurs humains et d'identités non-humaines. En réponse, les fournisseurs de solutions IGA ont investi dans des approches innovantes pour l'automatisation et la rationalisation des flux de travail à plusieurs étapes, ainsi que pour l'amélioration de la rapidité et de l'efficacité de la prise de décision à l'aide de moteurs d'analyse et de l'apprentissage automatique.

Compte tenu de ces tendances, les clients des solutions de sécurité de l'identité devraient rechercher des fournisseurs de solution qui proposent :

- Gestion du cycle de vie
- Gestion des rôles
- Gestion de conformité
- Gestion des risques
- Gouvernance du cloud/SaaS
- Rapports et tableau de bord
- Service et assistance
- Intégration et déploiement
- Etc ...

3.2 Les produits Comparés

Après avoir mis en évidence les besoins qu'un potentiel client doit chercher chez un fournisseurs IGA, le tableau suivant identifie un ensemble de solutions qui offrent les fonctionnalités souhaitables.

Fournisseur	Produit	Version
Oracle [3]	Oracle Identity Governance	12.2.1.4.0
IBM [11]	Security Verify Governance	v10
RSA Security [7]	SecurID Governance & Lifecycle	7.5.0
Okta [4]	Okta Lifecycle Management	N/A
One identity [10]	One Identity Manager by One Identity	8.1.4
SailPoint [11]	SailPoint Identity Platform (IdentityIQ & IdentityNow)	v8.1 & N/A
Saviynt [7]	Saviynt Entreprise Identity Cloud	v20

TABLE 3.1 – Les solutions comparées

3.3 Benchmark des solutions

Le Benchmarking est une méthode d'évaluation comparative utilisée pour mesurer la performance, les pratiques et les résultats d'une entité (entreprise, produit, service, etc.) par rapport à ses concurrents ou à des références de l'industrie. En identifiant les forces et les faiblesses par rapport à des produits concurrents, le benchmarking permet aux organisations de prendre des décisions éclairées pour atteindre leurs objectifs.

La note attribuée à chaque solution par rapport à la catégorie est principalement déterminée par les fonctionnalités fournies par la solution et son niveau de personnalisation, ainsi que par les commentaires des clients et les opinions sur divers sites web tels que Gartner[8] et Forrester[2].

Fournisseur	Oracle	IBM	RSA Security	Okta	One identity	SailPoint	Saviynt
Offre actuelle							
Gestion du cycle de vie	3,9	3,7	3,6	3,9	3,7	4,75	4,8
Gestion des droits	3,8	4,2	4,2	4,3	4,4	4,3	4,4
Système de demande d'accès	3,9	4,1	3,9	4,2	4,2	4,2	4,5
Flux de travail	3,9	4,2	3,9	4,2	4,4	4,3	4,4
Gestion des politiques	3,8	4,2	3,8	4,2	4,2	4,1	4,4
Gestion des rôles	3,4	3,6	3,4	4,4	3,6	4,6	4,2
Gestion des mots de passes	3,8	4,4	3,8	4,6	4,4	4,4	4,2
Gestion de conformité	3,8	3,45	3,3	4,3	3,2	4,1	4,1
Gestion des risques	1	5	1	3,7	5	4	4
Rapports et tableau de bord	2,25	2,5	3,45	4,2	3,5	4,4	4,7
Score /50	33,55	39,35	34,35	42	40,6	43,15	43,7
Intégration et déploiement							
Facilité du déploiement	3,2	3,9	3,9	4,4	4	4,1	4,1
Flexibilité des prix	3,6	3,9	3,9	4,2	4,2	4,3	4,5
Disponibilité des ressources des 3rd-Party	3,7	3,8	3,9	4,2	3,8	4,2	4,2
Intégration des connecteurs	3,7	4	3,9	4,3	4,1	4,5	4,5
Score /20	14,2	15,6	15,6	17,1	16,1	17,1	17,3
Service et assistance							
Rapidité des réponses du fournisseur	3,7	4,2	3,8	4,3	4,1	4,3	4,3
Qualité du support technique	3,7	4,2	3,8	4,3	4,3	4,3	4,3
Score /10	7,4	8,4	7,6	8,6	8,4	8,6	8,6
Total /80	55,15	63,35	57,55	67,7	65,1	68,85	69,6

TABLE 3.2 – Benchmarking des solutions IGA

Pour l'implémentation, nous avons choisi Saviynt EIC et Sailpoint IdentityIQ. Ces choix ont

été faits sur la base des résultats obtenus ci-dessus.

3.4 Présentation des solutions choisies

3.4.1 Saviynt



Saviynt Entreprise Identity Cloud (EIC) pour IGA est une solution avancée de gouvernance et d'administration des identités (IGA) fournie par Saviynt, dans le paysage numérique actuel, elle est conçue pour unifier la gouvernance des identités, l'accès granulaire aux applications et l'accès privilégié avec l'Enterprise Identity Cloud convergé. Pour délimiter le périmètre de sécurité de manière efficace, elle offre une vue unique et holistique des identités organisationnelles où les clients peuvent déterminer la politique, visualiser la posture, mettre en œuvre la conformité et répondre aux risques.

3.4.1.1 Architecture Saviynt :

Saviynt fournit une architecture de micro-services modulaire pour un déploiement et une mise à l'échelle flexibles. L'architecture micro-services divise l'application en ses fonctions principales. Chaque fonction est appelée service et est construite et déployée indépendamment, ce qui signifie que les services individuels fonctionnent sans affecter négativement les autres. Les services individuels communiquent entre eux sans état par l'intermédiaire d'interfaces de programmation d'applications API REST. Elle est construite sur un modèle conteneurisé pour augmenter ou réduire automatiquement l'échelle en fonction de l'utilisation d'un micro-service. On interagit avec une interface utilisateur web qui s'appuie sur une couche business , une couche d'interface utilisateur et une couche de base.

Saviynt utilise généralement une combinaison de technologies de conteneurisation et d'orchestration pour créer et gérer les microservices . Les microservices de chaque client sont déployés et gérés dans un conteneur ou un ensemble de conteneurs distincts, qui sont isolés des autres clients et de l'infrastructure sous-jacente.

- Kubernetes est une plateforme open-source qui automatise la gestion, la mise à l'échelle et le déploiement des conteneurs, en garantissant une haute disponibilité et en simplifiant la gestion des applications. Elle permet la découverte de services, l'équilibrage de la charge, l'autoréparation et prend en charge les mises à jour contrôlées.
- Instances EC2 sont des serveurs virtuels proposés par AWS, qui offrent aux utilisateurs des ressources informatiques personnalisables dans le cloud pour exécuter des applications et des workloads avec des capacités de flexibilité, d'évolutivité et d'intégration.
- Elastic Container Repository est un registre de conteneurs géré par AWS qui stocke et gère en toute sécurité les images de conteneurs. Il simplifie le déploiement d'applications conteneurisées et s'intègre aux services AWS, offrant des fonctionnalités telles que le contrôle d'accès, l'évolutivité et l'analyse des vulnérabilités.
- Terraform est un outil d'infrastructure en tant que code utilisé pour déployer et gérer des ressources d'infrastructure par le biais de scripts de configuration déclaratifs. Il automatise le provisionnement des ressources et permet un déploiement consistant et réitérable de l'infrastructure.

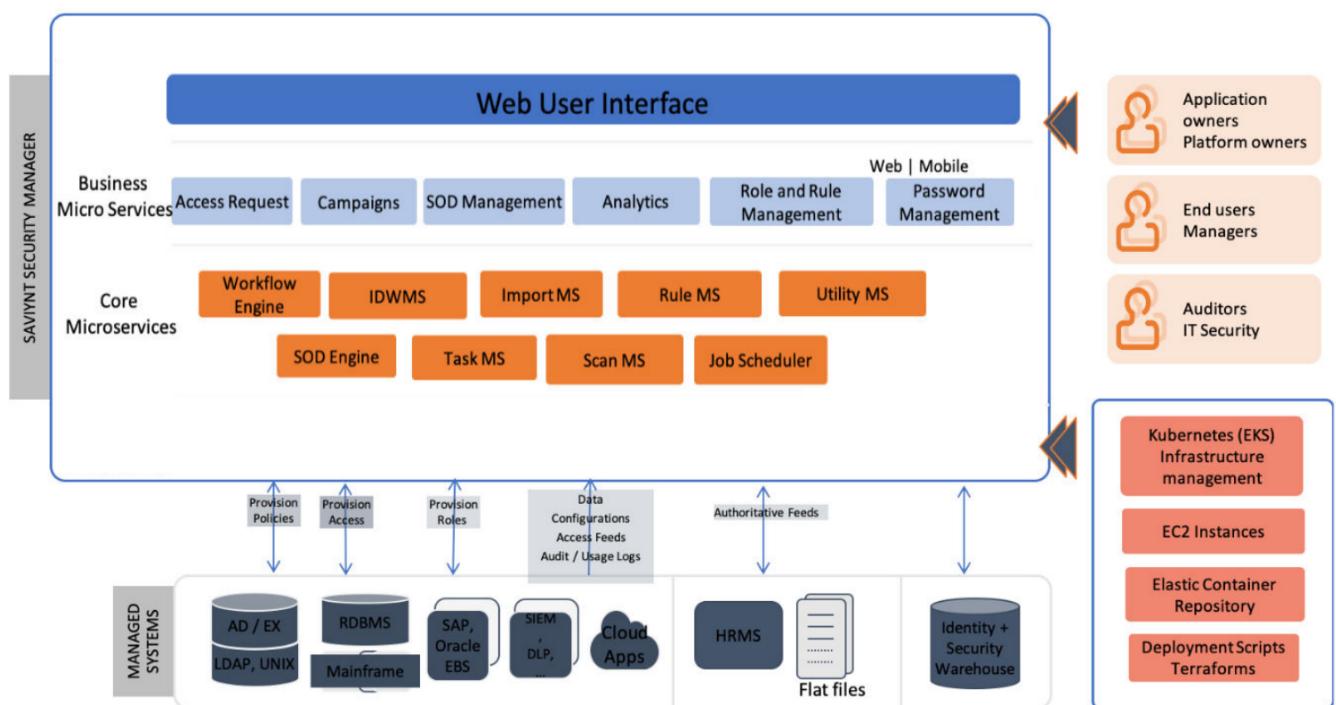


FIGURE 3.1 – Architecture Saviynt EIC

3.4.2 SailPoint IdentityIQ

Au cœur de la sécurité des identités, SailPoint IdentityIQ assure l'efficacité opérationnelle, l'intégration avec les systèmes existants, l'accès à toutes vos identités et la conformité aux entre-

prises dotées d'environnements complexes. SailPoint utilise les modules IdentityIQ Compliance Manager et Lifecycle Manager pour assurer la gestion des accès aux applications utilisées par une entreprise. Les données d'accès aux applications, telles que les personnes disposant d'un compte sur le système et ce qu'elles peuvent faire avec cet accès, sont collectées et stockées dans la base de données IdentityIQ, où elles sont partagées par les deux composants. Ces deux modules partagent également la même interface utilisateur (UI) et les mêmes processus de mise en œuvre.



