CLUSIF

COTER NUMERIQUE

Damien ALEXANDRE

Le Clusif est l'association de référence de la sécurité du numérique en France à travers ses conférences thématiques et les publications de ses groupes de travail.

Il réunit en parfaite équité au sein de deux collèges, offreurs et utilisateurs, tous les secteurs d'activité autour de la cybersécurité et de la confiance numérique.

Le Clusif, c'est aussi :

- Le Panorama de la cybercriminalité - #Panocrim
- L'étude Menaces informatiques et pratiques de sécurité en France - #MIPS
- L'exercice de cybercrise ECRANS

Les Clusir, liés au Clusif par une convention, ont pour vocation de rassembler les différents acteurs de la sécurité de l'information dans les territoires et à l'international.

DES GROUPES ET DES ESPACES DE TRAVAIL VARIÉS

- Espace AFNOR
- Espace CoTer
- Espace Risques et méthodes
- Espace RSSI
- Agilité et sécurité numériques
- Bug Bounty
- Cybersécurité des systèmes industriels
- Inclusion et diversité
- IOT
- Méhari
- Office 365
- Panocrim
- Shadow IT à l'ère du Cloud
- RSSI-DPO
- Sensibilisation numérique
- Zero Trust

CLUSIF

En accès libre sur notre site

DES PUBLICATIONS RECENTES

- Référentiel des logs
- Nouveau module Méhari Manager BC
- Guide cybersécurité des systèmes industriels
- Sécurité du Cloud
- Sécuriser Office 365

DES CONFERENCES A VOIR OU A REVOIR

- Office 365 et sécurité
- Quel SOC en 2020
- PANOCRIM
- MIPS

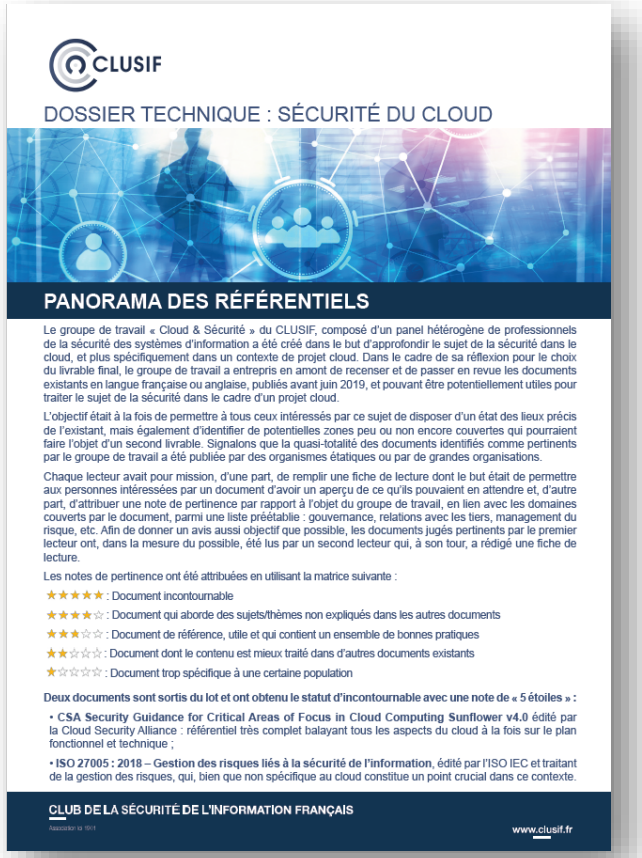
Prochain replay disponible:

La mobilité en 2021, enjeux et solutions

CLUSIF

En accès libre sur notre site

PUBLICATION SUR LA SECURITE DU CLOUD


CLUSIF

DOSSIER TECHNIQUE : SÉCURITÉ DU CLOUD

PANORAMA DES RÉFÉRENTIELS

Le groupe de travail « Cloud & Sécurité » du CLUSIF, composé d'un panel hétérogène de professionnels de la sécurité des systèmes d'information a été créé dans le but d'approfondir le sujet de la sécurité dans le cloud, et plus spécifiquement dans un contexte de projet cloud. Dans le cadre de sa réflexion pour le choix du livrable final, le groupe de travail a entrepris en amont de recenser et de passer en revue les documents existants en langue française ou anglaise, publiés avant juin 2019, et pouvant être potentiellement utiles pour traiter le sujet de la sécurité dans le cadre d'un projet cloud.

