Voici une liste exhaustive des critères pour le choix d'une solution IAM :

1. Objectifs et besoins de l'entreprise
2. Portée du projet en termes de périmètre, de calendrier et de budget
3. Fonctionnalités et capacités de la solution IAM
4. Intégrations avec d'autres systèmes et applications
5. Sécurité et protection des données
6. Administration et gestion de la solution IAM
7. Support et maintenance de la solution IAM
8. Options de formation et de documentation de la solution IAM
9. Évolutivité et flexibilité de la solution IAM
10. Coût total de possession (TCO) de la solution IAM
11. Expérience utilisateur de la solution IAM
12. Fiabilité et disponibilité de la solution IAM
13. Conformité réglementaire de la solution IAM
14. Interopérabilité de la solution IAM avec d'autres solutions IAM
15. Capacités d'analyse et de reporting de la solution IAM
16. Évaluation et certification de la solution IAM par des tiers indépendants
17. Plan de déploiement et de migration de la solution IAM
18. Gestion de projet et services professionnels proposés par le fournisseur de la solution IAM
19. Réputation et historique du fournisseur de la solution IAM
20. Avis et retours d'expérience d'autres entreprises utilisant la solution IAM.

Voici un exemple de cahier des charges pour une solution IAM :

1. Introduction

- Objectif : Ce cahier des charges a pour objectif de définir les besoins et les attentes de l'entreprise en matière de solution IAM, ainsi que les critères de sélection pour choisir la meilleure solution.
- Contexte : L'entreprise souhaite mettre en place une solution IAM pour gérer les identités et les accès de ses utilisateurs de manière sécurisée et efficace.

2. Description de l'entreprise

- Nom de l'entreprise : XYZ Inc.
- Secteur d'activité : Services financiers
- Nombre d'utilisateurs : 3 500 employés et 5 000 clients
- Pays d'implantation : France
- Environnement informatique actuel : Windows Server 2019, Active Directory, SAP, Salesforce, Office 365, Oracle Database 12c

3. Objectifs de la solution IAM

- Sécuriser les identités et les accès des utilisateurs, en particulier pour les applications sensibles telles que les systèmes de paiement et les données clientèles
- Réduire les risques de sécurité liés à la gestion des identités et des accès
- Faciliter la gestion des identités et des accès, en réduisant le temps nécessaire pour créer et gérer des comptes utilisateur
- Assurer la conformité réglementaire en matière de protection des données personnelles
- Permettre une gestion centralisée des identités et des accès
- Faciliter l'intégration avec les systèmes existants

4. Fonctionnalités attendues de la solution IAM

- Authentification multi-facteurs : La solution IAM doit offrir une authentification forte pour garantir l'identité de l'utilisateur. Cela peut inclure l'utilisation de la biométrie (par exemple, empreintes digitales, reconnaissance faciale), de jetons de sécurité (par exemple, cartes à puce, jetons de sécurité USB), ou d'autres mécanismes d'authentification tels que l'envoi de codes de vérification par SMS ou par e-mail.
- Gestion des identités et des accès : La solution IAM doit permettre la création, la modification et la suppression des comptes utilisateur de manière centralisée et sécurisée. Les administrateurs doivent pouvoir gérer les identités et les accès des utilisateurs de manière efficace, en fonction de leurs rôles et de leurs responsabilités. Les utilisateurs doivent également pouvoir accéder facilement à leurs comptes, avec des mécanismes de réinitialisation de mot de passe sécurisés en cas d'oubli.
- Gestion des privilèges : La solution IAM doit permettre l'attribution de privilèges en fonction des rôles de l'utilisateur, pour limiter l'accès aux données et aux ressources de l'entreprise. Les privilèges doivent être accordé de manière granulaire et en fonction des besoins de l'utilisateur, en évitant l'attribution de privilèges excessifs qui pourraient compromettre la sécurité de l'entreprise.
- Gestion des autorisations : La solution IAM doit permettre l'attribution de droits d'accès à des ressources spécifiques, telles que des applications, des dossiers partagés ou des bases de données. Les autorisations doivent être attribuées en fonction des rôles de l'utilisateur et de ses besoins spécifiques. Les administrateurs doivent pouvoir gérer les autorisations de manière centralisée et les modifier facilement en cas de besoin.
- Gestion des rôles : La solution IAM doit permettre la définition de rôles pour les différents types d'utilisateurs de l'entreprise, en fonction de leurs fonctions et de leurs responsabilités. Les rôles doivent être associés à des ensembles de privilèges et d'autorisations, afin de faciliter la gestion des identités et des accès. Les administrateurs doivent pouvoir définir de nouveaux rôles et les associer à des utilisateurs ou à des groupes d'utilisateurs.