FIGURE 3.2 – Architecture Saviynt EIC

Le module Lifecycle Manager fournit des demandes d'accès en libre-service pour un modèle d'approbation flexible et une application préventive des politiques. Il fournit également une gestion automatisée des événements du cycle de vie lorsque les utilisateurs rejoignent l'entreprise, changent de rôle ou quittent l'entreprise. Le module IdentityIQ Compliance Manager offre des fonctionnalités permettant de s'assurer que votre organisation respecte les normes de sécurité.

3.4.2.1 Architecture SailPoint

Il s'agit d'une application Java basée sur le web et, en tant que telle, elle doit être installée sur un serveur d'application supporté par un Runtime Java. Tous les objets IIQ sont stockés dans une base de données relationnelle.

Avant l'installation, l'équipe d'implémentation choisit et configure le serveur d'application et le système de gestion de base de données dans lequel la base de données de l'IIQ sera stockée. L'IIQ prévoit également d'accéder à un serveur de courrier électronique (via le protocole standard SMTP).

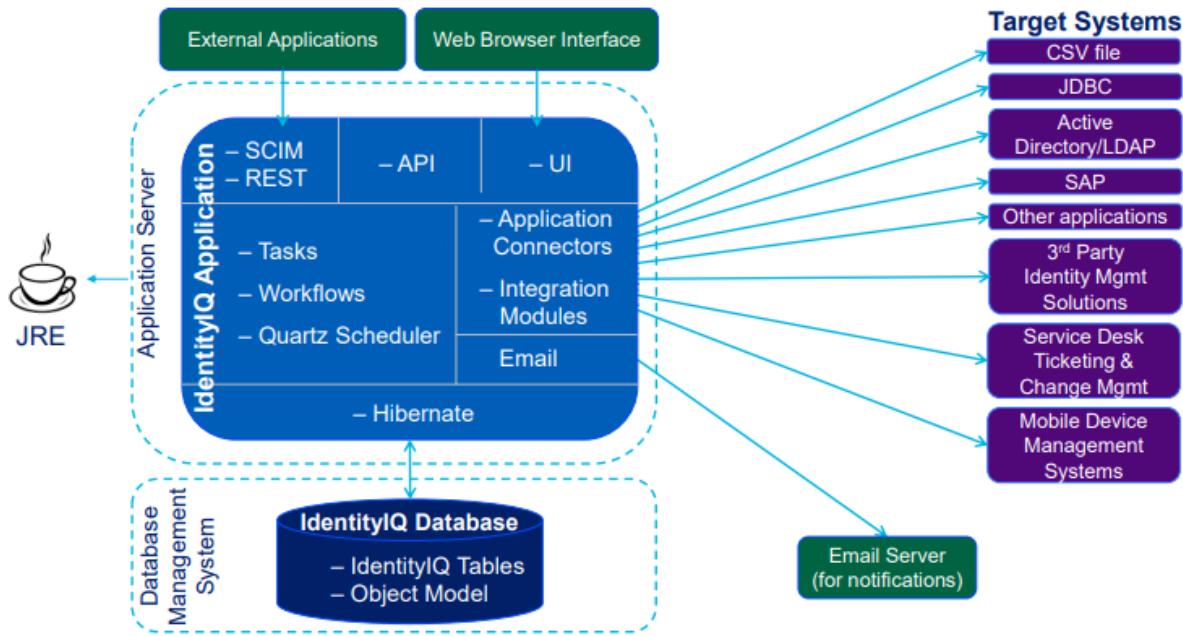


FIGURE 3.3 – Architecture SailPoint IdentityIQ

La boîte supérieure en pointillés représente notre serveur d’application et le carré bleu à l’intérieur représente notre installation d’IdentityIQ. Notre base de données est installée dans son propre serveur de base de données.

Sailpoint utilise un produit appelé Hibernate pour communiquer avec la base de données, il traduit les objets Java dans le modèle de base de données relationnelle. Le planificateur Quartz est utilisé pour programmer des tâches à exécuter régulièrement.

Sur la droite, nous voyons les applications, les systèmes de référence qui sont gérés dans IIQ et les produits tiers qui s’intègrent à IIQ. Les connecteurs et les modules d’intégration d’IIQ se trouvent dans le serveur d’application et doivent pouvoir se connecter à l’application dont vous gérez les données d’accès par l’intermédiaire d’IIQ. IIQ dispose de connecteurs permettant d’accéder à plus de 100 applications, ainsi que d’une API complète permettant d’écrire vos propres connecteurs en cas de besoin.

Nous pouvons faire interagir des systèmes externes avec les identités IIQ via des interfaces Restful. Par exemple, un système tiers qui a besoin de lancer un Workflow IIQ pour le provisionnement, le système externe peut accéder à IIQ via l’API REST. Plus SailPoint prend en charge la norme API pour la gestion des identités des utilisateurs, en appelant le système System for Cross-domain Identity Management (SCIM) pour la gestion des identités inter-domaines. Cette norme simplifie l’interaction entre les applications avec des informations d’identité partagées.

Les appels de l’API SCIM REST peuvent être utilisés pour mettre à jour directement un

compte ou d'autres informations. IIQ dispose d'une api interne qui est plus complète que l'API REST en termes d'accès aux objets internes, lorsque l'équipe rédige des règles, elle utilise l'api interne.

Puis nous avons un accès à l'interface utilisateur où les utilisateurs se connectent et ici nous travaillons avec IIQ par le biais d'une interface de navigateur Web.

Conclusion

Dans ce chapitre nous avons mis en évidence les spécifications fonctionnelles, ensuite nous avons fait un Benchmarking et nous avons présenté les solutions choisies, à savoir : SailPoint IdentityIQ et Saviynt EIC.

IMPLÉMENTATION DES CONTRÔLES SUR LES SOLUTIONS IGA

Introduction

Afin de garantir une sécurité et une protection des données solides au sein d'une organisation, il est essentiel d'adhérer à des normes internationales telles que la norme ISO 27001 :2013 et NIST CSF. Cette section traite un défi auquel l'IGA (Identity Governance and Administration) a dû faire face et de la manière dont elle a réussi à mettre en œuvre les contrôles spécifiés dans la norme ISO 27001 et NIST CSF en matière de gestion des identités.

4.1 Identity Warehouse et système de demande d'accès

Dans le processus d'intégration au sein de Saviynt et SailPoint, plusieurs contrôles de la norme ISO 27001 :2013 et NIST CSF sont mises en œuvre pour garantir une approche sécurisée et contrôlée. Ces contrôles se concentrent sur l'établissement des règles et des procédures pour le processus d'intégration, gestion des Privilèges d'accès et des informations secrètes d'authentification, ce qui est crucial pour prévenir les accès non autorisés et minimiser les risques de sécurité.

4.1.1 Saviynt EIC

Lors de l'importation ou mise à jour des utilisateurs et des droits d'accès, et même lors de la définition des rôles dans Saviynt EIC, nous avons la possibilité d'y affecter un responsable ou un propriétaire conformément aux contrôles A.6.1.1 de la norme ISO 27001 :2013 et de AC-2(1), AC-3(3), AC-3(4) et AC-3(15) de la norme NIST CSF.

USERNAME	RANK	FIRST NAME	LAST NAME	COMMENTS	END DATE
U045101	Primary Certifier	Siu Han	Chung		

FIGURE 4.1 – Affectation d'un propriétaire à un droits d'accès

Pour mettre en œuvre le contrôle A.9.2.1 de manière efficace, Saviynt a développé un processus d'intégration rationalisé au sein de Saviynt EIC. Ce processus comprend plusieurs éléments clés :

- Règle de génération des noms d'utilisateur et des emails :

The screenshot shows the 'Add Register User Rule' configuration screen. It includes a table for defining user generation rules based on attributes like first name and last name. The table has columns for 'Users', 'InitialChar', and 'Action'. There are also sections for 'Special Characters' and 'Mandatory Fields In Register User'.