L'objectif était à la fois de permettre à tous ceux intéressés par ce sujet de disposer d'un état des lieux précis de l'existant, mais également d'identifier de potentielles zones peu ou non encore couvertes qui pourraient faire l'objet d'un second livrable. Signalons que la quasi-totalité des documents identifiés comme pertinents par le groupe de travail a été publiée par des organismes étatiques ou par de grandes organisations.

Chaque lecteur avait pour mission, d'une part, de remplir une fiche de lecture dont le but était de permettre aux personnes intéressées par un document d'avoir un aperçu de ce qu'ils pouvaient en attendre et, d'autre part, d'attribuer une note de pertinence par rapport à l'objet du groupe de travail, en lien avec les domaines couverts par le document, parmi une liste préétablie : gouvernance, relations avec les tiers, management du risque, etc. Afin de donner un avis aussi objectif que possible, les documents jugés pertinents par le premier lecteur ont, dans la mesure du possible, été lus par un second lecteur qui, à son tour, a rédigé une fiche de lecture.

Les notes de pertinence ont été attribuées en utilisant la matrice suivante :

★★★★★ : Document incontournable

★★★★☆ : Document qui aborde des sujets/thèmes non expliqués dans les autres documents

★★★☆☆ : Document de référence, utile et qui contient un ensemble de bonnes pratiques

★★☆☆☆ : Document dont le contenu est mieux traité dans d'autres documents existants

★☆☆☆☆ : Document trop spécifique à une certaine population

Deux documents sont sortis du lot et ont obtenu le statut d'incontournable avec une note de « 5 étoiles » :

- **CSA Security Guidance for Critical Areas of Focus in Cloud Computing Sunflower v4.0** édité par la Cloud Security Alliance : référentiel très complet balayant tous les aspects du cloud à la fois sur le plan fonctionnel et technique ;
- **ISO 27005 : 2018 – Gestion des risques liés à la sécurité de l'information**, édité par l'ISO IEC et traitant de la gestion des risques, qui, bien que non spécifique au cloud constitue un point crucial dans ce contexte.

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

www.clusif.fr


LES DOSSIERS TECHNIQUES

INTEGRER LA SECURITE DANS LES PROJETS CLOUD

Juin 2021

CLUSIF

PUBLICATION SUR LA SECURITE DU CLOUD


CLUSIF

DOSSIER TECHNIQUE : SÉCURITÉ DU CLOUD

PANORAMA DES RÉFÉRENTIELS

Le groupe de travail « Cloud & Sécurité » du CLUSIF, composé d'un panel hétérogène de professionnels de la sécurité des systèmes d'information a été créé dans le but d'approfondir le sujet de la sécurité dans le cloud, et plus spécifiquement dans un contexte de projet cloud. Dans le cadre de sa réflexion pour le choix du livrable final, le groupe de travail a entrepris en amont de recenser et de passer en revue les documents existants en langue française ou anglaise, publiés avant juin 2019, et pouvant être potentiellement utiles pour traiter le sujet de la sécurité dans le cadre d'un projet cloud.

L'objectif était à la fois de permettre à tous ceux intéressés par ce sujet de disposer d'un état des lieux précis de l'existant, mais également d'identifier de potentielles zones peu ou non encore couvertes qui pourraient faire l'objet d'un second livrable. Signalons que la quasi-totalité des documents identifiés comme pertinents par le groupe de travail a été publiée par des organismes étatiques ou par de grandes organisations.

Chaque lecteur avait pour mission, d'une part, de remplir une fiche de lecture dont le but était de permettre aux personnes intéressées par un document d'avoir un aperçu de ce qu'ils pouvaient en attendre et, d'autre part, d'attribuer une note de pertinence par rapport à l'objet du groupe de travail, en lien avec les domaines couverts par le document, parmi une liste préétablie : gouvernance, relations avec les tiers, management du risque, etc. Afin de donner un avis aussi objectif que possible, les documents jugés pertinents par le premier lecteur ont, dans la mesure du possible, été lus par un second lecteur qui, à son tour, a rédigé une fiche de lecture.

