YAWIZE
Your ServiceNow Partner!

2023

Digital Operational Resilience Act

LIVRE BLANC

Sommaire

Sommaire

La véritable résilience opérationnelle digitale est un état d'esprit proactif, un engagement à anticiper les défis, à accepter le changement et à faire en sorte que votre organisation ne se contente pas de résister aux perturbations digitales, mais qu'elle en ressorte résiliente et prête à affronter la suite des événements.

I. Introduction

A. Présentation de la réglementation DORA

Le projet "Digital Operational Resilience" a été publié par la Commission Européenne à la fin du mois de septembre 2020 sous la forme d'une proposition de mesures visant à accroître la numérisation du secteur financier.

La règlementation DORA exige que les entreprises du secteur financier signalent, rapidement et de manière exhaustive, les incidents majeurs liés aux technologies de l'information et de la communication (TIC) aux autorités de surveillance et aux acteurs du marché afin que le système financier de l'Union Européenne (UE) puisse réagir rapidement et de manière appropriée aux perturbations et maintenir la résilience du système.

DORA vise à étendre et unifier les normes et exigences européennes et nationales existantes afin de créer un cadre détaillé, harmonisé et complet pour la résilience opérationnelle numérique des entités financières de l'UE.

B. L'importance croissante de la résilience opérationnelle numérique

En 2005, les accords de Bâle II (Basel Committee on Banking Supervision) introduisaient aux côtés des risques bancaires, le risque opérationnel « de pertes provenant de processus internes inadéquats ou défaillants, de personnes et systèmes ou d'évènements externes ».

Les gouvernements et les organismes de réglementation du monde entier reconnaissent de plus en plus l'importance cruciale d'assurer la résilience des systèmes et des infrastructures numériques. Voici quelques raisons pour lesquelles ces initiatives peuvent gagner en importance :

Le paysage des menaces de cybersécurité : Le paysage numérique est en constante évolution, et les cybermenaces continuent de gagner en sophistication et en fréquence. La législation et les cadres réglementaires sont essentiels pour fixer des normes et des exigences permettant d'améliorer la position des organisations en matière de cybersécurité.

Protection des infrastructures critiques : De nombreux aspects de la société moderne, notamment l'énergie, la finance, les soins de santé et les transports, dépendent fortement de l'infrastructure numérique. Garantir la résilience opérationnelle des infrastructures critiques est une priorité absolue pour les gouvernements afin d'éviter des perturbations qui pourraient avoir des conséquences considérables.

Protection des données et de la vie privée : Avec la quantité croissante de données personnelles et sensibles traitées et stockées numériquement, l'accent est mis de plus en plus sur les réglementations en matière de protection des données et de la vie privée. La législation peut porter non seulement sur la sécurité des données, mais aussi sur la résilience des systèmes qui traitent ces données.

Interconnexion mondiale : La nature interconnectée du monde numérique signifie que les perturbations ou les vulnérabilités dans une partie du globe peuvent avoir des effets d'entraînement ailleurs. La coopération internationale et les approches normalisées, facilitées par la législation, sont essentielles pour relever les défis mondiaux en matière de cybersécurité.

Réponse aux incidents et rétablissement : La législation comporte souvent des dispositions relatives à la réponse aux incidents et à la récupération. L'établissement de protocoles clairs pour la notification et la réponse aux incidents de cybersécurité aide les organisations à minimiser l'impact des violations et à se rétablir plus efficacement.

Confiance des consommateurs : Un cadre réglementaire solide contribue à renforcer la confiance des consommateurs et des entreprises. Le fait de savoir qu'il existe des normes établies en matière de résilience opérationnelle numérique peut renforcer la confiance dans les services et produits numériques.

Innovation technologique : À mesure que la technologie progresse, de nouveaux défis et de nouveaux risques apparaissent. La législation peut contribuer à garantir que l'innovation s'accompagne de garde-fous, empêchant ainsi que la résilience opérationnelle ne soit compromise dans la poursuite du progrès technologique.

Si la loi sur la résilience opérationnelle numérique est récente ou s'il y a eu des mises à jour depuis ma dernière mise à jour des connaissances en janvier 2022, je recommande de vérifier les sources les plus récentes pour obtenir les informations les plus exactes et les plus actuelles sur ses dispositions et son impact.

II. Compréhension de la Réglementation DORA

A.Explication détaillée et objectifs principaux de la réglementation

DORA répond à un contexte marqué par les crises et les incidents menaçant la continuité de l'activité économique globale. Ces évènements impactent plus spécifiquement les institutions financières, puisque ces dernières sont porteuses de la solidité des économies, et qu'elles ont donné ces dernières années une place incontournable aux outils digitaux, à la robotisation et à l'intelligence artificielle dans leurs systèmes informatiques, se rendant ainsi plus vulnérables.