Users	InitialChar	Action
firstname	1	<button>+ Add</button>
lastname		<button>X Remove</button> <button>+ Add</button>

Special Characters: Enter allowed special characters (@.-_)

Mandatory Fields In Register User: Specify the mandatory user fields fields registering a user(Deprecated)

FIGURE 4.2 – Règle de génération des noms d'utilisateurs

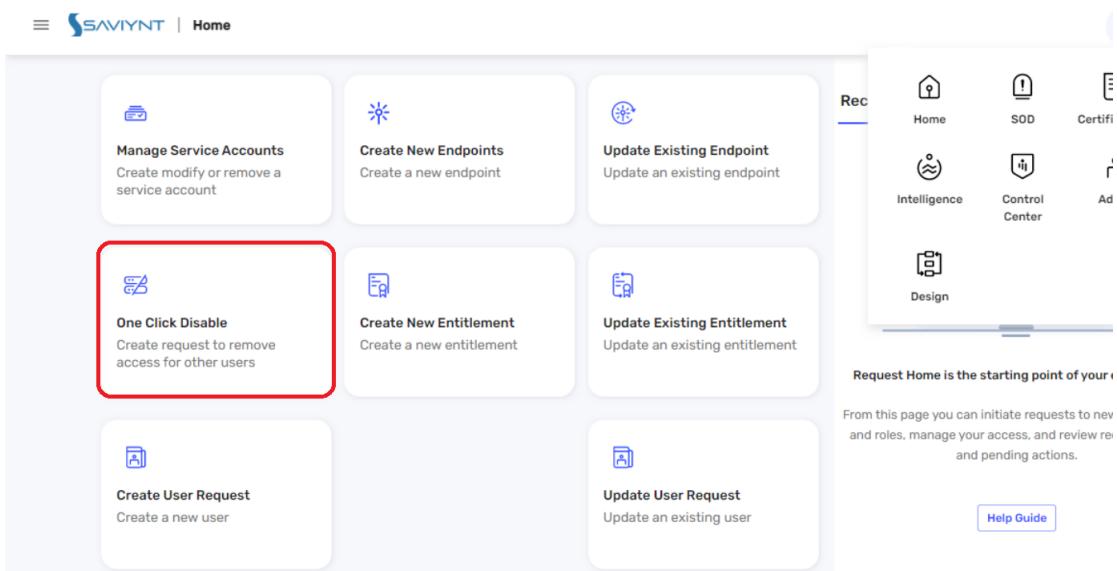
- L'importation des utilisateurs à partir d'un fichier .csv :

The screenshot shows the 'Upload User Preview' screen. It displays a table with columns for USERNAME, FIRSTNAME, LASTNAME, EMAIL, STATUSKEY, and EMPLOYEETYPE. The data rows show various users imported from a CSV file.

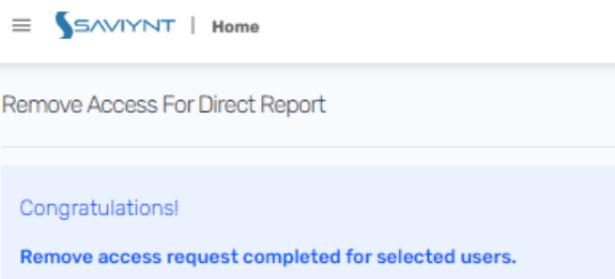
USERNAME	FIRSTNAME	LASTNAME	EMAIL	STATUSKEY	EMPLOYEETYPE
U123455	David	Wallace	[REDACTED]	1	Employee
U123466	Kimberly	Wells	[REDACTED]	1	Employee
U123477	Rachel	Rivera	[REDACTED]	1	Employee
U123488	Nick	Payne	[REDACTED]	1	Employee
U123499	Jason	Smith	[REDACTED]	1	Employee
U231863	Dawn	Miller	[REDACTED]	1	Employee

FIGURE 4.3 – Importation des utilisateurs

- La suppression ou le blocage immédiats des identifiants qui ont quitté l'organisation :



(a) La suppression immédiate sur Saviynt



(b)

FIGURE 4.4 – Suppression immédiate des identifiants

Pour implémenter le contrôle A.9.2.2 et A.9.4.1 et du contrôle AC-6(5), Saviynt a mis en place le système de demande d'accès qui permet aux utilisateurs de demander aux propriétaires des droits et au manager de leur accorder l'accès et ainsi de centraliser les demandes et les droits accordés.

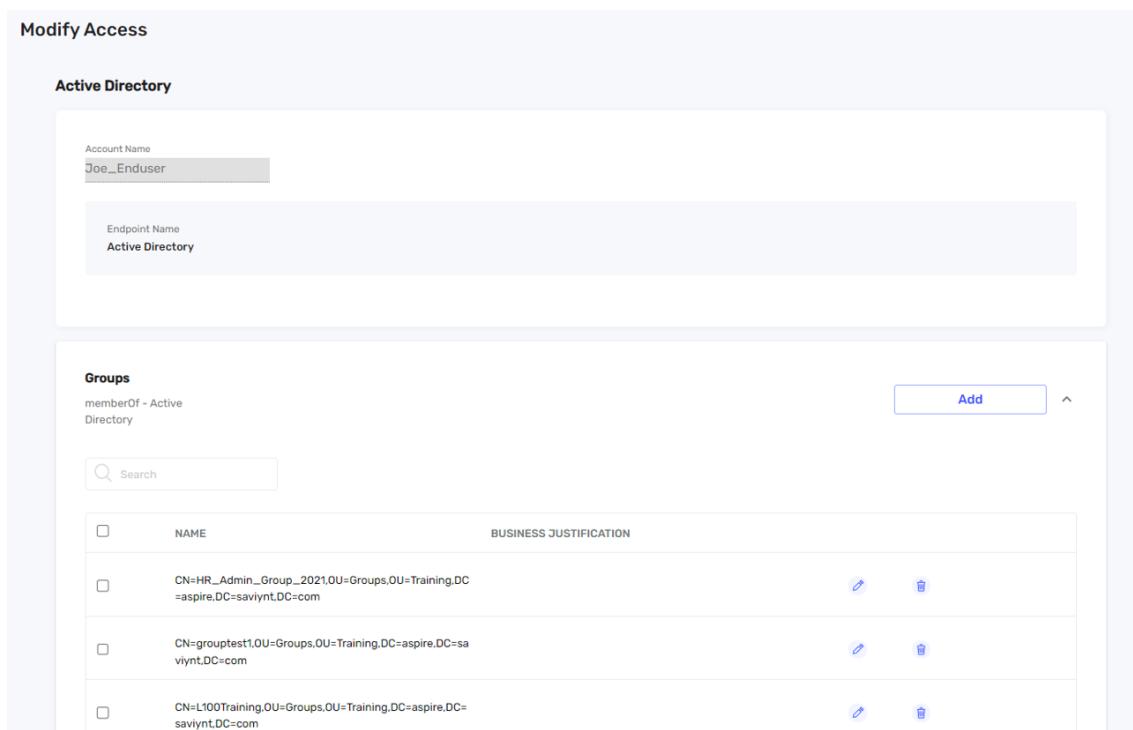


FIGURE 4.5 – Système de demande d'accès

Pour appliquer le contrôle A.9.2.4, la communication des mots de passe temporaires se fait en chiffrant le mots de passe dans un email à part et le nom d'utilisateur dans un autre. Les mots de passe choisis par les systèmes sont générés aléatoirement en se basant sur la politique des mots de passe déjà rédigée sur Saviynt et qu'on va détailler dans une prochaine section.

Saviynt propose de créer des "groupes d'application" sous le nom de 'Security System' ou on peut grouper des programmes utilitaires à privilèges qu'on appelle 'Endpoints' et ceci pour mettre en oeuvre le contrôle A.9.4.4 de la norme ISO 27001 et du contrôle du NIST CSF AC-2(7). On pourra ainsi séparer les programmes utilitaires des logiciels d'application et limiter les accès à ces programmes utilitaires et même d'augmenter le risque d'avoir ces accès.

The screenshot shows the Savyint web interface for managing security systems. On the left, a sidebar has 'Security Systems' selected. The main area is titled 'Security System List' and displays three entries:

SYSTEM NAME	CREATE TASK ACTION	WORKFLOW	STATUS	DEFAULT SYSTEM
Active Directory			Enable	false
Amigopod			Enable	false
AWS	Add :- One_Level_Manager_WF Remove :- One_Level_Manager_WF		Enable	false

FIGURE 4.6 – Groupes d'applications

4.1.2 SailPoint IdentityIQ

Comme pour Savyint, Sailpoint permet l'importation ou mise à jour des utilisateurs et des droits d'accès, tout en affectant un responsable ou un propriétaire à ces derniers, ceci conformément aux contrôles A.6.1.1 de la norme ISO 27001 :2013 et d AC-2(1), AC-3(3), AC-3(4) et AC-3(15) de la norme NIST CSF.

The screenshot shows the SailPoint Entitlement Catalog. It lists two entries:

Application	Attribute	Display Name	Type	Description	Owner
LDAP	groups	AccessBugTracking	Group	Access to Bug Tracking application	Admins
LDAP	groups	Contractors	Group	All contractors at the company	The Administrator

FIGURE 4.7 – Affectation d'un propriétaire à un droit d'accès

Afin de mettre en œuvre le contrôle A.9.2.1 de manière efficace, SailPoint a développé un processus d'intégration rationalisé au sein de SailPoint IdentityIQ. Ce processus comprend plusieurs éléments clés :

- L'importation des utilisateurs à partir d'un fichier .CSV :

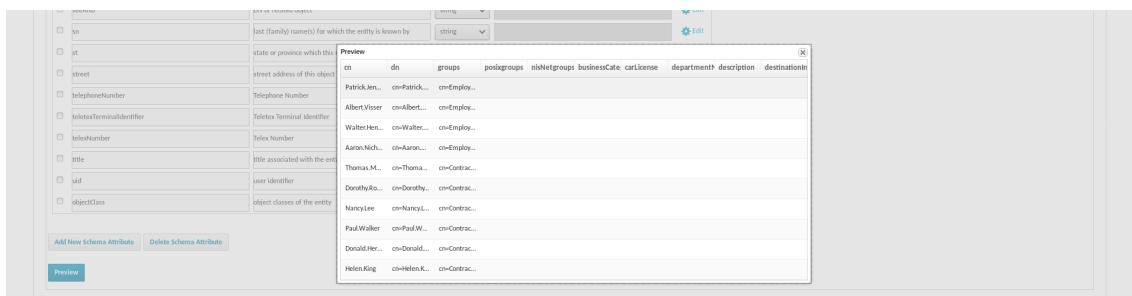


FIGURE 4.8 – Importation des utilisateurs

- La suppression ou le blocage immédiats des identifiants qui ont quitté l'organisation :