- Audit et rapports de conformité : La solution IAM doit permettre de suivre l'utilisation des ressources et de générer des rapports de conformité pour s'assurer que les politiques de sécurité et de conformité de l'entreprise sont respectées. Les rapports doivent être personnalisables et faciles à comprendre, afin de permettre aux administrateurs de détecter rapidement les problèmes de sécurité ou de conformité.
- Intégration avec les systèmes existants : La solution IAM doit être capable de s'intégrer avec les systèmes existants de l'entreprise, tels que Windows Server, Active Directory, SAP, Salesforce, Office 365 et Oracle Database. Les intégrations doivent être faciles à mettre en place et à gérer, afin de permettre une utilisation optimale des fonctionnalités des différents systèmes.
- Support multilingue : La solution IAM doit prendre en charge plusieurs langues pour permettre aux utilisateurs internationaux de l'entreprise de travailler facilement avec la solution. Les interfaces utilisateur, les messages d'erreur et les guides d'utilisation doivent être disponibles dans les langues appropriées.
- Facilité d'utilisation : La solution IAM doit être facile à utiliser pour les administrateurs et les utilisateurs, avec une interface utilisateur intuitive et des fonctionnalités clairement identifiées. La solution doit offrir des fonctionnalités de recherche et de filtrage pour faciliter la recherche d'utilisateurs et de groupes d'utilisateurs, et les administrateurs doivent pouvoir gérer les identités et les accès de manière efficace en quelques clics.
- Documentation complète : La solution IAM doit être accompagnée d'une documentation complète, qui explique toutes les fonctionnalités de la solution et les meilleures pratiques pour les utiliser efficacement. La documentation doit être disponible en ligne et en version imprimée, afin de permettre aux utilisateurs de l'entreprise de la consulter facilement.

5. Critères de sélection de la solution IAM
- Sécurité : niveau de sécurité de la solution, conformité aux normes de sécurité (par exemple, ISO 27001), intégration avec des solutions de sécurité tierces
- Fonctionnalités : correspondance des fonctionnalités aux besoins de l'entreprise, facilité d'utilisation, support multilingue
- Intégration : capacité de la solution à s'intégrer avec les systèmes existants, facilité d'intégration, support technique de l'éditeur
- Support et maintenance : qualité du support, facilité de maintenance, coût de la maintenance
- Coûts : coûts d'acquisition, coûts de maintenance et de mise à nivau

6. Échéancier
- Date limite de réception des offres
- Date limite de sélection de la solution
- Date prévue de mise en place de la solution IAM

7. Modalités de réponse
- Format de réponse attendu
- Informations à fournir
- Coordonnées pour les questions et demandes de clarification

Quelques éléments complémentaires peuvent être ajouté, notamment :

1. Sécurité : offrir des mécanismes de sécurité robustes pour protéger les identités et les données sensibles de l'entreprise. Cela peut inclure l'utilisation de protocoles de chiffrement de bout en bout, la prise en charge de la gestion des clés de chiffrement, l'authentification multi-facteurs, la détection et la réponse aux incidents de sécurité, et la gestion des certificats.

2. Évolutivité : La solution IAM doit être capable de s'adapter à l'évolution des besoins de l'entreprise en matière d'identité et d'accès. La solution doit pouvoir gérer un grand nombre d'utilisateurs et de ressources, et être capable de s'intégrer avec d'autres systèmes de l'entreprise. La solution doit également offrir des mécanismes d'extensibilité pour permettre l'ajout de nouveaux modules fonctionnels en cas de besoin.

3. Performance : La solution IAM doit offrir des temps de réponse rapides et une disponibilité élevée pour garantir une expérience utilisateur fluide et ininterrompue. La solution doit être capable de gérer des demandes d'authentification et d'autorisation en temps réel, et de gérer des volumes importants de données de manière efficace.

4. Interopérabilité : La solution IAM doit être compatible avec les standards et les normes de l'industrie, afin de garantir une intégration facile avec les autres systèmes de l'entreprise. La solution doit être conforme aux normes telles que LDAP, SAML, OAuth, OpenID Connect et SCIM.

5. Personnalisation : La solution IAM doit offrir des fonctionnalités de personnalisation pour permettre aux administrateurs de personnaliser l'interface utilisateur, les flux de travail et les règles d'attribution de privilèges et d'autorisations. La solution doit permettre aux administrateurs de créer des workflows personnalisés pour répondre aux besoins spécifiques de l'entreprise.