Parmi les piliers de DORA, nous pouvons compter quelques-uns, qui ont ainsi pour objectif un meilleur encadrement des risques cyber et informatiques :

- Le premier pilier de DORA se focalise sur la gestion des risques liés aux Technologies de l'information et de la communication (TIC) renforçant ainsi des exigences préexistantes : mise en place d'un cadre de gestion des risques comprenant l'identification des fonctions critiques et importantes, les risques associés et une cartographie des actifs TIC.
- Le second pilier quant à lui concerne le signalement des incidents liés aux TIC et introduit pour cela une méthodologie standard de classification des incidents.
- Le troisième pilier se focalise sur l'aspect préventif, en instaurant des tests de résilience opérationnelle très poussés (TLPT). Ce pilier comporte de nombreuses nouveautés. Ainsi, les entreprises devront définir un programme de tests avancés, exécutés par des parties indépendantes et comprenant une série d'évaluations, de tests et de méthodologies précises.
- Enfin, le quatrième pilier de la réglementation DORA établit une classification des tiers fournisseurs critiques. Un contrôle de ces tiers sera effectué par l'ACPR qui pourra réaliser des audits sur site, émettre des recommandations et imposer des sanctions pécuniaires en cas de non-conformité.

Pour les assureurs, de nombreux défis sont à relever, puisque divers dispositifs devront être mis en place ou renforcés afin de se conformer à ces nouvelles exigences. Désormais, les incidents classés comme majeurs devront être signalés à l'autorité de régulation compétente et un rapport de suivi devra être réalisé à destination des acteurs de la place. Il sera également exigé un réexamen de la politique de sécurité sur base annuelle, ainsi qu'en cas de survenance d'incidents majeurs, conformément aux instructions des autorités de surveillance ou aux conclusions des tests de résilience ou des processus d'audit pertinents.

Par ailleurs, les conditions contractuelles avec les prestataires TIC devront être revues, notamment en ce qui concerne les phases de résiliation et post-contractuelle. Plusieurs grands groupes ont déjà décidé de mettre en place des réflexions complémentaires autour de la gestion des risques informatiques, afin de mieux appréhender les relations avec les fournisseurs TIC dits critiques et les tests de résilience avancés à définir. Pour autant, DORA représente également une source d'opportunités indéniable en permettant de mettre en cohérence les directives existantes et en s'érigeant en réglementation chapeau, par exemple concernant le reporting des incidents de sécurité.

En effet, cette nouvelle réglementation a pour ambition de capitaliser sur les règles en vigueur pour asseoir un cadre européen homogène et unique, permettant aux assureurs d'optimiser leurs processus internes. C'est par exemple le cas pour le programme de tests avancés : tous les tests de pénétration effectués en France seront valables pour les autres pays européens, ce qui permettra aux acteurs financiers de rationaliser leurs coûts de mise en conformité et ne nécessitera plus de recourir systématiquement à des accords bilatéraux pour la reconnaissance de ces tests.

DORA aspire donc à enrichir, préciser et coordonner les exigences préexistantes en y ajoutant un enjeu de gouvernance et d'implication du top management qui pouvait paraître trop faible dans les réglementations précédentes. Ces exigences permettent ainsi une gestion plus fluide et surtout plus exhaustive des risques cyber et informatiques, nécessaire aux assureurs pour une parfaite maîtrise de leur activité.

Cette réglementation répond ainsi aux préoccupations actuelles des assureurs puisque les menaces sont bien réelles, comme le démontrent les multiples attaques cyber dont ont été victimes plusieurs assureurs français ces dernières années. Une compréhension rapide de cette réglementation et de ses impacts opérationnels, stratégiques et organisationnels, ainsi qu'un encadrement adapté dans ces actions permettra aux assureurs d'aborder sereinement cette mise en conformité.

B. Secteurs concernés par la réglementation DORA

La Commission Européenne a souhaité viser très largement les professionnels du secteur financier, en commençant par les acteurs traditionnels (établissements de crédit, entreprises d'investissement, assureurs, réassureurs et leurs intermédiaires). Tout en incluant des acteurs plus récents (établissements de paiement, de monnaie électronique, prestataires de services d'information sur les comptes) ou dont la régulation est en train de se consolider (prestataires de services sur cryptoactifs).

Le règlement vise également les établissements qui bénéficient d'exemptions en vertu de la directive monnaie électronique. A l'inverse les organisations exclues du champ d'application des directives CRD IV, AIFD, MIF2 et Solvabilité 2, bénéficient des mêmes exemptions au titre du règlement DORA.

En revanche, certains établissements, dont la taille est très réduite, bénéficient d'un aménagement significatif des règles, entrainant la création d'un régime de proportionnalité.

Une des plus grandes nouveautés apportées par DORA reste subordination des prestataires tiers dits critiques fournissant des services numériques. Ces prestataires, identifiés et désignés par les autorités de surveillance européennes, seront soumis à une supervision directe et renforcée. Cette supervision reprend globalement les exigences posées par DORA vis-à-vis des établissements, en particulier en matière de gouvernance, de gestion du risque, des mesures de sécurité et de continuité mises en place, etc.

III. DORA et ServiceNow

Cette section vise à démontrer comment ServiceNow peut devenir un allié de premier plan pour atteindre efficacement et rapidement la conformité DORA. Nous débuterons par une brève présentation de la plateforme, mettant en lumière ses fonctionnalités clés. Ensuite, nous explorerons la manière dont ServiceNow est déjà aligné avec les objectifs de la réglementation DORA, soulignant ainsi son potentiel à faciliter la conformité et à répondre aux exigences réglementaires de manière proactive.