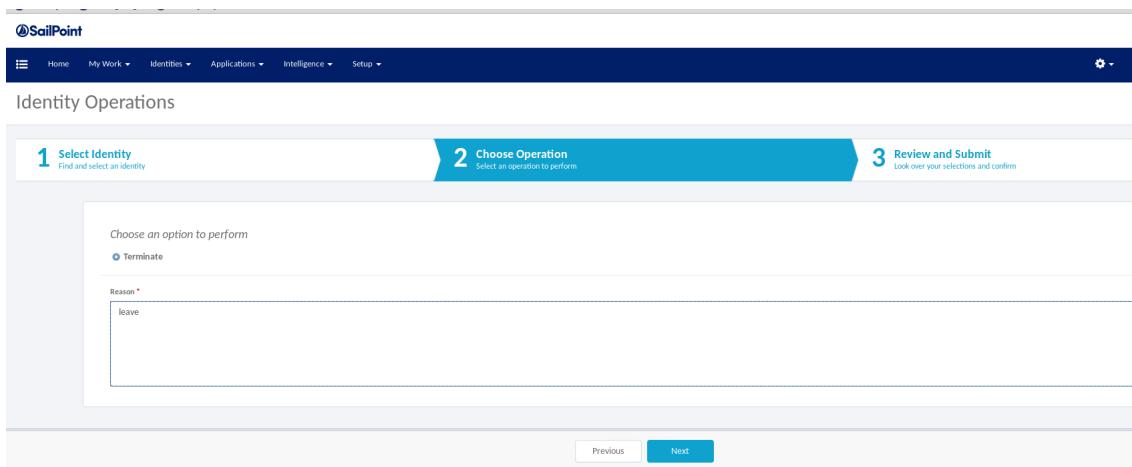


FIGURE 4.9 – Suppression immédiate des identifiants

Pour l'implémentation du contrôle A.9.2.2 et A.9.4.1 et du contrôle AC-6(5) SailPoint a mis en place le système de demande d'accès qui permet aux utilisateurs de demander aux propriétaires des droits, et au manager de leur accorder l'accès, ainsi il est possible de centraliser les demandes et les droits accordés :

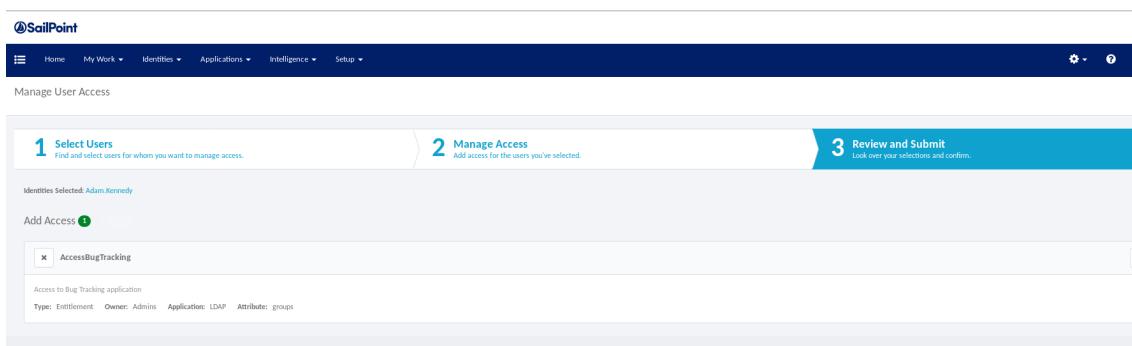
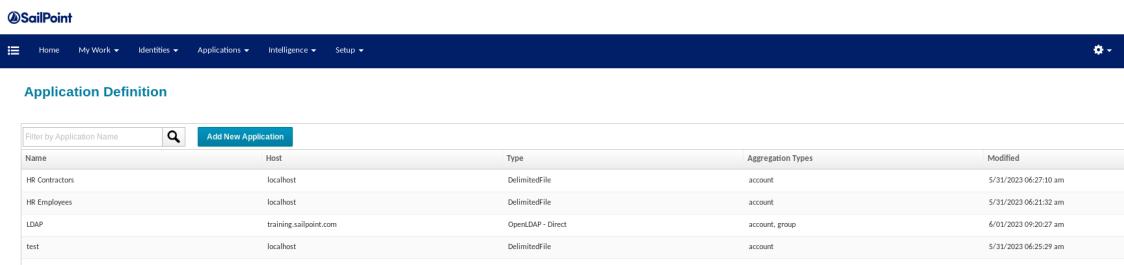


FIGURE 4.10 – Système de demande d'accès

SailPoint propose de définir des applications où on peut créer des programmes utilitaires à priviléges, et ainsi contrôler les accès à ces programmes, ceci pour mettre en oeuvre les

contrôles A.9.4.4 de la norme ISO 27001 et du contrôle du NIST CSF AC-2(7). On pourra, de cette façon, séparer les programmes utilitaires des logiciels d'application et limiter les accès à ces programmes utilitaires, et même d'augmenter le risque d'avoir ces accès.



The screenshot shows the SailPoint application definition interface. At the top, there is a navigation bar with links for Home, My Work, Identities, Applications, Intelligence, and Setup. Below the navigation bar, the title 'Application Definition' is displayed. There is a search bar labeled 'Filter by Application Name' and a button 'Add New Application'. A table lists five applications:

Name	Host	Type	Aggregation Types	Modified
HR Contractors	localhost	Delimitedfile	account	5/31/2023 06:27:10 am
HR Employees	localhost	Delimitedfile	account	5/31/2023 06:21:32 am
LDAP	training.sailpoint.com	OpenLDAP - Direct	account, group	6/01/2023 09:20:27 am
test	localhost	Delimitedfile	account	5/31/2023 06:25:29 am

FIGURE 4.11 – Définition des applications

4.2 Séparation des tâches

Conformément au contrôle A.6.1.2 et le contrôle AC-5 du NIST CSF il convient de séparer les tâches et les domaines de responsabilité incompatibles pour limiter les mauvais usages des actifs de l'entreprise.

4.2.1 Saviynt EIC

Saviynt propose "la granularité fine" avec laquelle le provisionnement, les révisions d'accès et toutes les spécifications de sécurité se font au niveau des droits enfants. Si des modifications sont apportées au niveau des droits enfants, elles seront identifiées dans le ruleset (ensemble de règles). Dans cet exemple, nous avons une visibilité sur les droits enfants comme le T-code et l'Auth Object dans le cas de SAP.

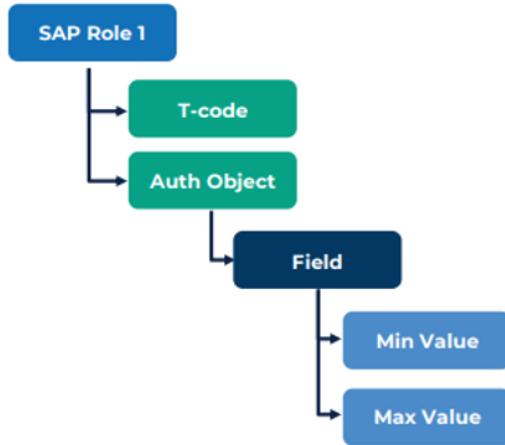


FIGURE 4.12 – La granularité fine

Saviynt fournit un ensemble de règles prêtées à l'emploi qui peuvent être utilisées facilement pour analyser les risques et les SOD. Le workbench de la violation SOD affiche chaque violation SoD avec des informations différencierées telles que la priorité du risque et si l'utilisateur a déjà franchi la violation ou pourrait la franchir, etc. la figure suivante montre l'architecture du "SOD RULESET" au sein de Saviynt :

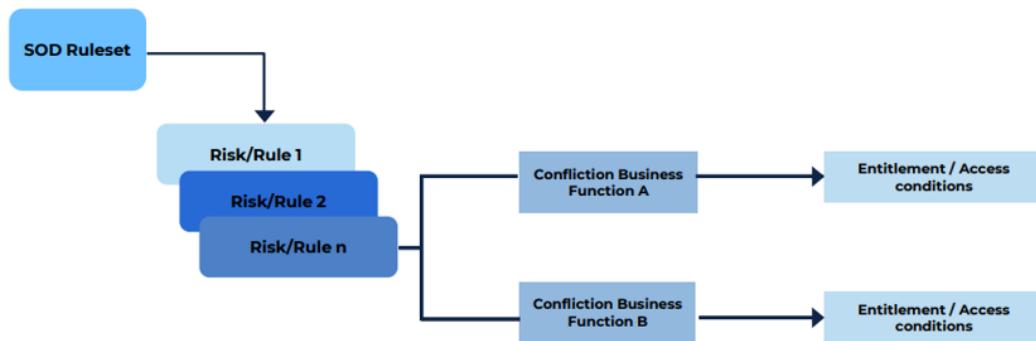


FIGURE 4.13 – L'architecture du "SOD RULESET"

Dans cette architecture on trouve :

- Les fonctions : sont des regroupements logiques de droits d'accès qui définissent la capacité des utilisateurs à effectuer des tâches professionnelles.
- Les risques sont des facteurs/accès conflictuels qui introduisent une incertitude dans la capacité d'une organisation à atteindre ses objectifs. Un risque comprend une ou plusieurs fonctions.

- Ruleset : Un ensemble de risques constitue un Ruleset. Ils peuvent être utilisés pour gérer les fonctionnalités de violation de la SOD.

Dans cette figure on peut voir sur la solution un ensemble de Risks sous le Ruleset oracle :

The screenshot shows the SAVIYNT application interface. In the top left, there's a logo and the text 'SAVIYNT | sod'. On the left side, there's a sidebar with 'Rulesets' and two tabs: 'Ruleset Info' (which is greyed out) and 'Risks' (which is blue). The main area has a green header bar with the text 'Total Risks : 195'. Below this, there's a list of 11 risk items, each with a green background and an 'Active' button with a right-pointing arrow. The risks listed are:

- Approve Invoices conflicts with Payables Payments
- Enter Purchase Order Release conflicts with Payables Invoices
- Enter Purchase Order Release conflicts with Receive Goods and Services
- Payables Invoices conflicts with Payables Payments
- Purchase Orders conflicts with Approval Authorization Control
- Purchase Orders conflicts with Approve Invoices
- Purchase Orders conflicts with Receive Goods and Services
- Create Requisition conflicts with Enter Purchase Order Release
- Create Requisition conflicts with Payables Invoices
- Create Requisition conflicts with Payables Payments
- Create Requisition conflicts with Create Suppliers

FIGURE 4.14 – Exemples de "SOD RULESET"

Saviynt utilise le SOD pour identifier les problèmes à différents stades :

- Analyse SOD détective : Lorsqu'un utilisateur dispose déjà d'un accès, il est porté à l'attention d'une partie responsable.