Les notes de pertinence ont été attribuées en utilisant la matrice suivante :

★★★★★ : Document incontournable

★★★★☆ : Document qui aborde des sujets/thèmes non expliqués dans les autres documents

★★★☆☆ : Document de référence, utile et qui contient un ensemble de bonnes pratiques

★★☆☆☆ : Document dont le contenu est mieux traité dans d'autres documents existants

★☆☆☆☆ : Document trop spécifique à une certaine population

Deux documents sont sortis du lot et ont obtenu le statut d'incontournable avec une note de « 5 étoiles » :

- **CSA Security Guidance for Critical Areas of Focus in Cloud Computing Sunflower v4.0** édité par la Cloud Security Alliance : référentiel très complet balayant tous les aspects du cloud à la fois sur le plan fonctionnel et technique ;
- **ISO 27005 : 2018 – Gestion des risques liés à la sécurité de l'information**, édité par l'ISO IEC et traitant de la gestion des risques, qui, bien que non spécifique au cloud constitue un point crucial dans ce contexte.

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

www.clusif.fr

Tableau de synthèse des documentations existantes avec identifications des domaines selon la typologie :
Gouvernance Architecture et conception

- Expertises en cybersécurité
- Modélisation et cartographie
- Intégration et déploiement
- Relation avec les tiers /
- externalisation des services
- Management du risque et classification
- Maintien en condition de cybersécurité
- Etude de cas

PUBLICATION SUR LA SECURITE DU CLOUD

CLUSIF

DOSSIER TECHNIQUE : SÉCURITÉ DU CLOUD

PANORAMA DES RÉFÉRENTIELS

Le groupe de travail « Cloud & Sécurité » du CLUSIF, composé d'un panel hétérogène de professionnels de la sécurité des systèmes d'information a été créé dans le but d'approfondir le sujet de la sécurité dans le cloud, et plus spécifiquement dans un contexte de projet cloud. Dans le cadre de sa réflexion pour le choix du livrable final, le groupe de travail a entrepris en amont de recenser et de passer en revue les documents existants en langue française ou anglaise, publiés avant juin 2019, et pouvant être potentiellement utiles pour traiter le sujet de la sécurité dans le cadre d'un projet cloud.

L'objectif était à la fois de permettre à tous ceux intéressés par ce sujet de disposer d'un état des lieux précis de l'existant, mais également d'identifier de potentielles zones peu ou non encore couvertes qui pourraient faire l'objet d'un second livrable. Signalons que la quasi-totalité des documents identifiés comme pertinents par le groupe de travail a été publiée par des organismes étatiques ou par de grandes organisations.

Chaque lecteur avait pour mission, d'une part, de remplir une fiche de lecture dont le but était de permettre aux personnes intéressées par un document d'avoir un aperçu de ce qu'ils pouvaient en attendre et, d'autre part, d'attribuer une note de pertinence par rapport à l'objet du groupe de travail, en lien avec les domaines couverts par le document, parmi une liste préétablie : gouvernance, relations avec les tiers, management du risque, etc. Afin de donner un avis aussi objectif que possible, les documents jugés pertinents par le premier lecteur ont, dans la mesure du possible, été lus par un second lecteur qui, à son tour, a rédigé une fiche de lecture.

Les notes de pertinence ont été attribuées en utilisant la matrice suivante :

★★★★★ : Document incontournable

★★★★☆ : Document qui aborde des sujets/thèmes non expliqués dans les autres documents

★★★☆☆ : Document de référence, utile et qui contient un ensemble de bonnes pratiques

★★☆☆☆ : Document dont le contenu est mieux traité dans d'autres documents existants

★☆☆☆☆ : Document trop spécifique à une certaine population

Deux documents sont sortis du lot et ont obtenu le statut d'incontournable avec une note de « 5 étoiles » :

- **CSA Security Guidance for Critical Areas of Focus in Cloud Computing Sunflower v4.0** édité par la Cloud Security Alliance : référentiel très complet balayant tous les aspects du cloud à la fois sur le plan fonctionnel et technique ;
- **ISO 27005 : 2018 – Gestion des risques liés à la sécurité de l'information**, édité par l'ISO IEC et traitant de la gestion des risques, qui, bien que non spécifique au cloud constitue un point crucial dans ce contexte.