A. ServiceNow comme plateforme de gestion de services d'entreprise

ServiceNow se distingue en tant qu'entreprise de technologie de l'information offrant une plateforme cloud de gestion des services et des processus. Cette plateforme automatise et supervise une gamme étendue de processus métier au sein des organisations, englobant la gestion des services informatiques (ITSM), la gestion des opérations informatiques (ITOM), la gestion des opérations de sécurité (Security Operations), et bien d'autres . Aussi la plateforme ServiceNow aide dans la gestion opérationnelle, grâce à des outils avancés de reporting et d'analyse. Axée sur l'automatisation et l'optimisation des flux de travail, elle vise à accroître l'efficacité opérationnelle tout en offrant une expérience utilisateur de premier ordre.

Fondée sur une architecture de données unifiée, la plateforme assure une intégration transparente des informations entre ses divers modules, favorisant ainsi la collaboration entre les équipes et augmentant la visibilité des processus organisationnels.

B. Alignement de ServiceNow avec les objectifs de la réglementation DORA

Comme énoncé plus haut, la réglementation DORA s'appuie sur les piliers suivant : la gestion des risques liées aux TIC, la gestion de la classification et du reporting des incidents TIC et cyber-menaces, les tests de résilience opérationnelle numérique, la gestion des risques liées aux prestataires de service TIC, le partage d'informations en matière de cybersécurité.

ServiceNow, avec sa large gamme d'applications, représente une solution complète pour atteindre la résilience opérationnelle et est totalement compatible avec la norme DORA. L'avantage de ServiceNow est qu'il permet de centraliser tous les processus au niveau d'une même plateforme ce qui facilite la création d'un cadre commun de gestion et de contrôle des normes et réglementations.
Le diagramme ci-après présentent les différents modules de ServiceNow qui couvrent et répondent aux cinq piliers de la norme DORA.

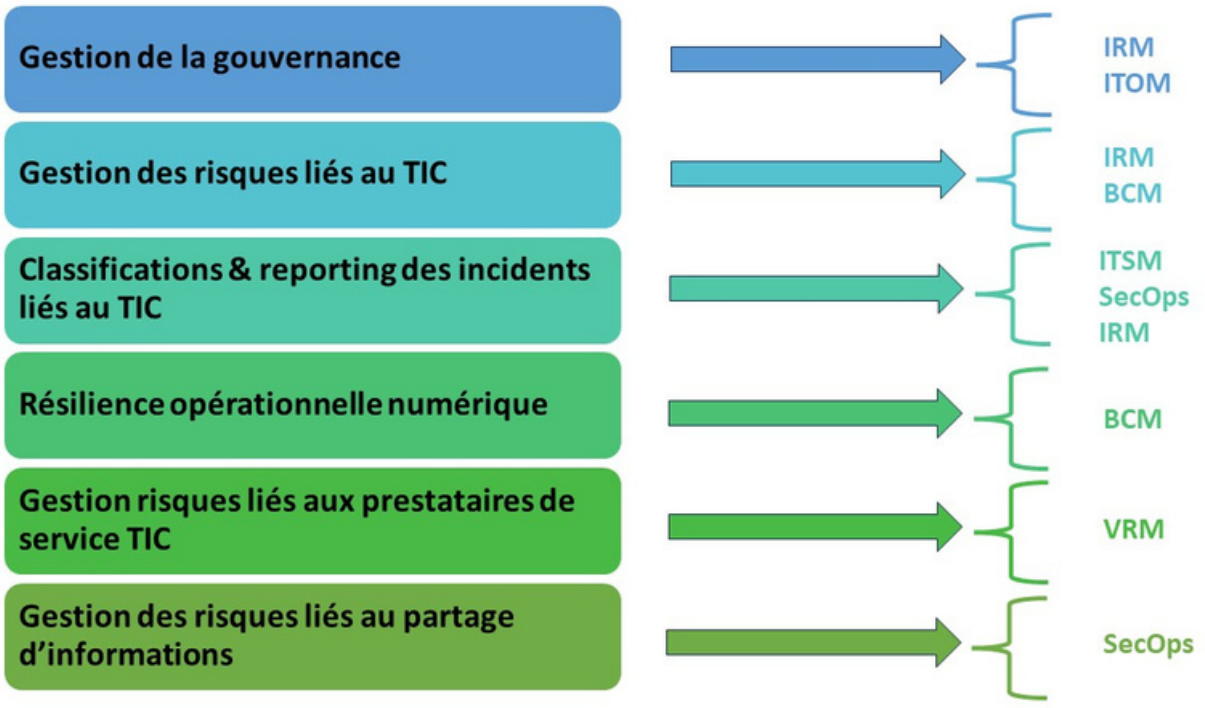

Figure 1: Mapping entre les piliers de DORA et les produits ServiceNow

C. Présentation des produits

1. *IRM (Integrated Risk Management)*

IRM est une partie de la suite Gestion des risques de ServiceNow, qui vise à aider les organisations à gérer et atténuer les risques liés à leurs opérations et à leurs processus. IRM se concentre essentiellement sur la gestion des risques liés à l'intégration de systèmes, d'applications et de services d'une entreprise.