The screenshot shows a modal dialog titled 'Create New Trigger'. Inside, there are several input fields and dropdown menus:

- Job Name***: Detective_SOD_Evaluation
- Job Type***: SOD Evaluation (RiskSODEvaluationJob)
- SoD Notification**: Select
- Ruleset**: Active Directory_Ruleset
- System**: Active Directory
- Entitlement Evaluation Criteria**: AND ENTITLEMENT_VALUES.ENTITLEMENTVAL...
- User Account Evaluation Criteria**: ACCOUNTS.ACOUNTTYPE = 'A' AND...
- Calculate Inherent Entitlement SOD Violations**: ON

FIGURE 4.15 – Analyse SOD détective

- Analyse SOD préventive : Avant qu'un risque ne se présente, l'analyse SOD préventive permet d'éviter que l'utilisateur ne se voie accorder un accès conflictuel.

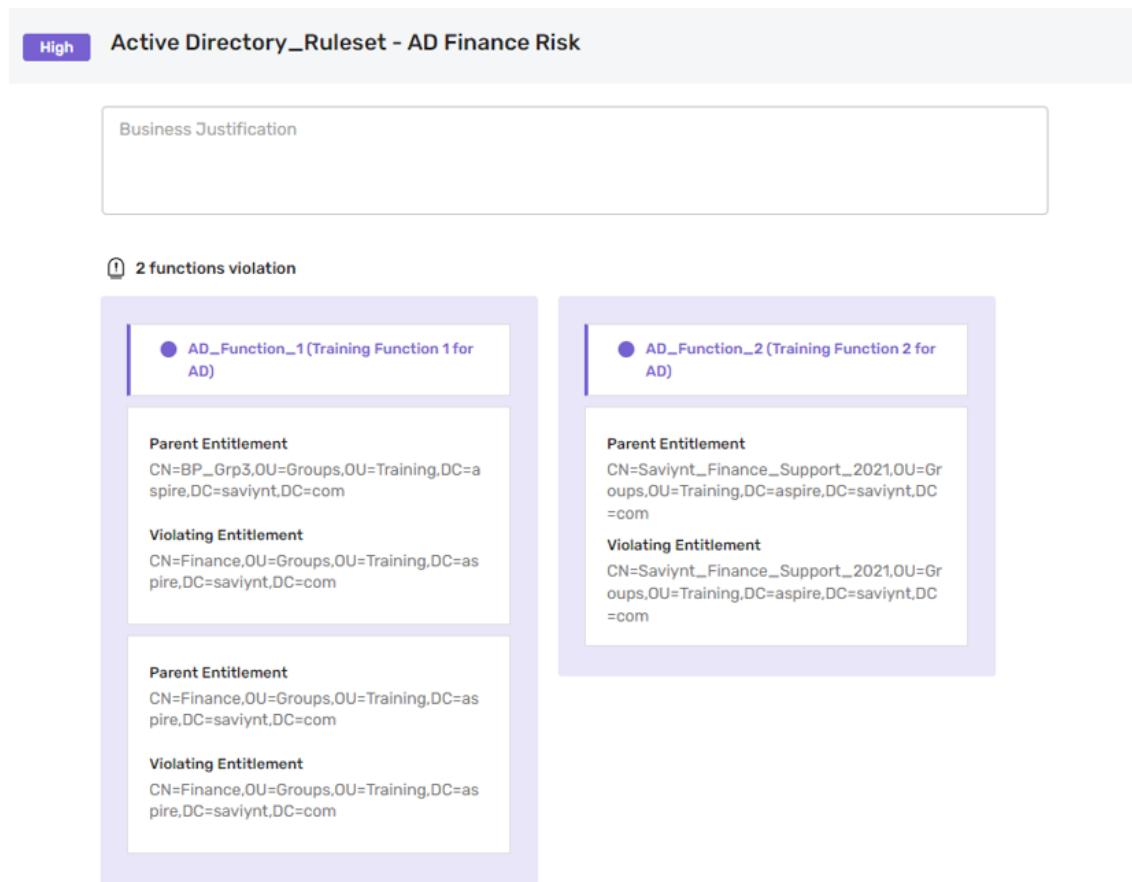


FIGURE 4.16 – Analyse SOD préventive

- Simulation : Capacité à prédire ce qui pourrait se produire lors de la modification d'une application ou d'un accès.

Des contrôles d'atténuation peuvent être mis en œuvre pour limiter le risque posé par un utilisateur violent un SoD ou un accès critique.

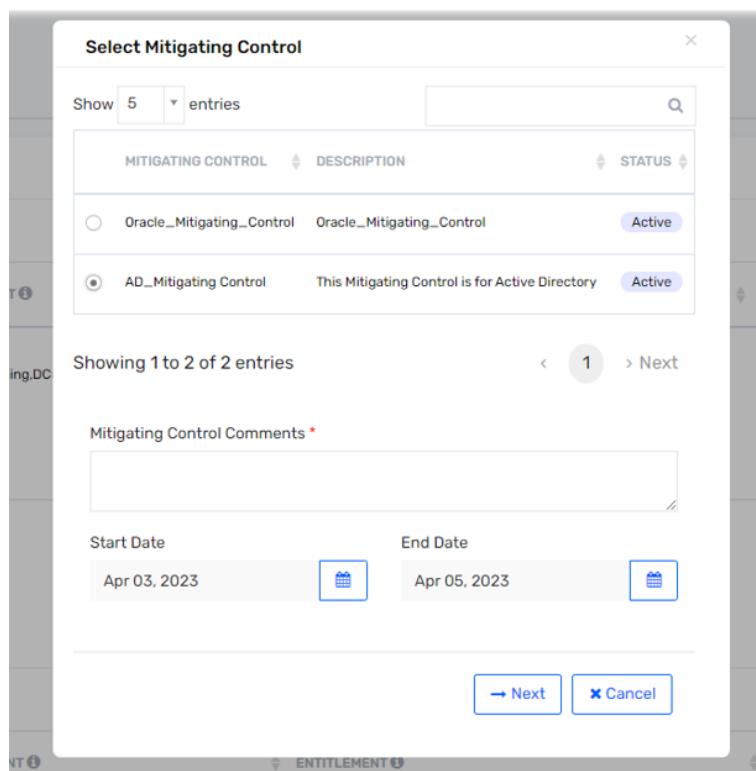


FIGURE 4.17 – Contrôles d’atténuation

4.2.2 SailPoint IdentityIQ

Pour implémenter le contrôle A.6.1.2 et le contrôle AC-5 du NIST CSF dans SailPoint, il propose de créer une politique pour séparer les tâches propres aux droits d'accès.



FIGURE 4.18 – Politiques de séparation des tâches

Réaliser cette séparation revient à créer deux ensembles de droits d'accès (Entitlement Sets), où chaque ensemble doit contenir des droits d'accès propres à une ou plusieurs applications. Les accès dans les deux ensembles ne doivent pas être accordés à un même utilisateur (Violation de politique).

First Entitlement Set

Second Entitlement Set

FIGURE 4.19 – Entitlement Sets

SailPoint fournit trois règles prêtées à l'emploi qui peuvent être utilisées facilement pour la détection, prévention et simulation des violations.

Le SOD est utilisé pour identifier les problèmes aux différents stades cités :

- Analyse SOD détective : Lorsqu'un utilisateur dispose déjà d'un accès, il est porté à l'attention d'une partie responsable

FIGURE 4.20 – SOD détective

- Analyse SOD préventive : Avant qu'un risque ne se présente, l'analyse SOD préventive permet d'éviter que l'utilisateur ne se voie accorder un accès conflictuel.

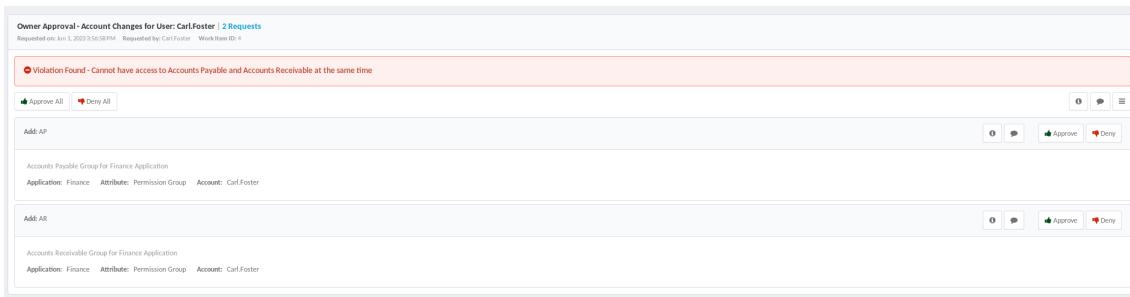


FIGURE 4.21 – SOD préventive

- Simulation : Capacité à prédire ce qui pourrait se produire lors de la modification d'une application ou d'un accès.

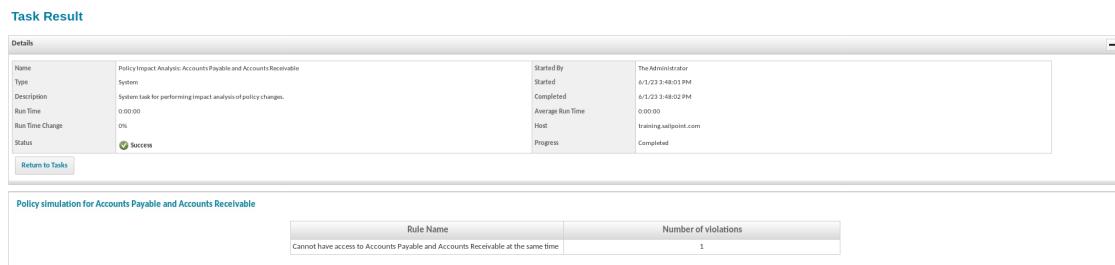


FIGURE 4.22 – SOD simulation

4.3 Politiques

la section 2.1.6 explique l'importance de l'automatisation de l'attribution et la révocation des permissions aux utilisateurs.

4.3.1 Saviynt EIC

Pour mettre en œuvre les contrôles de ISO 27001 A.9.1.1, A.9.2.6 et A.9.2.1 et les contrôles AC-3(13), AC-3(7), AC-2(8) et AC-3(8) de NIST CSF de manière efficace, Saviynt a fourni différents types de règles pour configurer des politiques automatisées pour les identités dans l'organisation.

- Règles techniques : Appliquées pour fournir un accès de droit aux employés qui rejoignent une organisation.
- Règles de mise à jour : Utilisées en cas de modification de la valeur de l'attribut de l'utilisateur.
- Mise à jour des droits : Utilisé en conjonction avec un contrôle analytique non élastique de l'exécution de type préventif.

- Règles de requête : Utilisées lorsque des demandes d'utilisateur unique, d'utilisateurs multiples ou d'utilisateurs en masse sont faites à partir du système de demande d'accès.
- Règles d'analyse : Utilisées pour permettre l'analyse de toute information sensible ou confidentielle
- Règles de mise à jour de l'organisation : Utilisées dans le cadre de la gestion des organisations dans l'EIC.

Dans l'exemple suivant nous pouvons voir l'exemple de la création d'une règle technique qui permet lors de la création de vérifier si la ville de l'utilisateur est 'Los Angeles' et va créer automatiquement un compte sur l'application de démonstration et puis on va attribuer l'accès aux deux droits d'accès d'oracle EBS.

NAME	DETAIL	STATUS	ACTION
Employee_City_Rule_LosAngeles	If Users.city EQUALS "Los Angeles" Then Create Account on TrainingDemoApp AND Assign OEBS-Responsibility::ABM SUPERVISOR AND Assign OEBS-Responsibility::ASO_REPORTS	Active	
Employee_City_Rule_Bangalore	If Users.city EQUALS "Bangalore" Then Create Account on OracleEBS AND Assign OEBS-Responsibility::ABM SUPERVISOR AND Assign OEBS-Responsibility::ABM_WEB_REPORTS	Active	

FIGURE 4.23 – Règles techniques

Nous allons créer une règle de mise à jour des utilisateurs si l'attribut de la ville de l'utilisateur devient "Vancouver", l'accès au compte Oracle EBS et ses droits seront révoqués.

NAME	DETAIL	STATUS	DETECTIVE	TYPE	ACTION
User_Transfer	If Users.city is updated "Vancouver" Then (Revoke Selected Access [Endpoint: OracleEBS, Entitlement Value: General Ledger Post - SG, attributeConfig: ("executeOn":0)])	Active	No	User Update Rule	

FIGURE 4.24 – Règles de mise à jour des utilisateurs

Saviynt propose aussi une politique de mot de passe qui permet de définir les règles que les

mots de passe doivent satisfaire, telles que la longueur et le type de caractères autorisés ou non. Vous pouvez imposer des mots de passe forts par le biais de la stratégie de mot de passe dans Enterprise Identity Cloud (EIC). Et ainsi le Contrôle A.9.4.3 sera appliqué dans cette solution.

4.3.2 SailPoint IdentityIQ

IdentityIQ quant à lui prend en charge ces types de politiques pour mettre en œuvre les contrôles de ISO 27001 A.9.1.1. Chaque politique peut contenir une ou plusieurs règles de politique qui constituent l'ensemble de la politique :

- Politique de séparation des tâches : Ce type de politique de séparation des tâches (SOD) vérifie les rôles conflictuels qu'une identité pourrait avoir.
- Politique de séparation des droits : Ce type de politique de séparation des droits vérifie l'existence de droits conflictuels au sein d'une application ou entre applications. Elle est similaire à la politique de séparation des tâches des rôles, mais elle est utilisée pour les valeurs des attributs de l'application qui sont marqués comme des droits dans le schéma de l'application. Il a été détaillé dans la section. 4.2.2
- Politique de contrôle des droits effectifs : Une politique de contrôle des droits effectifs est similaire à une politique de contrôle des droits, mais elle vérifie les droits effectifs plutôt que les droits directs. Les droits effectifs sont tout accès indirect accordé par le biais d'un autre objet, tel qu'un groupe imbriqué, une cible non structurée ou un autre rôle.
- Politique d'activité Lorsque les sources de données d'activité sont activées sur une ou plusieurs applications, ce type de politique peut être utilisé pour vérifier toute activité indésirable, telle que la connexion, la déconnexion, la création ou la suppression de comptes. Une règle d'activité peut d'abord sélectionner les identités à contrôler à l'aide d'un ensemble de filtres. Les identités correspondant à ces critères sont alors évaluées à l'aide des filtres d'activité définis. Une politique d'activité analyse les données d'activité à la recherche d'événements spécifiques, avec la possibilité de sélectionner des périodes de temps, des applications sources et cibles, etc.
- Politique de compte : Les politiques de compte n'ont qu'une seule règle : elles vérifient si une identité possède plusieurs comptes sur une application.
- Politique de risque : Les politiques de risque vérifient si une identité a un score de risque composite égal ou supérieur au seuil configuré. Tout comme la politique de compte, ce type de politique ne comporte qu'une seule règle.

- Politique avancée : Une politique avancée gère les situations où les autres types de politiques ne suffisent pas. Une stratégie avancée peut contenir plusieurs types de règles utilisant des listes de correspondance, des filtres, des scripts, des règles BeanShell ou des populations, ce qui permet une plus grande flexibilité.

Pour mettre en oeuvre les contrôles A.9.2.6 et A.9.2.1 de la norme ISO 27001 SailPoint propose trois processus 'Joiner', 'Mover' et 'Leaver' où on peut gérer le cycle de vie des identités de manière automatique.

La figure suivante illustre un exemple de joiner configuration :

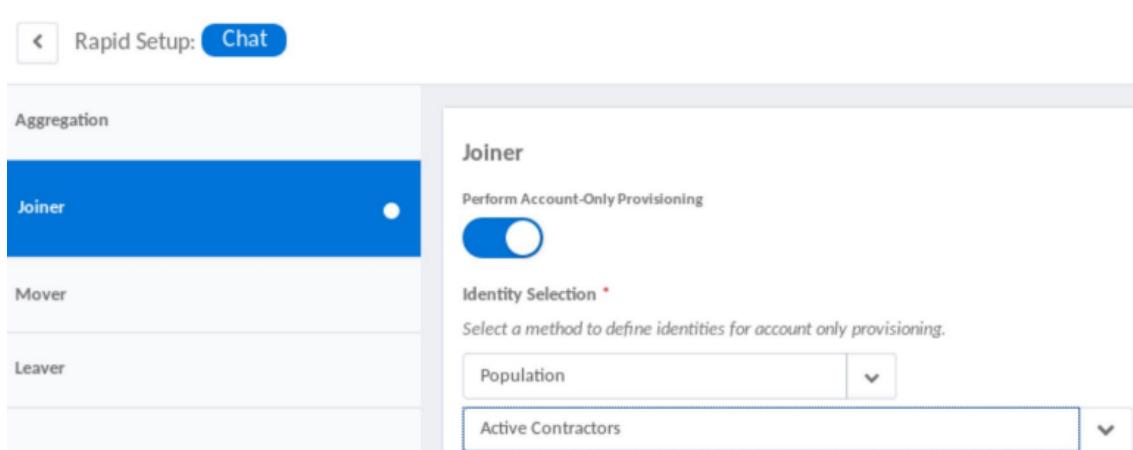


FIGURE 4.25 – Joiner configuration

4.4 Certifications

4.4.1 Saviynt EIC

Comme convenu par la norme ISO 27001 dans le contrôle A.9.2.5 et les contrôles AC-4(9), AC-2(3), AC-2(4) et AC-6(7) convenu par NIST CSF, des revue des droits d'accès utilisateurs doivent être effectuer à intervalles réguliers par les propriétaires des actifs.

Saviynt propose la notion de campagne qui simplifie et regroupe les types de certifications similaires pour qu'au lieu de lancer des certifications individuelles, il est possible d'avoir une campagne unique avec plusieurs certifications englobées dans la campagne. Cela permet de surveiller et d'agir facilement sur toutes les certifications qui font partie de la campagne.

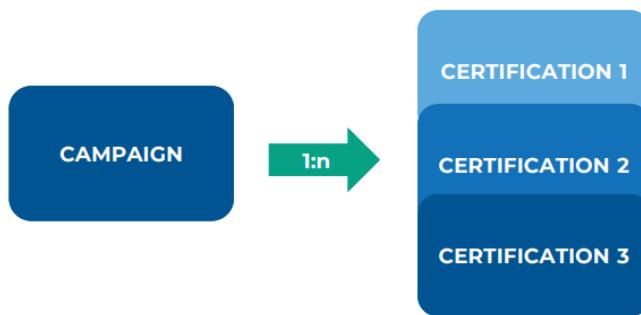


FIGURE 4.26 – Architecture de la campagne de Saviynt

Dans cet exemple nous allons créer une campagne de certification pour vérifier les droits d'accès, les comptes et les rôles pour les valider ou les révoquer :

FIGURE 4.27 – Crédit de la campagne dans Saviynt

Et ainsi, après configuration de la campagne, le certificateur (le manager) pourra commencer à approuver ou de révoquer les droits d'accès :

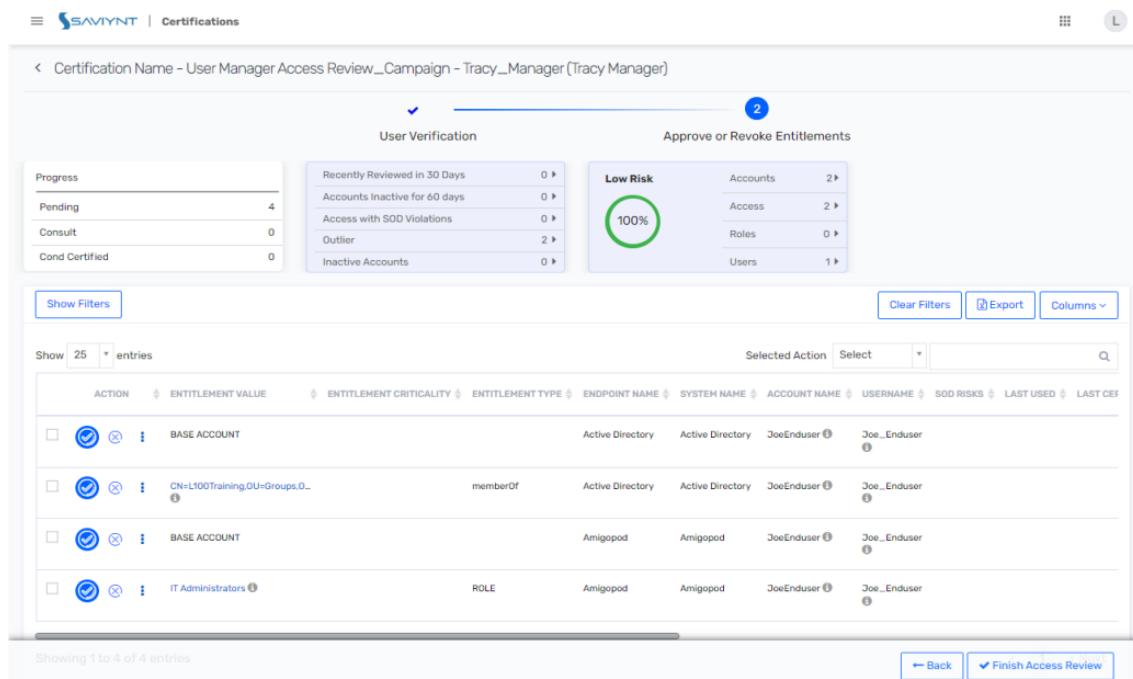


FIGURE 4.28 – Processus de certification

4.4.2 SailPoint IdentityIQ

Dans IdentityIQ, les certifications vous permettent d'automatiser l'examen et l'approbation des privilèges d'accès à l'identité. Dans une certification, IdentityIQ recueille des données d'accès ou d'habilitation très précises et formate les informations dans des rapports interactifs, qui sont envoyés aux réviseurs appropriés en tant que révisions d'accès. Vous pouvez également utiliser les certifications pour valider des éléments tels que les rôles et les groupes de comptes.

Dans cet exemple nous allons lancer une certification pour confirmer l'accès des employés à l'application Finance :

What do you want to certify?

Define the items you would like to certify in this campaign.

Roles / Entitlements Accounts Only

Roles

Additional Entitlements

Application Equals Finance

Include Accounts without Entitlements

Include Policy Violations Exclude Logical Tier Entitlements

Include IdentityIQ Capabilities Filter Logical Application Entitlements

Include IdentityIQ Scopes

FIGURE 4.29 – Créeation de la certification

Après lancement de la certification, le certificateur va pouvoir approuver et révoquer les accès des utilisateurs.

The screenshot shows the SailPoint interface for a 'Targeted Access Review for Admins'. The main area displays a table of entitlements:

Type	Display Name	Description	Application	Account Name	Identity	Decision
Entitlement	ACCOUNTING on Permission Group	Accounting Group for Finance Application	Finance	Carl.Foster	Carl.Foster	<input type="button" value="Approve"/> <input type="button" value="Revoke"/>
Entitlement	IT on Permission Group	IT Group for Finance Application	Finance	Carl.Foster	Carl.Foster	<input type="button" value="Approve"/> <input type="button" value="Revoke"/>
Entitlement	ACCOUNTING on Permission Group	Accounting Group for Finance Application	Finance	James.Smith	James.Smith	<input type="button" value="Approve"/> <input type="button" value="Revoke"/>
Entitlement	FINANCE on Permission Group	Finance Group for Finance Application	Finance	Joe.Silva	Joe.Silva	<input type="button" value="Approve"/> <input type="button" value="Revoke"/>
Entitlement	HR on Permission Group	HR Group for Finance Application	Finance	Joe.Silva	Joe.Silva	<input type="button" value="Approve"/> <input type="button" value="Revoke"/>

FIGURE 4.30 – La certification de SailPoint

SailPoint offre aussi un dashboard pour pouvoir voir l'avancement de la certification :

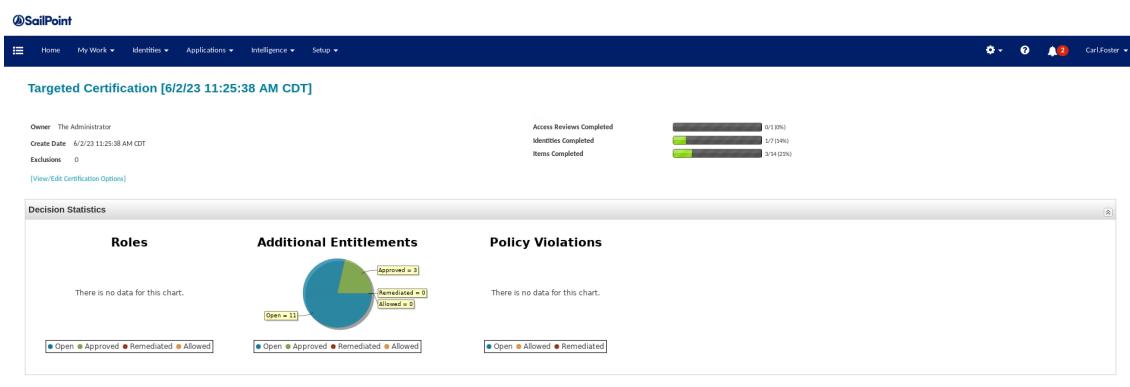


FIGURE 4.31 – Dashboard de certification

4.5 Flux de Travail

La création des flux de travail convenable est essentiel pour établir un processus normalisé et contrôlé de demande et d'approbation d'accès. Les flux de travail garantissent la cohérence, la séparation des tâches, la conformité, l'atténuation des risques et l'allocation efficace des ressources.

4.5.1 Saviynt EIC

Dans Saviynt on peut traiter plusieurs types de flux de travails de différents niveaux d'approbations

- Le workflow suivant met en oeuvre le contrôle AC-3(2) qui met en place une double couche d'autorisation

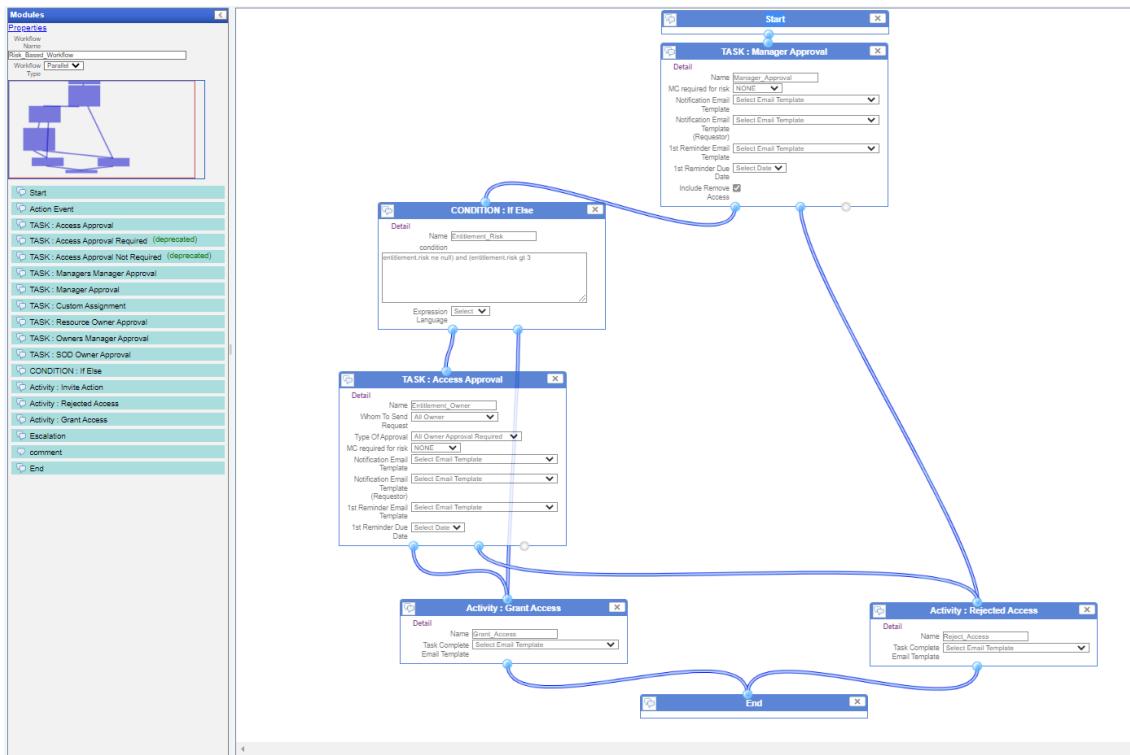


FIGURE 4.32 – Flux de travail d'une double approbation

4.5.2 Sailpoint IdentityIQ

Le flux de travail de SailPoint est conçu et mis en œuvre selon une logique et des principes sous-jacents similaires à ceux utilisés dans Saviynt. Le workflow donc met en oeuvre le contrôle AC-3(2).

