



 IDENTITY DAYS

L'avenir de la conformité

Rob Byrne

One Identity, Field Strategy

#IdentityDays





Conformité : le règlement des comptes

Eh... sommes-nous en quelque sorte conformes ?



Conformité en matière de cybersécurité



ISO
27001



SOX



PCI-DSS



HIPPA



ISA/IEC
62443



TSA



CRA



NIS 2



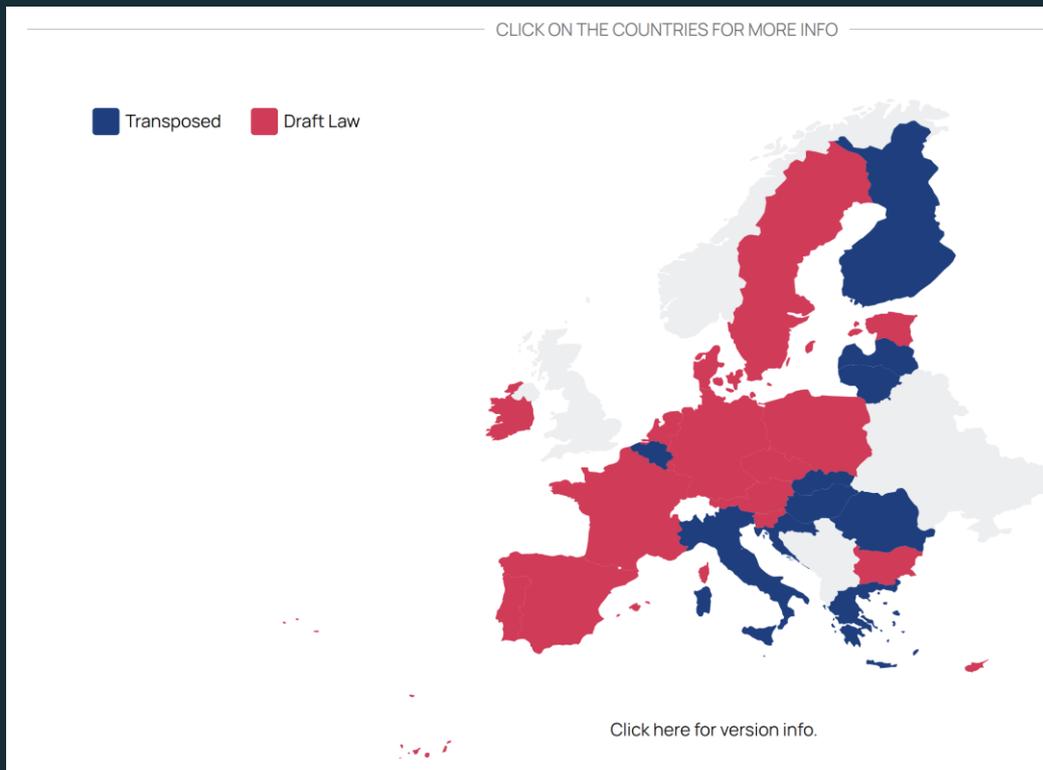
NIS2 et DORA



CDR = Commission Delegated Regulation

RTS = Regulatory Technical Standards

Pas si abstrait que ça



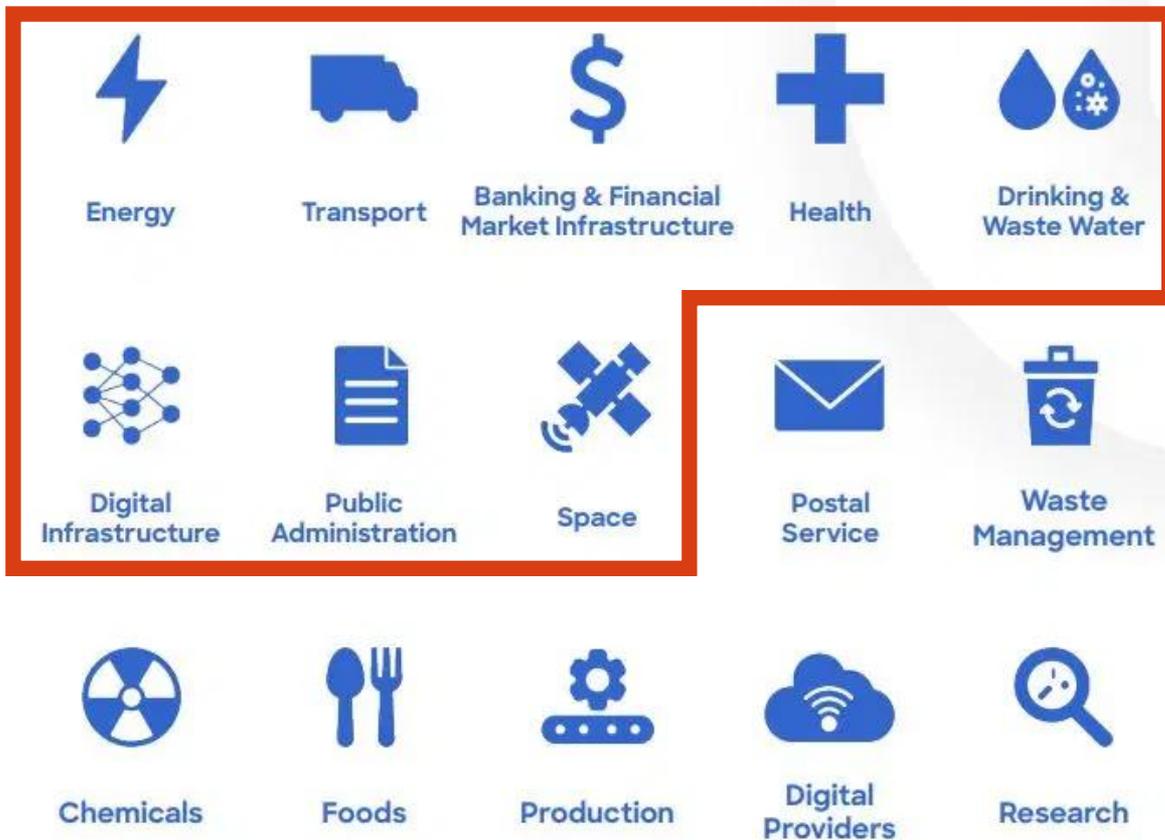
<https://ecs-org.eu/activities/nis2-directive-transposition-tracker/>

NIS2

NIS2 concerne toutes les entités qui fournissent des services **essentiels** ou **importants** à l'économie et à la société européenne, y compris les entreprises et les fournisseurs.

Essential Entities Important Entities

Mesures de gestion des risques de cybersécurité et obligations de déclaration :
20 - 25



<https://nis2directive.eu/who-are-affected-by-nis2/>

#IdentityDays

 IDENTITY DAYS

Highlights: 2024/1774 **Articles 20 & 21**

Access Management

- L'authentification forte
 - Accès à distance
 - Accès privilégié
 - Ressources critiques ou accessibles au public
- Physical Access Controls

PAM

- Accès privilégié
- Surveillance et Recertification
- L'authentification pour Utilisateurs à Privilèges
- Responsabilité de l'utilisateur

IGA

- Affectation des droits d'accès
- SOD
- Recertification régulière de l'accès
- Politique d'accès
- Processus JML

Se souvenir...



- **DORA** est une réglementation

Un règlement est une législation de l'UE qui est directement applicable aux États membres.



- **NIS 2** est une Directive

Une directive est une exigence de l'UE pour que les États membres mettent en œuvre des lois locales qui correspondent aux exigences de la directive.

Les règlements sont directement contraignants ; les directives sont indirectement contraignantes.