C'est une suite d'applications permettant de documenter et démontrer de manière efficace les niveaux de risques et de conformité des entreprises. Elle transforme les processus manuels, cloisonnés et peu efficaces de gestion de risque en des processus centralisés dans une vue unifiée, intégrée et fournissant des informations temps réel des risques de l'ensemble de l'entreprise.

L'application fournit également des flux de travail structurés pour la gestion des évaluations de risques et des indicateurs de risques.

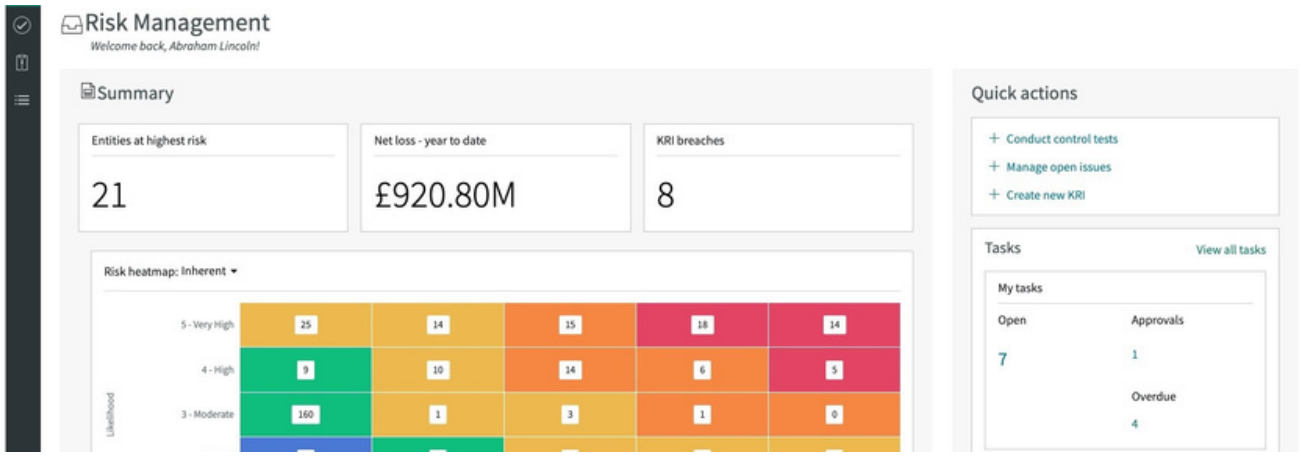

Figure 2: Espace de travail pour la gestion des risques

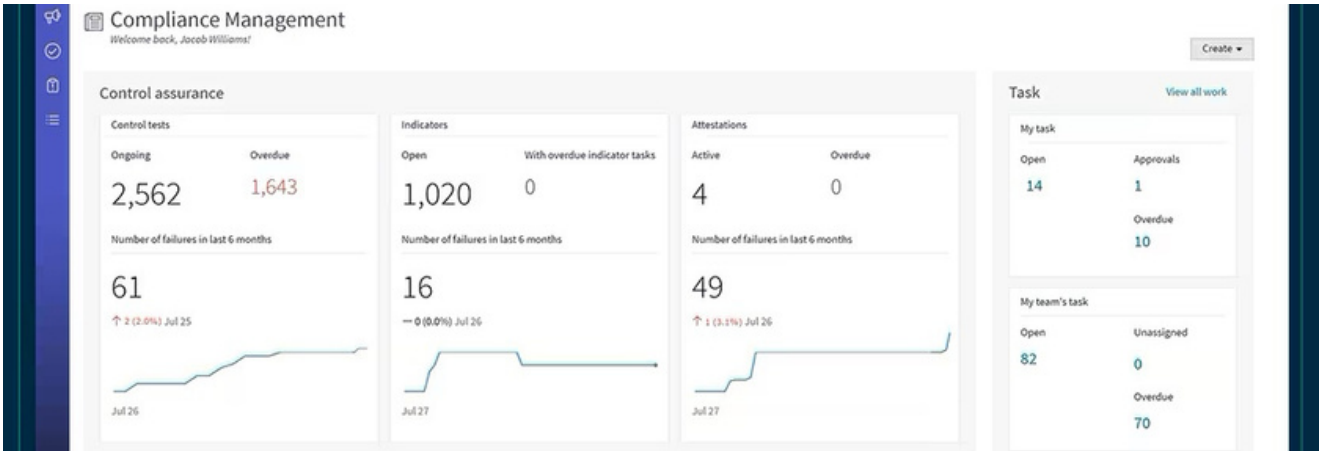

Figure 3: Espace de travail pour la gestion de la conformité

2. VRM (Vendor Risk Management) maintenant Third-Party Risk Management

L'application de gestion des risques liés aux partenaires (fournisseurs, sous-traitant, etc.) permet de s'assurer que le recours à des prestataires et fournisseurs externes ne crée pas un risque non acceptable de perturbation des activités pouvant avoir un impact négatif sur les performances de l'entreprise. Elle propose des processus centralisés et une vue unifiée pour gérer et réduire les risques des tiers.

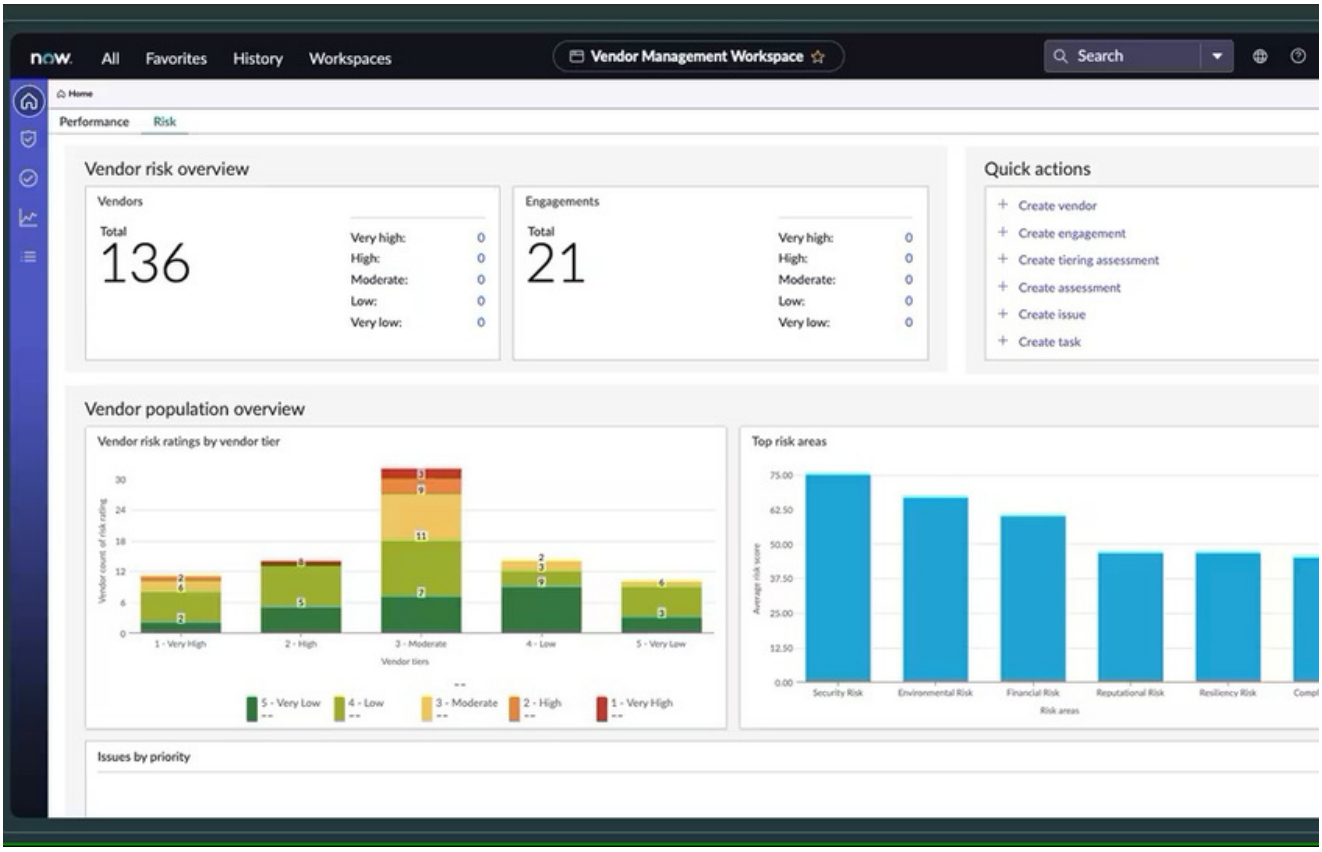

Figure 4: Espace de travail de gestion des tiers

VRM offre la possibilité d'évaluer, de manière très automatisée, les partenaires afin d'avoir une vue continue sur le risque qu'ils représentent pour l'entreprise. Le but est de maintenir une communication efficace, de suivre les performances et la conformité des partenaires afin de garantir que les intérêts de l'organisation sont préservés pendant toute la durée de la collaboration.

Les évaluations dans VRM sont des **questionnaires et/ou des demandes de documents de preuves.** Les évaluations suivent un barème de notation défini par l'entreprise ou reprenant des Framework de notations externes.

Ces évaluations sont directement disponibles sur le portail destiné aux partenaires. En fonction des réponses fournis par le prestataires, les processus définis en amont sont déclenchés.

Par exemple, supposons que l'une des question est: **'Avez-vous mis en place un plan de continuité d'activité en cas panne d'électricité ?'** . Si un tiers répond par la négative à la question ceci peut générer un problème qui l'obligera à remédier à la situation, ou cette situation peut être pris comme un risque acceptable lié au fait de faire affaire avec ce fournisseur.

