Exigences thématiques – Conseils pratiques d'application et notes issues de l'évaluation externe de la qualité

Management Summary

Avec l'introduction des Normes internationales d'audit interne 2024 (ci-après dénommées « Normes »), The Institute of Internal Auditors (IIA) a introduit un nouvel élément obligatoire au sein du Cadre de référence international des pratiques professionnelles (CRIPP / IPPF) : les exigences thématiques (Topical Requirements, TR). Celles-ci définissent un socle minimal contraignant pour les audits portant sur certains domaines de risque et visent à garantir des standards de qualité uniformes pour l'audit interne à l'échelle mondiale.

Les premières TR entreront en vigueur en 2026. Les fonctions d'audit interne devront donc adapter en conséquence leurs processus de planification et d'audit. L'IIA met à disposition plusieurs documents officiels qui clarifient les principales questions et soutiennent la mise en œuvre pratique. Un principe essentiel est que les TR ne doivent être appliquées que lorsqu'un thème est jugé matériel dans le cadre de l'analyse périodique des risques (ou de l'analyse des risques au niveau de la mission) et qu'une mission d'assurance est prévue sur ce thème. Cette matérialité s'apprécie au regard de l'appétence au risque et des objectifs stratégiques de l'organisation. La question de savoir si une TR doit être appliquée dépend du résultat de l'analyse des risques, du périmètre de la mission qui en découle et du jugement professionnel de l'auditeur interne.

L'IIA souligne l'importance d'un processus de justification clair et compréhensible. Lorsqu'une TR n'est pas appliquée, ou ne l'est que partiellement, alors qu'un risque matériel a été identifié dans son champ d'application, il convient de documenter les raisons pour lesquelles la TR concernée, ou certaines de ses exigences, n'est pas pertinente ou ne correspond pas à la cause du risque.

Dans cet esprit, le groupe de travail « Professional Services Firms » de l'IIA Switzerland a élaboré ce livre blanc. Celui-ci combine les enseignements tirés de premiers projets pilotes menés sur le marché suisse avec des perspectives issues d'évaluations externes de la qualité. Il vise à soutenir les responsables de l'audit interne dans une mise en œuvre cohérente, fondée sur les risques et pragmatique de ces nouvelles exigences. Le document ne prétend pas être exhaustif ni officiellement contraignant ; il reflète l'opinion et l'interprétation des auteurs et du groupe de travail au moment de sa publication et se veut un guide pratique.

Première étape : orientation vers les TR et les sources officielles

L'IIA met à disposition sur son site web l'ensemble des informations essentielles relatives aux TR.

- Lien vers la page : https://www.theiia.org/en/standards/2024-standards/topical-requirements/

Ce contenu est régulièrement mis à jour et constitue la base de référence pour l'application des TR dans les travaux d'audit. Il comprend les TR publiées, les consultations en cours et les publications à venir. Pour chaque TR, la date à partir de laquelle son application devient obligatoire est clairement indiquée, en règle générale un an après sa publication.

Les premières TR entrant en vigueur sont les suivantes :

- Cybersécurité : à partir du 5 février 2026,
- Tierces parties : à partir du 15 septembre 2026,
- Comportement organisationnel : à partir du 15 décembre 2026,
- Résilience organisationnelle : à partir du 30 avril 2027.

Outre les TR elles-mêmes, l'IIA met à disposition plusieurs documents complémentaires qui soutiennent une application cohérente :

- Le Guide d'application des exigences thématiques, disponible en plusieurs langues, fournit des indications générales et pratiques pour leur application.
  - https://www.theiia.org/en/content/topical-requirements/topical-requirements-application-guidance
- Une section FAQ est publiée sur le site des TR.
- Le document « Assessing Topical Requirements Conformance » (Insights to Quality) fournit des indications sur la manière dont les TR sont prises en compte dans le cadre des évaluations internes et externes de la qualité, ainsi que sur la façon dont les fonctions d'audit interne peuvent s'y préparer au moyen d'une mise en œuvre pertinente et d'une documentation transparente.
  - https://www.theiia.org/globalassets/site/content/insights-to-quality/insights-to-quality-assessing-topical-requirements-conformance.pdf

Pour l'audit interne, il est recommandé de mettre en place un suivi structuré et régulier afin de prendre en compte les mises à jour en temps utile. Ce suivi comprend notamment :

- la détection précoce des nouvelles TR ou des TR révisées,
- la participation aux processus de consultation,
- la garantie d’une mise en œuvre dans les délais.

Perspectives sur les thèmes prévus

L'IIA prépare d'autres TR. Au moment de la publication du présent document, le processus de consultation relatif à la TR « Anti-corruption » est en cours. En outre, une lettre de recherche sur le thème « Talent Management » a été annoncée ; le processus de consultation correspondant est prévu pour octobre 2026. Ces deux TR ne seront pas applicables avant 2027 au plus tôt.

L'IIA présente également régulièrement son Risk and Topic Radar lors d'événements et de webinaires. Les thèmes qui y apparaissent au stade « Mature » (voir Fig. 1, en bleu) sont considérés comme établis ; l'élaboration de TR à leur sujet est donc particulièrement probable. Les thèmes importants et fortement évolutifs qui apparaissent dans le radar comme « Emerging » (voir Fig. 1, en vert) ne sont actuellement pas traduits en TR.

Le processus de suivi régulier recommandé dans la section précédente devrait donc également inclure une revue périodique du site web de l'IIA, afin de rester informé suffisamment tôt des nouvelles consultations et des futurs thèmes de TR.

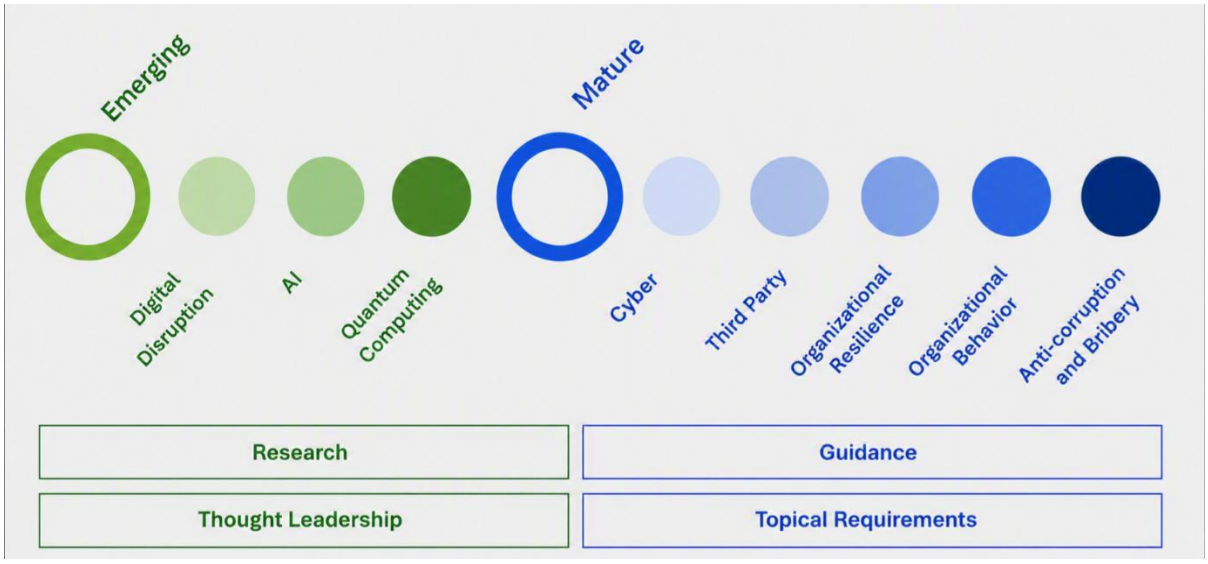

Fig. 1 : « Risk and Topics Maturity Radar de l'IIA », source : IIA

Application des TR

Les TR font partie intégrante du CRIPP (IPPF) de l'IIA et sont donc obligatoires pour les missions d'assurance, au même titre que les Normes. Pour les missions de conseil portant sur des domaines de risque pertinents, leur application est recommandée, mais non obligatoire.

Le Guide d'application des exigences thématiques précise que les TR peuvent s'appliquer dans les cas suivants :

- si le thème est expressément inclus comme objet d'audit dans le plan d'audit,
- si le thème est identifié au cours d'une mission d'audit,
- si le thème est inclus dans une mission d'audit, même s'il n'était pas initialement prévu dans le plan d'audit.

L'identification des thèmes d'audit s'effectue généralement dans le cadre de l'analyse périodique des risques (conformément à la Norme 9.4), lors de l'analyse des risques au niveau de la mission (conformément à la Norme 13.2) ou pendant la réalisation de l'audit. