Redguard

Security Survey

2023

REDGUARD
SECURING YOUR ASSETS

Avec la publication de la norme minimale pour les TIC[1] par la Confédération, la Suisse dispose depuis 2018 d'une spécification uniforme et intersectorielle en matière de protection contre les cyberrisques. Mais quel est le niveau de sécurité actuel en Suisse?

Depuis cinq ans, nous demandons aux organisations et aux entreprises suisses de s'auto-évaluer sur leur niveau de sécurité actuel. À cet effet, nous avons développé un Quick-Test de la norme minimale pour les TIC (www.ikt-redguard.ch). Vous découvrirez dans ce rapport quels résultats et tendances se sont dégagées ces dernières années.

Cinquième année consécutive d'enquêtes Redguard Security Survey

Redguard AG publie les résultats de son enquête sur la norme minimale pour les TIC pour la cinquième fois déjà: le moment est venu d'en faire une synthèse.

La bonne nouvelle d'abord: les entreprises sont aujourd'hui plus sensibilisées au thème de la cybersécurité qu'il y a quelques années. C'est ce que montrent non seulement les résultats des sondages de ces dernières années, mais aussi nos discussions quotidiennes avec notre clientèle et les entreprises qui recherchent un soutien.

La mauvaise nouvelle: cette tendance est principalement due à la hausse des signalements d'attaques au rançongiciel, phishing et autres moyens. Celles-ci se multiplient et se rapprochent, ce qui incite de nombreuses entreprises à prendre des contre-mesures.

Focus sur la surveillance continue

Sur les cinq années écoulées, il apparait que, malgré la sensibilisation à la cybersécurité et les efforts pour l'assurer, la plupart des entreprises n'atteignent pas le niveau de sécurité minimal.

De nombreux incidents de sécurité signalés à notre équipe de réponse aux incidents auraient pu être évités grâce à une surveillance systématique.

Cela nous a incités à nous doter durant une année d'un centre des opérations de sécurité moderne avec des technologies de sécurité Microsoft dans le cloud et une équipe dédiée . Après une phase d'exploitation pilote réussie, nous avons externalisé le SOC dans notre société sœur FusionOne. Le SOC as a Service permet d'assurer une détection précoce des cybermenaces et une réaction à celles-ci, même avec le budget d'une PME.

La tendance est à une surveillance plus proactive et continue. Car les agresseurs ne dorment jamais. Des tests d'intrusion (Penetration Test) réguliers révèlent où se trouvent les failles – des plus courantes à celles qui rendent spécifiquement votre entreprise vulnérable.

Un scan continu de sécurité (Continuous Security Scanning), c'est-à-dire des scans de vulnérabilité réguliers et automatisés, s'impose pour surveiller le niveau de sécurité actuel entre les tests d'intrusion. En se basant sur plus de dix ans d'expérience dans la détection des vulnérabilités, Redguard a développé une plateforme suisse à la fois intuitive et compréhensible.

Les dangers du futur

Bien que de nombreux nouveaux outils et services soient en cours de développement et d'amélioration, ils sont encore trop peu utilisés par les entreprises. De plus, les cybermenaces évoluent et se renforcent constamment.

Les nouvelles technologies telles que ChatGPT sont par exemple capables d'écrire des codes malveillants et des e-mails de phishing, ce qui peut multiplier leur quantité et perfectionner leur exécution. Équipé de ces «assistants», quiconque a un minimum d'expérience est en mesure de compenser son manque de compétences et de s'ajouter au nombre déjà élevé d'agresseurs.

[1] 1 Norme minimale pour les TIC (technologies d'information et de communication) de l'Office fédéral pour l'approvisionnement économique du pays (OFAE): https://www.bwl.admin.ch/bwl/fr/home/themen/ikt/ikt_minimalstandard.html

Regarder vers le passé permet parfois de percevoir les contours de l'avenir. Ainsi, les résultats des cinq dernières années suggèrent que les organisations (en particulier les PME) ne sont que partiellement en mesure de mettre en œuvre la norme minimale TIC de manière autonome, et qu'elles dépendent pour cela d'un soutien externe, comme par exemple de la part de Redguard.

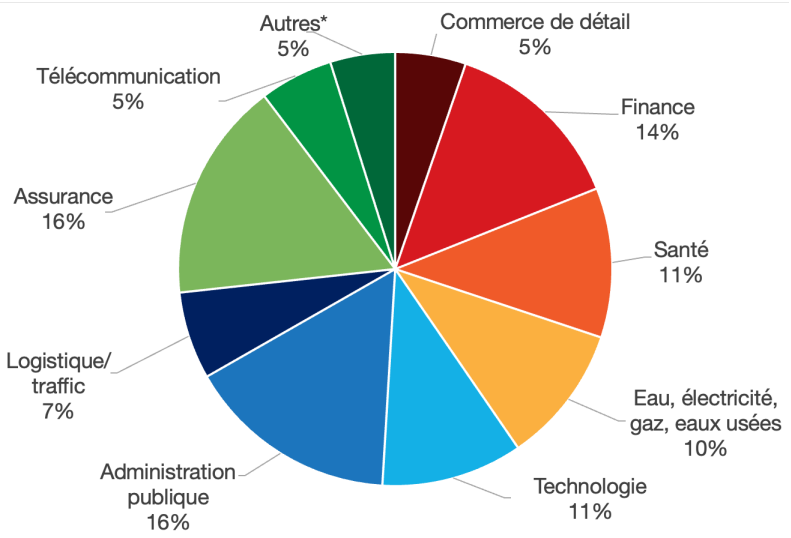
Depuis plus de dix ans, notre objectif est de veiller à votre cybersécurité et de protéger vos valeurs – aujourd'hui plutôt que demain.

Nos plus vifs remerciements pour votre coopération.
Votre équipe Redguard

Évaluation Quick-Test de Redguard

Les résultats de l'enquête Redguard Security Survey sont basés sur une auto-évaluation des entreprises et organisations. Avec ce Quick-Test, ces dernières ont l'occasion d'évaluer leur niveau de sécurité en un temps record et de prendre les mesures qui s'imposent en conséquence.

Le Quick-Test de la norme minimale pour les TIC développé par Redguard comporte dix questions qui ciblent les éléments essentiels de ladite norme. Les thèmes abordés sont les suivants: Gestion des risques, Stratégie de cybersécurité, Sensibilisation & Formation, Surveillance des systèmes, Gestion des incidents (Incident Management), Gestion de la continuité des activités (Business Continuity Management), reprise après sinistre (Disaster Recovery) et Communication de crise.



*Autres:	
Industrie	50.0%
Consultation	16.7%
Education	16.7%
Bureau d'ingénieur	8.3%
Développement de logiciels	8.3%

Figure 1: Entreprises interrogées par branche (%)

Organisations participant à l'enquête

Redguard a invité près de 2000 organisations suisses à évaluer leur niveau de sécurité au moyen du Quick-Test de la norme minimale pour les TIC. Cette année encore, plus de 100 organisations de différentes branches s'y sont intéressées et nous ont fourni leur auto-évaluation.

La figure 1 montre que les résultats de l'enquête Security Survey sont une nouvelle fois largement étayés. Les entreprises et organisations participantes proviennent des branches les plus variées, avec une répartition très équilibrée. Parallèlement, des entreprises de tailles très diverses ont contribué à l'enquête Security Survey, comme nous pouvons le voir dans la figure 2. D'après leur réponses, 41% d'entre elles sont de grandes entreprises de plus de 500 collaboratrices et collaborateurs. Les PME représentent la plus grande part avec 25% de petites entreprises (1-50 employés) et 22% de moyennes entreprises (50-200 employés).

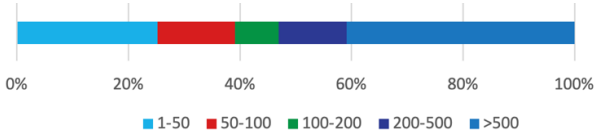


Figure 2: Organisations interrogées par nombre d'employé

La norme minimale pour les TIC n'est pas respectée pour la plupart d'entre elles

Bien que les entreprises estiment que leur niveau de sécurité en 2023 est meilleur ou inchangé sur tous les points par rapport aux années précédentes, la valeur actuelle est également nettement inférieure au niveau minimal recommandé par la Confédération et les associations.

Néanmoins, nous nous réjouissons aussi des petits pas dans la bonne direction, que nous percevons également dans les demandes croissantes des PME. De plus en plus sensibilisées, elles savent qu'elles sont une cible particulièrement appréciée des agresseurs. Ces derniers escomptent en effet que les PME ne prennent que peu ou pas de mesures de sécurité, ce qui leur facilite la tâche en cas d'attaque. C'est pourquoi il est indispensable pour les PME d'élever leur niveau de sécurité au moins au niveau minimum. Vous trouverez de l'aide à ce sujet sous le point Mesures.

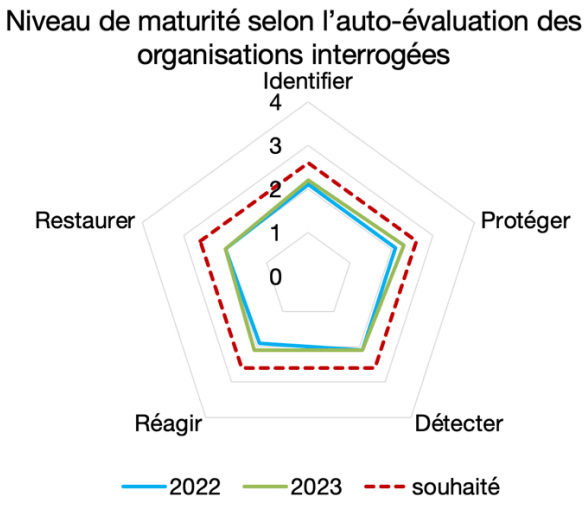


Figure 3: Résultats de l'enquête Redguard Security Survey

	2019	2020	2021	2022	2023	souhaité
Identifier	2.0	2.0	2.0	2.1	2.2	2.6
Protéger	2.3	2.3	2.1	2.1	2.3	2.6
Détecter	2.2	1.9	1.9	2.1	2.1	2.6
Réagir	2.2	1.8	1.7	1.9	2.1	2.6
Restaurer	1.7	1.7	1.8	2.0	2.0	2.6

Tableau 2: Résultats par fonction par rapport à l'année précédente

La figure 3 montre que, selon leur propre évaluation, la majorité des organisations interrogées n'ont pas encore atteint le niveau de sécurité minimal de la norme minimale pour les TIC.

	2022		2023	
Fonction	**Non atteint**	**Atteint**	**Non atteint**	**Atteint**
Identifier	66%	34%	60%	40%
Protéger	57%	43%	54%	46%
Détecter	63%	37%	59%	41%
Réagir	61%	39%	58%	42%
Restaurer	66%	34%	63%	37%
Total	**63%**	**37%**	**59%**	**41%**

Tableau 1 : Résultats de l'enquête concernant les cinq fonctions et comparaison avec l'année précédente

Nous constatons une stagnation dans les domaines *Identifier*, *Détecter* et *Récupérer*. Une légère amélioration est en revanche signalée pour les fonctions *Protéger* et *Réagir.*

Un examen des réponses (Tableau 1) ventilées selon les cinq fonctions de la norme minimale pour les TIC montre clairement que seules 41% des organisations considèrent qu'elles atteignent le niveau de sécurité requis.

Dans le tableau 2, nous obtenons un aperçu intéressant des auto-évaluations des cinq dernières années, toutes analysées par Redguard. La fonction *Protéger* obtient systématiquement les meilleurs points. L'une des raisons pourrait être que, dans le développement de logiciels en particulier, la sécurité est de plus en plus

souvent prise en compte dès le début. Grâce à l'approche DevSecOps, l'interaction fluide entre les secteurs développement logiciel (Dev), sécurité (Sec) et opérationnel (Ops) est assurée.

Redguard recommande cette approche depuis longtemps, car elle est plus efficace et moins coûteuse. Un aspect particulièrement important est la sécurité des conteneurs et la configuration des outils d'orchestration comme Kubernetes. Les fonctions *Identifier* et *Détecter* obtiennent des résultats légèrement moins bons. Cela indique que de nombreux incidents de sécurité sont détectés trop tard parce que les systèmes ne sont pas suffisamment surveillés en continu et qu'il n'est pas possible de donner l'alerte à temps. Là encore, nous recommandons des contre-mesures, par exemple sous la forme d'un scan continu de sécurité (Continuous Security Scanning), c'est-à-dire des scans de vulnérabilité réguliers qui reflètent le niveau de sécurité d'une entreprise entre des tests d'intrusion (Penetration Test) programmés périodiquement, et qui évitent les mauvaises surprises. Un centre d'opérations de sécurité, par exemple, permet de détecter et de réagir rapidement aux cybermenaces dans le cloud. Cela peut considérablement alléger la charge de travail de l'équipe informatique interne et massivement augmenter la sécurité.

En regardant le tableau 2, on voit clairement que les entreprises se sont le plus mal notées dans les fonctions *Réagir* et *Récupérer*, toutes années confondues. Redguard a reconnu ce besoin et accompagne sa clientèle depuis de nombreuses années en tant que partenaire d'incident dans le cadre de mandats de CISO. Depuis plus d'un an, les clientes et clients recourent également à notre équipe de réponse aux incidents (Incident Response Team) en tant que service indépendant. Ici aussi, nous constatons une sensibilisation croissante au thème de la cybersécurité et des incidents. Cependant, selon leur propre auto-évaluation, la plupart des entreprises participantes s'estiment trop peu préparées pour gérer un incident de sécurité.

Redguard vous aide à vous conformer à la norme minimale pour les TIC

La norme minimale pour les TIC est conçue de manière à pouvoir être mise en œuvre par toutes les entreprises, quelle que soit leur branche ou leur taille. Les lignes directrices et l'outil d'auto-évaluation de l'Office fédéral pour l'approvisionnement économique du pays3 présupposent de solides connaissances spécialisées et une approche pragmatique est indispensable pour réussir à implémenter la norme minimale pour les TIC. Redguard apporte son expertise aux entreprises à cet égard.

Identifier – Connaissez vos risques et adoptez une approche stratégique de la sécurité de l'information

- Redguard vous aide à identifier les risques cyber de votre organisation et à les répertorier de manière systématique. Ensemble, nous mettons sur pied une stratégie de sécurité de l'information basée sur vos risques afin de les gérer et de les contrôler.

Protéger – Protégez vos systèmes et formez vos employés

- Élaborez des directives pour protéger vos systèmes et mettez-les en œuvre. Redguard vous aide à élaborer les bonnes mesures dans les domaines de la gestion des accès, de concept Firewall, de concept de zone réseau ainsi que de la protection contre les Malwares.
- Les mesures techniques ne suffisent souvent pas: formez vos employés et montrez-leur comment ils peuvent contribuer à sécuriser les informations. Redguard vous apporte son soutien, soit à l'aide d'offres de formation classiques, soit par des campagnes de Live Hacking ou de phishing.

Détecter – Connaissez vos points faibles et testez votre défense

- Mettez en place vos systèmes et processus de sorte que les incidents de sécurité potentiels puissent être détectés.
- Mettez vos systèmes et votre sécurité informatique à l'épreuve en effectuant des tests de pénétration ou de simulation d'attaque. Les spécialistes de Redguard effectuent des tests et des attaques ciblées en votre nom afin d'identifier les opportunités d'amélioration.

Réagir – Planifiez et pratiquez votre réaction aux incidents de cybersécurité

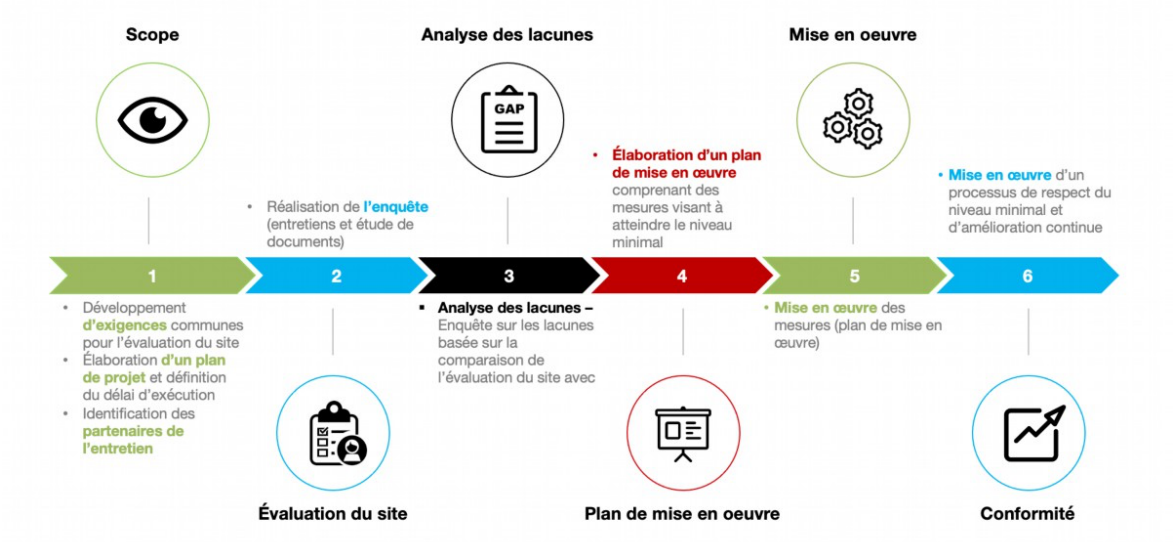
- Un plan de réponse vous aide à réagir correctement en cas d'urgence et à gagner du temps. Lorsqu'un plan de réaction est en place, vous avez déjà répondu à de nombreuses questions: Qui est responsable dans votre organisation en cas d'incident de cybersécurité? Comment informez-vous vos employés et vos clients? Fermezvous complètement les systèmes ou maintenez-vous un fonctionnement d'urgence de certaines activités?
- Chez Redguard, vous pouvez vous entraîner à gérer un cas d'urgence à l'aide d'un exercice Tabletop. Jouez un scénario adapté à votre organisation, étape par étape, et tirez-en des opportunités d'amélioration et des mesures à prendre.

Récupérer – Retour à la normale

- Établissez un plan de récupération et fixez des objectifs de récupération spécifiques: Pour quelle durée maximum pouvez-vous vous passer de vos systèmes? Combien de pertes de données pouvez-vous supporter?
- Redguard aide votre organisation à atteindre le niveau minimum de sécurité recommandé dans la fonction «Récupérer» en travaillant avec vous pour développer des plans de récupération.

Mise en œuvre globale de la norme minimale pour les TIC

Concentrez-vous sur votre activité principale, pendant que nous faisons passer votre sécurité informatique au niveau supérieur. Avec une équipe de plus de 50 spécialistes de la sécurité, nous vous offrons des services complets.



Évaluation du site selon la norme minimale pour les TIC

Faites déterminer le degré de maturité de votre sécurité de l'information par un organisme indépendant. Nos spécialistes vérifient vos systèmes, documents et processus. Les résultats obtenus sont discutés plus en détail dans le cadre d'entretiens. Au final, vous recevez un rapport énumérant les vulnérabilités qui ont été identifiées et les mesures et recommandations d'action concrètes pour y remédier et améliorer la sécurité des informations.

CISOaaS – Mise en œuvre et maintien de la norme minimale pour les TIC

Avec le service «Security Officer as a Service» (SOaaS), vous avez un interlocuteur personnel qui met à votre disposition tout le savoir-faire de Redguard. Cette personne agit en tant que chef de projet au sein de votre organisation pour appliquer les recommandations d'actions issues de l'évaluation du site. Ce faisant, elle garantit le maintien de la norme minimale pour les TIC et l'amélioration continue du degré de maturité.

Aide en cas d'incident

Si, malgré toutes les mesures prises, votre entreprise est touchée par un incident de cybersécurité, les spécialistes de Redguard sont toujours disponibles pour vous aider.

Mesures

1.1 Mesures – Centre des opérations de sécurité (Security Operations Center, SOC)

Les opérations de sécurité se réfèrent au processus de surveillance, de vérification et de réaction aux événements de sécurité et aux menaces dans une infrastructure informatique. Elles permettent d'améliorer considérablement la cybersécurité d'une entreprise. Il s'agit avant tout de détecter et d'arrêter à temps les activités inhabituelles et potentiellement dommageables.

SOC as a Service

Avec notre Security Operations Center basé sur le cloud, vous externalisez votre cybersécurité aux experts Redguard de notre société sœur FusionOne. L'offre de services est accessible à toutes les organisations et entreprises qui utilisent Microsoft 365. Le SOC a également été développé et testé avec des PME et répond à leurs besoins au quotidien et à leur budget.

Pour plus d'informations: https://www.fusionone.ch

1.2 Mesures – Scan continu de sécurité (Continuous Security Scanning)

Grâce à des scans de vulnérabilité permanents et automatisés, vous garantissez à votre entreprise un niveau de sécurité toujours suffisant. Le Continuous Security Scanning convient pour faire le pont entre les tests d'intrusion réguliers.

Vérification automatisée des vulnérabilités

La plateforme suisse Vulnerability Guard développée par Redguard vous permet d'évaluer au mieux votre niveau de sécurité et de replacer les données dans un contexte historique. Vous pouvez ainsi voir clairement quelles nouvelles vulnérabilités ont été identifiées ou comblées et, par conséquent, comment la protection de votre infrastructure évolue au fil du temps. Vous démasquez ainsi non seulement les vulnérabilités génériques, mais aussi celles qui sont spécifiquement contenues dans vos applications.

Dix ans d'expérience en matière de cybersécurité ont été mis à profit pour développer cette plateforme. Néanmoins, contrairement à d'autres scans de vulnérabilité, elle peut être utilisée sans expert en sécurité informatique et demande un budget limité.

1.3 Mesures – Réponse aux incidents

Même si vous vous préparez et formez vos collaboratrices et collaborateurs, un incident de sécurité peut survenir. En cas d'attaque, il est essentiel de réagir immédiatement et de manière ciblée. Nos spécialistes en sécurité vous aident à vous préparer au mieux. Lors d'un incident, vous pouvez en outre compter sur le soutien de notre équipe de réponse aux incidents. Nous veillons à ce qu'aucun temps précieux ne soit perdu et que les dommages causés à votre entreprise soient aussi limités que possible.

Équipe de réponse aux incidents – En cas d'urgence vous n'êtes pas seuls

Nous vous aidons à endiguer et à analyser les cyberincidents 24 heures sur 24 et 7 jours sur 7 et à rétablir les activités de votre entreprise. Votre équipe de réponse aux incidents couvre toutes les expertises nécessaires (technologie, exigences réglementaires, etc.) et est en contact permanent avec les autorités et les autres équipes de réponses aux incidents. Nous assurons un déroulement structuré et gardons la tête froide.

Pour plus d'informations: https://www.redguard.ch/fr/consulting/cyber-security-incident/

1.4 Mesures – DevSecOps

Pour les personnes concernées, DevSecOps ressemble souvent à un puzzle dont les pièces ne sont pas encore assemblées. Un partenaire global comme Redguard vous aide à les relier de manière optimale et à impliquer toutes les parties prenantes.

Organisation

Le succès de DevSecOps nécessite une compréhension uniforme à l'échelle de l'organisation et des processus correspondants. Avec notre évaluation DevSecOps, nous relevons le degré de maturité actuel et vous aidons à élaborer des processus et des concepts DevSecOps en tenant compte de toutes les parties prenantes.

Technique

Le succès de DevSecOps nécessite une compréhension uniforme à l'échelle de l'organisation et des processus correspondants. Avec notre évaluation DevSecOps, nous relevons le degré de maturité actuel et vous aidons à élaborer des processus et des concepts DevSecOps en tenant compte de toutes les parties prenantes.

Usagers

Pour garantir durablement le succès de DevSecOps, il faut également développer un savoir-faire interne. Nous proposons à cet effet des ateliers d'introduction au thème DevSecOps, mais aussi des formations approfondies pour les spécialistes, par exemple dans le domaine de la sécurité des conteneurs et de Kubernetes.