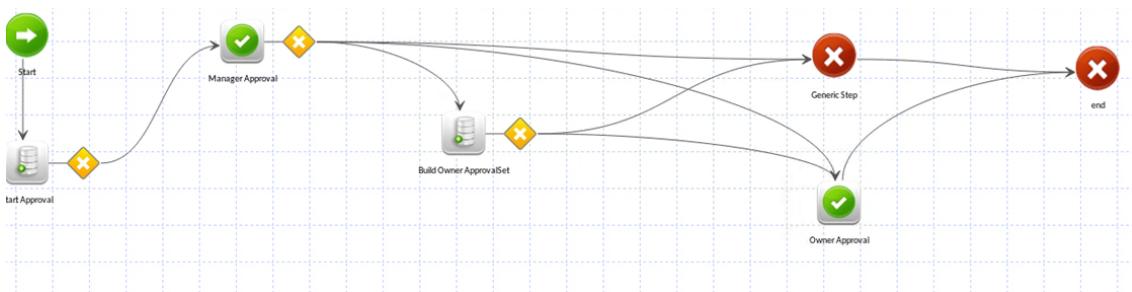


FIGURE 4.33 – Flux de travail d'une double approbation

Dans les flux de travail précédents, le processus d'attribution de l'accès suit un chemin spécifique basé sur différentes conditions. Voici une explication du flux :

- Demande d'accès : Un utilisateur soumet une demande d'accès à une ressource particulière.

- Approbation du manager : La demande est d'abord examinée par le manager de l'utilisateur. Si le manager approuve la demande, le processus se poursuit.
- Évaluation du risque : Le système vérifie la valeur du risque de l'accès demandé si c'est supérieur à 3, une approbation supplémentaire est requise.
- Approbation du titulaire du droit : Dans ce cas, le titulaire du droit, qui est responsable de la gestion de la ressource ou de l'accès spécifique, est notifié. Il examine la demande et l'approuve ou la refuse.
- Mise à disposition de l'accès : Si le titulaire du droit approuve la demande, l'accès à la ressource demandée est fourni à l'utilisateur. Si le titulaire du droit refuse la demande, l'accès n'est pas accordé.
- Refus du manager : Si le manager a initialement refusé d'approuver la demande, l'accès n'est pas accordé.

Conclusion

On va maintenant évaluer et comparer les performances de Saviynt et SailPoint IIQ selon des critères clés :

- Facilité de mise en œuvre : Le degré de simplicité et d'efficacité du déploiement et de la mise en place de la solution.
- Sécurité et conformité : Les mesures et les capacités de la solution à assurer la protection contre les accès non autorisés, les violations de données et le respect des exigences réglementaires.
- Capacités d'intégration : La capacité de la solution à se connecter et à interagir de manière transparente avec d'autres systèmes et applications.
- Performance et Scalabilité : La capacité de la solution à fournir des performances efficaces et fiables, ainsi que sa capacité à gérer des charges de travail accrues et à s'adapter à l'augmentation du nombre d'utilisateurs ou à l'expansion des besoins de l'organisation.
- Configurabilité : Le degré de flexibilité et les options de personnalisation offertes par la solution, permettant l'adaptation aux exigences et aux flux de travail spécifiques de l'organisation.

L'analyse comprend un diagramme en radar et prend en compte le pourcentage de contrôles mis en œuvre à partir des normes NIST et ISO afin d'évaluer l'adhésion aux meilleures pratiques de l'industrie.

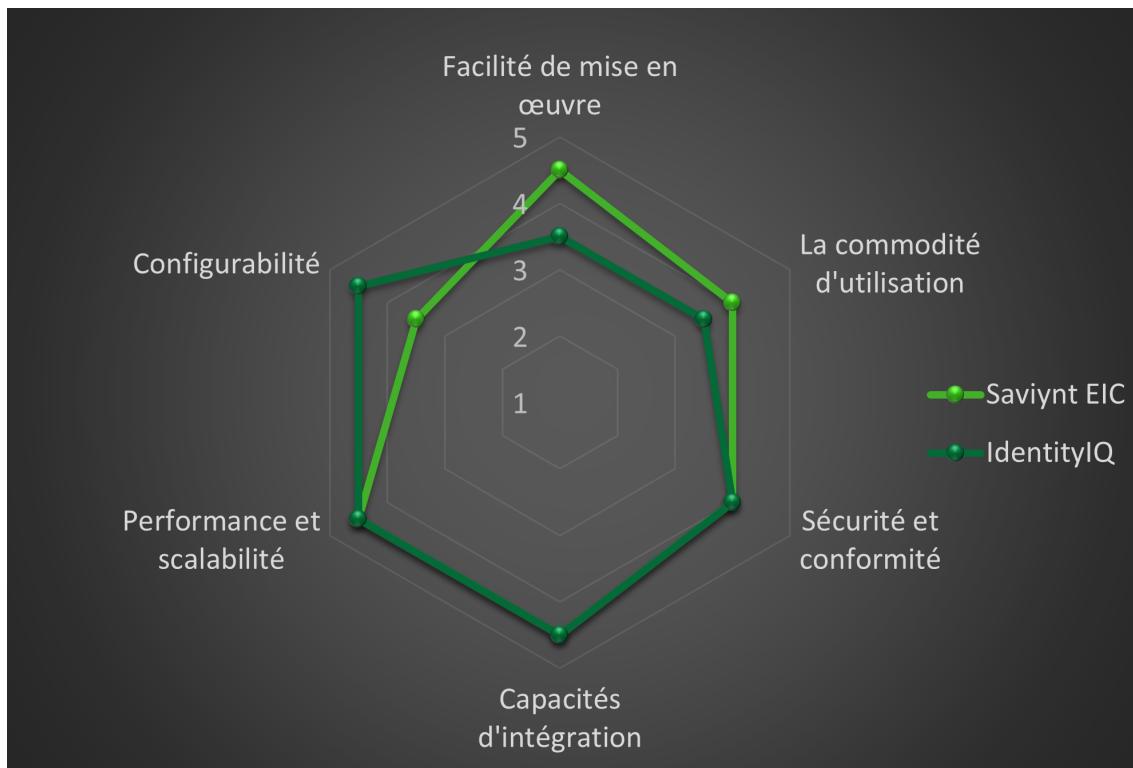


FIGURE 4.34 – Radar d'évaluation de Saviynt et Sailpoint IIQ



FIGURE 4.35 – Pourcentage des contrôles utilisés des familles choisies

Conclusion générale

Ce mémoire s'inscrit dans le cadre de la formation d'ingénieur en Sécurité Informatique et Cybersécurité de l'ENSAO (Ecole Nationale des Sciences Appliquées d'Oujda). Ce Projet de Fin d'Etudes a été réalisé au siège de Deloitte Morocco Cyber Center, localisé à Casablanca au sein du pilier de l'Identity and Access Management (IAM).

Dans ce Projet de Fin d'Etudes, nous avons réussi à répondre à la problématique posée à savoir la compréhension du cadre normatif lié à la gestion de l'identité, identifier les meilleures solutions IGA conformément à ces normes et assurant la protection contre les risques d'attaques basées sur l'identité. Cette réponse a été formulée par le biais des solutions IGA Saviynt et SailPoint, assurant la centralisation et l'automatisation de la gestion des identités. Ainsi, en s'appuyant sur le résultat de notre recherche, analyse et implémentation des contrôles au niveau des deux solutions, on a pu faciliter le processus de sélection de Deloitte et de ses clients sur leurs stratégies de cyber sécurité. Nous avons aussi procédé l'explication des notions fondamentales de l'IGA puis faire une étude normative sur la norme ISO 27001 et du NIST CSF pour en extraire les contrôles liés à la gestion d'identité, comptant respectivement 13 et 15 contrôles et sous contrôles, puis nous avons procédé à l'implémentation de ces contrôles moyennant les outils IGA, à savoir SailPoint IdentityIQ et Saviynt EIC comme des solutions de base que nous avons personnalisées et configurées.

Grâce aux acquis d'une méthodologie de travail forte que Deloitte nous a transmise, combinée à la formation que qu'on a reçu, on a pu contribuer à un sujet très important qui traite à la fois l'aspect technique et l'aspect managérial de la sécurité de l'information. Cette problématique est de plus en plus en vogue et est devenue une tendance majeure dans le domaine de la sécurité de l'information, les entreprises numériques sécurisées veillent à construire des modèles et des architectures de solutions qui exploitent et mettent en oeuvre les contrôles requis par les normes et les lois liées à la gestion des identités. En termes de perspectives, on peut approfondir la recherche sur d'autres normes et cadres normatifs pertinents dans le domaine de la gestion des identités selon le besoin du client, tels que le RGPD (Règlement général sur la protection des données) et d'autres réglementations sectorielles spécifiques, on peut également élargir la portée de l'analyse et de l'implémentation des contrôles de gestion des identités pour inclure d'autres solutions IGA et évaluer leur efficacité et leur adaptation aux besoins spécifiques des organisations.

Bibliographie

- [1] Deloitte. <https://www2.deloitte.com/fr/fr/pages/home.html>.
- [2] Forrester. <https://reprints2.forrester.com/#/assets/2/214/RES176519/report>.
- [3] IBM. <https://www.ibm.com/products/verify-governance>.
- [4] One Identity. <https://www.oneidentity.com/products/identity-manager/>.
- [5] SailPoint IdentityIQ. IdentityIQ Administrators and Implementers, Version 8.2, 2023.
- [6] NIST. <https://www.nist.gov/cyberframework/online-learning/cybersecurity-framework-components#:~:text=The%20Tiers%20range%20from%20Partial,cybersecurity%20info%20from%20external%20parties>.
- [7] Okta. <https://www.okta.com/products/lifecycle-management/>.
- [8] Oracle. <https://www.oracle.com/fr/security/identity-management/governance/>.
- [9] SailPoint. <https://university.sailpoint.com>.
- [10] Saviynt. Saviynt, IGA Level 100 lecture manual, 2023.
- [11] RSA Security. <https://community.rsa.com/t5/securid-governance-lifecycle/tkb-p/identity-g-and-l-product-documentation>.