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

www.clusif.fr

Fiche détaillée

Titre	**ISO/IEC 27005:2018 – Gestion des risques liés à la sécurité de l'information**						
Publication	07/2018	**Éditeur**	ISO/IEC	**Pages**	57	**Accès**	Payant
Typologie et usage	IaaS : X	PaaS : X		SaaS : X	Autre		
	Compta/RH	Cybersécurité : X		Marketing	Autre		
Secteur	Entreprise : X	Finance : X	Industrie : X	Santé : X	Transverse/autre : X		
Populations concernées	DSI : X	RSSI : X		Hébergeurs : X	Infogérants : X		
	Éditeurs : X	Directions générales		Métiers	Autre		
Contenu	Lignes directrices relatives à la gestion des risques en sécurité de l'information dans un organisme.						
Synthèse	La norme ISO 27005 présente une approche concrète de la gestion des risques liés à la sécurité de l'information, mais suffisamment générique pour s'adapter au contexte auquel on souhaite la mettre en application. La méthode est découpée en quatre phases principales et deux transverses. Phases principales : 1. Établissement du contexte : cette phase consiste à établir le contexte de la gestion des risques de sécurité à travers la définition des objectifs, des critères (d'évaluation, d'impact et d'acceptation), du domaine d'application, des limites et enfin de l'organisation à mettre en place ; 2. Appréciation des risques : cette étape représente le cœur de la méthode. Elle est composée de trois sous-parties : • identification des risques ou des différents éléments relatifs aux risques (actifs, menaces, mesures de sécurité existantes, vulnérabilités et conséquences) sur le périmètre convenu lors de la phase d'établissement du contexte, • analyse des risques, en utilisant la méthode choisie couplée à une formule basée sur l'appréciation des conséquences et de la vraisemblance de scénarios d'incident, afin de pouvoir estimer le niveau des risques, • évaluation des risques, consistant à confronter le niveau de risque (résultat de l'analyse précédente) avec les critères d'évaluation définis lors de l'établissement du contexte ; 3. Traitement des risques : cette phase vise à comparer un à un les risques (classés par ordre de priorité en cohérence avec les critères d'évaluation et en relation avec les scénarios d'incident) avec les critères d'acceptation définis lors de l'établissement du contexte. Chaque risque sera au choix « réduit » (par exemple à l'aide de la mise en place d'une mesure de sécurité), « maintenu » (a priori parce que son niveau est acceptable), « refusé » (cas le plus rare qui consiste à adopter une méthode draconienne telle que supprimer le processus ou l'actif exposé) ou encore « partagé » (en faisant intervenir une tierce partie, par exemple) ; 4. Acceptation des risques : plus formelle que les précédentes, cette étape nécessite la participation des décideurs et/ou des dirigeants, qui doivent approuver le plan d'acceptation des risques proposé et justifier le cas échéant les risques exclus par les critères prédéfinis. Les deux phases transverses à l'ensemble du processus sont la « Communication et concertation relatives aux risques », qui doit survenir tout au long de la démarche et la « Surveillance et réexamen des risques », qui s'inscrit dans une démarche d'amélioration continue.						

CLUSIF

En accès libre sur notre site

PUBLICATION SUR LA SECURITE DU CLOUD

Organisé autour des chapitres :

Qu’est-ce que le cloud ?

Bien gérer son projet Cloud

La sécurité dans le Cloud

Exemple d’un projet Cloud

EVALUER LA SECURITE DU CLOUD

Aux critères usuels de sensibilité des actifs

- Disponibilité
- Intégrité
- Confidentialité

Il convient d'ajouter

- Réversibilité
- Capacité à localiser les droits applicables

EVALUER LES RISQUES

- Etablir un dialogue avec la Direction Générale et un partage des responsabilités;
- Définir les mesures préventives appropriées ;
- Organiser les réactions en cas de survenance d’un incident cyber (PCA/PRA);

MAITRISER LE DEPLOIEMENT

- Maitriser le vocabulaire imposé par les fournisseurs
- Maitriser le partage des responsabilités afin de sécuriser la configuration et le paramétrage
- Maitriser la consommation du service
- Maitriser la dépendance en abordant le retour arrière dès le début du projet

GERER LA SECURITE

- Documenter les bonnes pratiques
  - Sécurisation des accès
  - Protection contre la perte de données
  - Respect des réglementations
- Sécuriser les accès
  - Gérer les permissions
  - Centraliser l'authentification
  - Authentification forte
  - Provisionnement automatisé
  - Sécuriser le réseau

CLUSIF

MERCI POUR VOTRE ÉCOUTE