Annexe

1.5 Annexe 1: Présentation du Quick-Test

Enquête sur la norme minimale pour les TIC

Le Quick-Test développé pour cette étude est basé sur les cinq fonctions de la norme minimale pour les TIC et comporte dix questions spécifiques. Cela permet de se prononcer sur le niveau de maturité des organisations interrogées. Vous trouverez le Quick-Test à l'adresse suivante: (FR) http://ikt-fr.redguard.ch (DE) http://ikt.redguard.ch

N°	Question
1	**Risques et vulnérabilités (Identifier)** J'étudie les risques et les vulnérabilités et j'identifie les systèmes critiques.
2	**Stratégie de cybersécurité (Identifier)** J'ai émis des directives pour la cybersécurité dans mon entreprise, par exemple sous la forme d'une stratégie et d'une politique/de directives.
3	**Politique & processus (Protéger)** Je fixe une politique de protection des systèmes d'information et les actifs, y compris un processus d'amélioration continue et de développement de la sécurité de l'information.
4	**Sensibilisation & formation (Protéger)** Je m'assure que tous les employés de notre organisation sont formés à la sécurité de l'information, à chaque niveau et pour chaque fonction, et qu'ils connaissent leurs responsabilités et le comportement à adopter.
5	**Détection / monitoring (Détecter)** Je mets en place un monitoring continu des systèmes et des réseaux pour détecter les incidents potentiels de cybersécurité.
6	**Détection / contention (Détecter)** Je définis le processus pour m'assurer que l'on détecte à temps les anomalies et les incidents de sécurité et que l'on comprenne l'impact potentiel d'un incident.
7	**Mon organisation est prête à faire face à des incidents majeurs (Réagir)** J'ai développé et teste régulièrement un processus pour répondre aux incidents qui se produisent – par exemple Business Continuity Management, Incident Response Planning, Disaster Recovery.
8	**Processus de gestion des incidents (Réagir)** Je veille à ce que les incidents de cybersécurité puissent être contenus et à ce que leur propagation soit stoppée, afin de limiter leur impact.
9	**Planification de la récupération (Récupérer)** Je m'assure que j'ai mis en place un plan de récupération qui garantisse le rétablissement rapide des systèmes après un incident.
10	**Plan de communication (Récupérer)** J'ai préparé un plan de communication en cas d'incident de cybersécurité et je m'assure qu'il tient compte de l'image de mon organisation auprès du public.

1.6 Annexe 2: Présentation de l'échelle de maturité

Chacune des dix questions du Quick-Test est notée sur une échelle de 0 à 4. Pour chacune des cinq fonctions (Identifier, Protéger, Détecter, Réagir et Récupérer), le niveau de maturité est déterminé par la moyenne des scores obtenus aux questions.

Niveau	Réponse
0 – Non mis en œuvre	Ce point serait important pour mon organisation, mais jusqu'à présent il n'existe que très peu d'informations à ce sujet.
1 – Mis en œuvre de manière limitée	Le processus / la directive n'est pas entièrement définie et n'est pas approuvée.
2 – Partiellement mis en œuvre	Le processus / la directive est presque entièrement définie et acceptée, mais déjà quelque peu dépassée, au moins en partie.
3 – Mis en œuvre	Le processus / la directive est entièrement définie et en grande partie approuvée. Le processus / la directive est également relativement récente et toujours valable et correcte. Toutefois, cette approche est largement statique.
4 – Optimisé	Le processus / la directive est entièrement mise en œuvre. Le processus / la directive est revue en permanence, améliorée régulièrement et son efficacité est assurée.

Pour en savoir plus sur la norme minimale pour les TIC:

- Site web de l'Office fédéral pour l'approvisionnement économique du pays : https://www.bwl.admin.ch/bwl/fr/home.html
- Factsheet norme minimale pour les TIC de Redguard https://www.redguard.ch/downloads/factsheet_ikt_minimalstandard_de.pdf
- Quick-Test de la norme minimale pour les TIC de Redguard
  DE: http://ikt.redguard.ch
  FR: http://ikt-fr.redguard.ch
- Site web de Redguard https://www.redguard.ch/fr/