3. *Business Continuity Management*

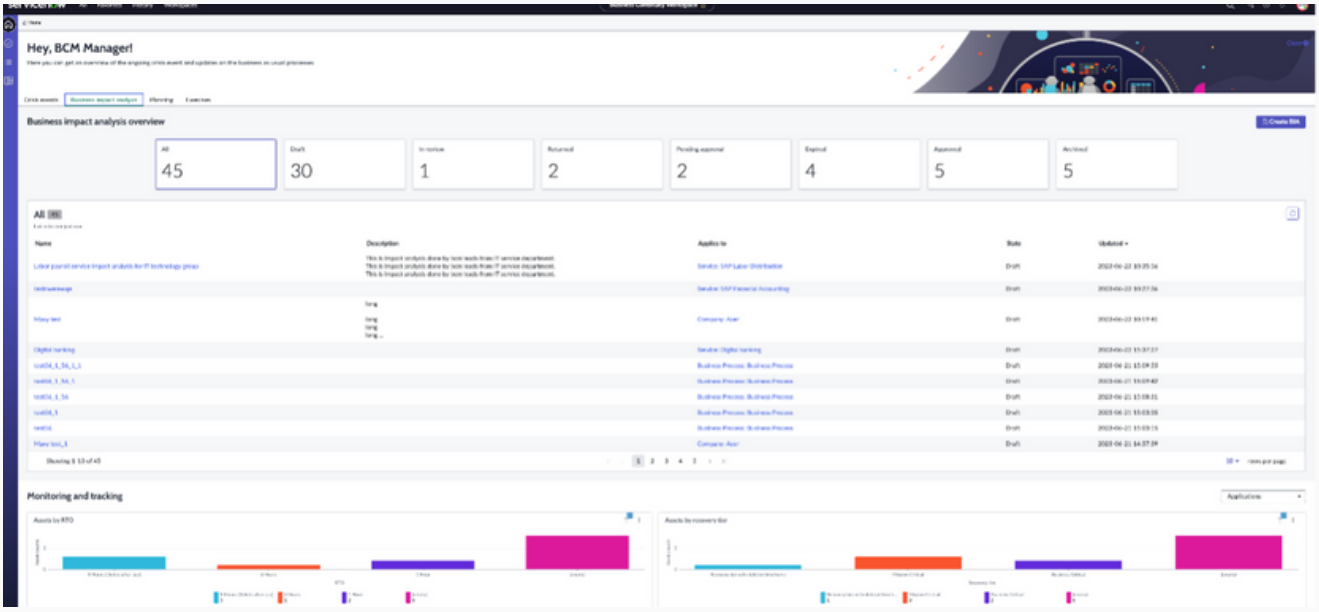

Figure 5: BCM Workspace

ServiceNow Business Continuity Management (BCM) est un produit qui a pour objectif d'aider les entreprises et organisations à planifier, gérer et maintenir leur continuité opérationnelle en cas d'incidents, de catastrophes ou de perturbations majeures.

BCM fournit un cadre permettant de créer des plans de continuité en cas de crise:

- Planification des ressources humaines;
- Analyse de l'impact sur les activités,
- Communication efficace avec les parties prenantes;
- Récupération des systèmes informatiques;
- Gestion de la formation du personnel à la conduite à tenir en cas de crise.

Les flux de travail structurés de l'application Business Continuity Management améliorent la capacité des entreprises et organisation à répondre aux problèmes et à se remettre rapidement des perturbations, crises ou catastrophes.
Comme les autres produits de ServiceNow, BCM offre une vue unifié des processus et des informations en temps réel, via un espace de travail dédié à la gestion de la continuité.

4. SecOps (Security Operations)

ServiceNow SecOps, est un module de la plateforme ServiceNow qui se concentre sur la coordination et la réponse aux incidents de sécurité. SecOps a pour objectif d'améliorer la détection, la prise en charge et la résolution des incidents liés à la sécurité via des processus et des workflow automatisés.

SecOps facilite la collaboration entre les équipes : analystes de sécurité, responsables des vulnérabilité et service informatique peuvent collaborer de manière transparente sur une plateforme unifiée. SecOps fournit, en plus des automatismes, des tableaux de bords pour suivre et analyser en temps réel les tendances, les performances et l'efficacité des opérations de sécurité.

SecOps s'intègre facilement avec des outils de sécurité tiers tels que les IDS (Intrusion Detection System), les plates-formes de gestion des informations et des événements de sécurité (SIEM) et d'autres solutions de sécurité.

IV.Exemple d'une stratégie de conformité à DORA basée sur les outils de ServiceNow

L'un des objectifs de DORA est d'harmoniser et de clarifier les processus de classifications des incidents afin d'identifier plus rapidement les incidents majeurs.

DORA définit sept (07) critères de classifications des incidents liés aux Technologies de l'information ou incidents liés aux opérations et paiements de sécurité. Ces critères sont divisés en deux groupes :

Les critères primaires :

- Nombre de clients, contreparties et transactions financières affectées;
- Implication de pertes de données ;
- Criticité des services affectés.

Les critères secondaires

- Impact sur la réputation ;
- Durée et temps d'arrêt des services impactés ;
- Impact économique ;
- Etendu géographique.

Nous avons accompagné une organisation dans sa démarche de conformité à la règlementation DORA, en se concentrant particulièrement sur la gestion de la classification des incidents majeurs.

La première étape de ce processus consistait à faire une analyse approfondie de leurs méthodes actuelles de classification et d'identification des incidents majeurs ; l'objectif visé était d'établir les écarts par rapport aux exigences stipulées par DORA.

À la suite de cette analyse, il est apparu nécessaire de :

- Définir des éléments de mesure tangibles au niveau des incidents pour chaque critère défini par DORA ;
- Automatiser le processus de détection et/ou d'escalade des incidents majeurs en établissant des règles fondées sur les critères de DORA et en mettant en place des algorithmes de prise de décision.

Les capacités offertes par le **Module de Gestion des Incidents Majeurs** (**MIM**) de la suite ITSM de ServiceNow se sont révélées être une fondation prometteuse pour répondre aux besoins de notre client.

En effet **MIM** offre une configuration simplifiée des règles et des algorithmes d'identification et de classification des incidents majeurs. Lorsqu'un incident est déclaré, les mécanismes automatiques de détection se fondent sur les critères définis pour déterminer si l'incident doit être classé en tant qu'incident majeur ou non.

En plus de cela nous avons configuré MIM et développé des workflows sur ServiceNow pour améliorer de bout en bout le processus de prise en charge des incidents majeurs ce qui a permis de :

- Faciliter la collaboration entre les équipes d'intervention ;
- Automatiser certaines tâches pour accélérer la résolution des incidents majeurs et minimiser leur impact sur les opérations.
- Rendre proactive la communication avec les parties prenantes (services et/ou clients affectés) par la diffusion d'informations en temps réel pour renforcer la transparence et la gestion des attentes ;
- Optimiser le suivi en temps réel et la génération de rapports pour évaluer les performances de la gestion des incidents majeurs et identifier des opportunités d'amélioration.

V.Avantages Supplémentaires de la Conformité à DORA

A. Amélioration de la résilience opérationnelle globale

La conformité à la réglementation DORA ne se limite pas à déployer des process pour atteindre les exigences venant avec la norme. Elle apporte des avantages significatifs, notamment l'amélioration de la résilience opérationnelle globale. En se conformant à DORA, les entreprises renforcent leur capacité à faire face aux perturbations et aux crises, ce qui est essentiel dans un monde en constante évolution.

La mise en place de processus de conformité exige une réflexion approfondie sur la gestion des risques, la continuité des activités et la reprise après incident. En fin de compte, cela se traduit par une entreprise mieux préparée à faire face aux défis inattendus.

B. Renforcement de la confiance des clients et des partenaires

La conformité à DORA va au-delà des avantages internes ; elle renforce également la confiance des clients et des partenaires. Les clients sont de plus en plus attentifs à la manière dont les entreprises gèrent leurs données et leurs opérations.

En démontrant un engagement envers la conformité, les entreprises montrent qu'elles prennent au sérieux la protection des données et la gestion des risques. Cela peut conduire à des relations commerciales plus solides et à une meilleure réputation de l'entreprise, ce qui est essentiel dans un monde axé sur la confiance.

C. Positionnement concurrentiel renforcé grâce à la conformité

La conformité à DORA peut également renforcer le positionnement concurrentiel d'une entreprise. En respectant les normes et les réglementations, une entreprise peut se démarquer de la concurrence en démontrant son engagement envers la qualité et la sécurité.

Les clients et les partenaires sont plus enclins à choisir des entreprises qui respectent des normes élevées de conformité, ce qui peut donner un avantage concurrentiel considérable.

VI. Défis et Stratégies d'Adaptation

A. Les défis potentiels de la conformité à DORA

Bien que la conformité à DORA comporte de nombreux avantages, elle n'est pas exempte de défis. Les entreprises peuvent être confrontées à un certain nombre d'investissements pour atteindre la conformité, à la complexité des réglementations et à la nécessité de former leur personnel.

De plus, les exigences de conformité évoluent constamment, ce qui nécessite une vigilance continue pour rester à jour. Les entreprises doivent également faire face aux risques potentiels en cas de non-conformité, ce qui peut avoir des conséquences juridiques et financières graves.

B. Stratégies pour surmonter ces défis en utilisant ServiceNow

ServiceNow offre des solutions puissantes pour aider les entreprises à surmonter ces défis. Grâce à des outils de gestion des opérations et de conformité, ServiceNow simplifie la mise en place de processus de conformité. Il permet également une automatisation avancée pour réduire les coûts et améliorer l'efficacité. La formation et le support de ServiceNow aident les entreprises à former leur personnel pour faire face aux nouvelles exigences de conformité.

En fin de compte, ServiceNow offre une plateforme complète pour aider les entreprises à atteindre et à maintenir la conformité à DORA de manière efficace.

C. Importance de la collaboration interne et de l'expertise externe

La conformité à DORA nécessite une collaboration interne étroite. Les équipes informatiques, juridiques, de conformité et de gestion des risques doivent travailler de concert pour mettre en œuvre des processus conformes.

De plus, il peut être bénéfique de faire appel à des experts externes en conformité et en cybersécurité pour garantir que les efforts de conformité sont complets et actualisés. ServiceNow offre des fonctionnalités de collaboration et de gestion de projet qui facilitent cette coordination interne et externe.

VII. Conclusion

- ## Récapitulation de l'impact de DORA sur ServiceNow

La réglementation DORA représente un défi et une opportunité pour les entreprises. En se conformant à DORA grâce à des solutions comme ServiceNow, les entreprises peuvent améliorer leur résilience, renforcer la confiance des clients, et renforcer leur position concurrentielle.