- Ni l'un ni l'autre n'est possible sans la collaboration de **PAM, IGA et Access Management**

Thèmes récurrents dans la législation récente de l'UE

- Harmonisation des exigences et des processus de l'UE
- Surveillance exigée par les autorités autorisées et compétentes
- Notification de l'incident et menaces aux autorités
- Responsabilité de la direction
- Le risque est défini par les risques numériques ET physiques (Tous Risques, NIS2 et DORA)
- La sécurité de la chaîne d'approvisionnement incluse dans les obligations
- Ça mord ! Amendes et sanctions



Conformité vs Sécurité

Eh... sommes-nous en sécurité ?





Cybersécurité... « nous pourrions faire beaucoup mieux »



MONEYWATCH

UnitedHealth says Change Healthcare cyberattack cost it \$872 million

MONEY
WATCH

By Khristopher J. Brooks
Edited By Anne Marie Lee
Updated on: April 18, 2024 / 10:30 AM EDT / CBS News

Le coût pourrait doubler pour atteindre 1,6 milliard de dollars

« Des patients meurent à cause de cela »

Augmentation de plus de 20 % de la mortalité des patients dans un hôpital touché par les ransomwares

 IDENTITY DAYS

Wirecard founder Braun arrested on suspicion of false accounting

Ex-chief released on €5m bail • Suspected of inflating balance sheet • Share sale details emerge



Oh, also, **Juniper Networks** recently paid \$23M to settle bribery charges. **Barclays** and **Deutsche Bank** each settled cases recently as well.

RISK & COMPLIANCE JOURNAL

Microsoft to Pay \$25 Million to Settle Foreign Bribery Probe

Software company reaches joint settlements with the Justice Department and the Securities and Exchange Commission

By Dylan Tokar and Drew Hinshaw
Updated July 22, 2019 5:46 pm ET

Share

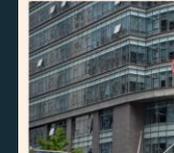
AA Resize



Microsoft agreed to pay \$25 million to settle an investigation into potentially prohibiting the bribery of foreign government officials. PHOTO: PETER SI

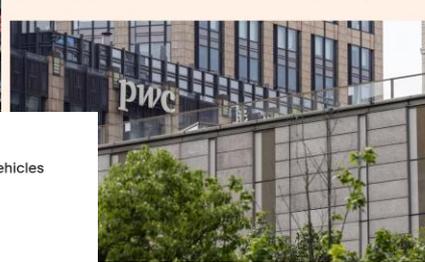
China suspends Deloitte's Beijing office over Huarong audit 'deficiencies'

Finance ministry says accounti



PwC banned for 6 months in China for 'concealing fraud' at Evergrande

Big Four firm pays \$62mn fine and fires 11 staff over audit of collapsed developer



China had approved Evergrande's accounts even though the developer had inflated its revenues

Home > News > News > 2021 News >
Volvo faces legal claim over toxic emissions from diesel vehicles

Volvo faces legal claim over toxic emissions from diesel vehicles

Volvo is facing a legal claim over its record on toxic emissions despite its pledge to build greener cars in future

The Volkswagen emissions scandal explained

The chief executive has quit after the firm admitted diesel cars

What Really Brought Down the Boeing 737 Max?

Malfunctions caused two deadly crashes. But an issue that puts unprepared pilots in the cockpit is just as

Grenfell Tower fire: Final report delivers damning verdict

Due to a dizzying series of errors and negligence, 72 people lost their lives when a social housing building in North Kensington, London, burst into flames on June 14, 2017.

By Cécile Ducourtieux (London, correspondent)
Published on September 4, 2024, at 4:09 pm (Paris) · 4 min read · Lire en français



Causes - I

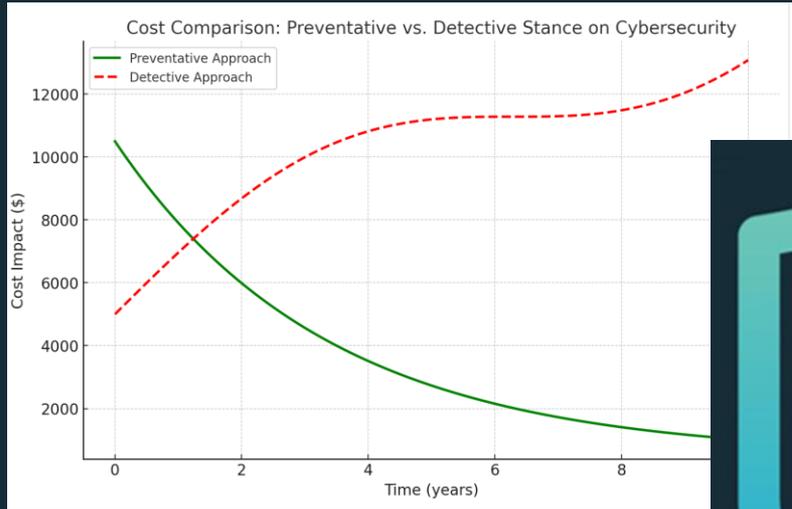
- Les dirigeants et les conseils d'administration ne sont pas tenus responsables des défaillances en matière de cybersécurité
- Sous-évaluation et sous-financement de la sécurité et de la cybersécurité

“Les incitations privées à faire face aux cyber-risques peuvent différer du niveau socialement optimal de cybersécurité, ce qui rend nécessaire une intervention publique.”

- FMI Global Stability Report, 2024



Causes- II



ii IDENTITY DA



Conformité assistée par l'IA ?

ChatGPT ▾

Tell me up to 10 types of report that an Identity Governance and Administration system can generate relevant to proving compliance for the Cybersecurity Maturity Model Certification

An Identity Governance and Administration (IGA) system can generate several types of reports that are relevant for demonstrating compliance with the Cybersecurity Maturity Model Certification (CMMC). Here are ten key types of reports that can help meet various CMMC requirements:

1. **Access Control Report:** Lists all users, roles, and their respective access levels to ensure that only authorized users have access to sensitive systems and data, addressing CMMC access control practices.
2. **Access Recertification Report:** Provides a review history of access recertification activities, showing that access rights have been periodically reviewed and validated.
3. **Privileged Account Usage Report:** Logs activities of privileged accounts, detailing who accessed what and when, to verify that privileged access is appropriately managed and used only when necessary.
4. **Separation of Duties Report:** Highlights any conflicts where users may have access to conflicting roles, supporting the segregation of duties as required by compliance frameworks.

Conformité assisté par l'IA ?



for each of these reports please identify the precise CMMC document reference

Here's a breakdown of the relevant CMMC document references for each report type, using version 2.0 of the CMMC framework. The references typically map to practices within specific CMMC domains, primarily Access Control (AC), Audit and Accountability (AU), and Incident Response (IR).

1. Access Control Report

- **CMMC Ref:** AC.L2-3.1.1, AC.L2-3.1.2, AC.L2-3.1.4, AC.L2-3.1.5
- **Description:** Ensures authorized users are identified and their access levels defined, enforcing access control policies.

2. Access Recertification Report

- **CMMC Ref:** AC.L2-3.1.5, AC.L2-3.1.6
- **Description:** Supports periodic review and validation of user access rights, confirming appropriate access levels.



3. Privileged Account Usage Report

Conformité assisté par l'IA ?

One Identity Manager Web Portal

Requests Attestation Responsibilities Data administration Statistics Setup

Welcome

Ask AI [START CONVERSATION](#)

Ask Azure OpenAI about data in Identity Manager

Password Questions
Specify your password questions to be able to unlock your user account.
[SPECIFY PASSWORD QUESTIONS](#)

Notifications
Allow this website to send you notifications.
[ALLOW NOTIFICATIONS](#)

New Request
Request products for yourself or for others.
[REQUEST PRODUCTS](#)

My Responsibilities
View and manage objects you are responsible for.
One Identity Manager application roles 1

My Direct Reports (8) [VIEW](#)
View and manage identities you are directly responsible for.
Adams, Abigail (ADAMS.ABIG)
QRUser10_Test (QRUSER10.T)
QRUser11_Test (QRUSER11.T)
QRUser12_Test (QRUSER12.T)
QRUser12Bis_Test (QRUSER12.1)

Ask Azure OpenAI about data in Identity Manager

Ask One Identity AI One Identity AI Administration

Request history

- Combine users into peer groups defined by department and title. Show entitlements in each group and how many users in the group have this entitlement.
- Include percentage of users in each group who has each entitlement
- remove percentage, add total users in peer group
- How can users with entitlements be larger than total users in groups
- Good. Now show percent of users in a group that have the entitlement

Enter request [New Conversation](#) [Follow Up Question](#)

AI Summary

Displaying users in peer groups defined by department and title, the entitlements in each group, the number of users with each entitlement, the total users in each peer group, and the percentage (rounded to two decimal places) of users in the group that have each entitlement.

AI Query

```
SELECT d.DepartmentName, p.Title, g.DisplayName AS EntitlementName, COUNT(DISTINCT ug.UID_UNSAccount) AS UsersWithEntitlement, (SELECT COUNT(1) FROM Person p2 JOIN adDepartment d2 ON p2.UID_Person = d2.UID_Person WHERE d2.DepartmentName = d.DepartmentName AND (p2.Title = p.Title OR p2.Title IS NULL)) AS TotalUsersInPeerGroup, ROUND((CAST(COUNT(DISTINCT ug.UID_UNSAccount) AS FLOAT) / (SELECT COUNT(1) FROM Person p2 JOIN adDepartment d2 ON p2.UID_Person = d2.UID_Person WHERE d2.DepartmentName = d.DepartmentName AND (p2.Title = p.Title OR p2.Title IS NULL)) * 100, 2) AS PercentageUsersWithEntitlement FROM Person p JOIN adDepartment d ON p.UID_Person = d.UID_Person JOIN UNSAccount ua ON p.UID_Person = ua.UID_Person JOIN UNSAccountGroup ug ON ua.UID_UNSAccount = ug.UID_UNSAccount JOIN UNSGroup g ON ug.UID_UNSAccount = g.UID_UNSAccount WHERE (p.Title IS NOT NULL OR p.Title IS NULL) AND (d.DepartmentName IS NOT NULL OR d.DepartmentName IS NULL) GROUP BY d.DepartmentName, p.Title, g.DisplayName HAVING COUNT(DISTINCT ug.UID_UNSAccount) <= (SELECT COUNT(1) FROM Person p2 JOIN adDepartment d2 ON p2.UID_Person = d2.UID_Person WHERE d2.DepartmentName = d.DepartmentName AND (p2.Title = p.Title OR p2.Title IS NULL)) ORDER BY d.DepartmentName, p.Title, g.DisplayName
```

DepartmentName	Title	EntitlementName	UsersWithEntitlement	TotalUsersInPeerGroup	PercentageUsersWithEntitlement
Accounting and Finance	Bookkeeper	Test Group 12	2	2	100
Compliance and Legal		ServiceNow	2	3	66.67
Compliance and Legal	Computer Technician	Bookkeeper	1	4	25
Compliance and Legal	Computer Technician	Compliance and Legal	1	4	25
Compliance and Legal	Computer Technician	Group2	1	4	25
Compliance and Legal	Computer Technician	Group4	1	4	25
Compliance and Legal	Computer Technician	Legal Analyst	1	4	25

Les Points Clés

- La conformité ne fait que devenir plus onéreuse
- Conformité \neq Sécurité
- L'identité numérique est critique pour la conformité
- L'IA devrait aider, mais les audits ont besoin d'un humain dans la boucle



Discussion