Cependant, elles doivent également faire face à des défis potentiels liés à la complexité et aux coûts de la conformité. ServiceNow offre des solutions pour surmonter ces défis et faciliter la conformité.

- ## Appel à l'action pour les entreprises à prendre des mesures préventives

Il est essentiel pour les entreprises de prendre des mesures préventives dès maintenant pour se conformer à DORA. Attendez-vous à ce que les réglementations en matière de protection des données et de cybersécurité continuent d'évoluer.

En utilisant des outils comme ServiceNow, les entreprises peuvent simplifier le processus de conformité et se préparer à un avenir où la protection des données et la gestion des risques sont des priorités essentielles.

- ## ServiceNow comme partenaire de choix pour atteindre la conformité à DORA

ServiceNow se positionne comme un partenaire de choix pour les entreprises cherchant à atteindre la conformité à DORA. Avec ses solutions de gestion des opérations numériques et de conformité, ServiceNow offre les outils nécessaires pour relever les défis de la conformité et tirer parti des avantages qui en découlent.

Les entreprises qui choisissent ServiceNow sont mieux préparées à l'avenir de la conformité à DORA et à la protection des données.

Ressources

1. Liens & informations utiles

- https://www.digital-operational-resilience-act.com/
- https://assets.kpmg.com/content/dam/kpmg/ie/pdf/2023/06/ie-digital-operational-resilience-2.pdf
- https://www.dora-info.eu/
- https://docs.servicenow.com/bundle/tokyo-governance-risk-compliance/page/product/grc-vendor-risk/concept/what-is-vendor-risk.html
- https://docs.servicenow.com/bundle/vancouver-governance-risk-compliance/page/product/grc-business-continuity-management/concept/exploring-bcm.html#d192575e66
- https://docs.servicenow.com/bundle/vancouver-governance-risk-compliance/page/product/grc-risk/concept/grc-risk-overview.html
- https://docs.servicenow.com/bundle/vancouver-security-management/page/product/security-operations/concept/security-operations-intro.html

Prêts...

...à vous conformer à la réglementation DORA?

Notre équipe expérimentée offre une compréhension approfondie des exigences et des meilleures pratiques.

Ensemble, renforçons la résilience opérationnelle numérique de votre entreprise.

Contactez-nous aujourd'hui pour une consultation personnalisée et assurez-vous d'être à la pointe de la conformité digitale.

Parler à un Expert!

FRANCE - 99 AV Achille Peretti 92200 Neuilly-Sur-Seine

SÉNÉGAL - Immeuble Seydi Djamil, Rue Léo Frobénius X Avenue Cheikh Anta Diop, Fann Résidence

sales@yawize.com

www.yawize.com

DORA FAQ?

Quels sont les aspects clés de la réglementation DORA (Digital Operational Resilience Act) que notre entreprise doit comprendre en profondeur ?

Mauris finibus tortor sed odio laoreet volutpat. Aenean nibh lectus, fermentum eget nisl a, laoreet mattis nulla. Maecenas volutpat vitae tortor pharetra venenatis. Suspendisse quis est a enim vehicula commodo non sed ante. Cras eleifend erat tortor.

Quels sont les principaux risques auxquels notre entreprise pourrait être exposée en termes de cybersécurité et de résilience opérationnelle ?

Mauris finibus tortor sed odio laoreet volutpat. Aenean nibh lectus, fermentum eget nisl a, laoreet mattis nulla. Maecenas volutpat vitae tortor pharetra venenatis. Suspendisse quis est a enim vehicula commodo non sed ante. Cras eleifend erat tortor.

Nos systèmes actuels sont-ils conformes aux exigences de la réglementation DORA, et quelle est la marche à suivre pour atteindre la conformité le cas échéant ?

Mauris finibus tortor sed odio laoreet volutpat. Aenean nibh lectus, fermentum eget nisl a, laoreet mattis nulla. Maecenas volutpat vitae tortor pharetra venenatis. Suspendisse quis est a enim vehicula commodo non sed ante. Cras eleifend erat tortor.

Comment évalue-t-on actuellement la résilience opérationnelle numérique de notre organisation ?

Mauris finibus tortor sed odio laoreet volutpat. Aenean nibh lectus, fermentum eget nisl a, laoreet mattis nulla. Maecenas volutpat vitae tortor pharetra venenatis. Suspendisse quis est a enim vehicula commodo non sed ante. Cras eleifend erat tortor.

Quelles sont les implications financières de la mise en œuvre des mesures nécessaires pour respecter les exigences de la DORA ?

Mauris finibus tortor sed odio laoreet volutpat. Aenean nibh lectus, fermentum eget nisl a, laoreet mattis nulla. Maecenas volutpat vitae tortor pharetra venenatis. Suspendisse quis est a enim vehicula commodo non sed ante. Cras eleifend erat tortor.

Comment notre entreprise prévoit-elle de maintenir une culture de cybersécurité et de résilience opérationnelle à long terme, alignée sur les normes de la DORA ?

Mauris finibus tortor sed odio laoreet volutpat. Aenean nibh lectus, fermentum eget nisl a, laoreet mattis nulla. Maecenas volutpat vitae tortor pharetra venenatis. Suspendisse quis est a enim vehicula commodo non sed ante. Cras eleifend erat tortor.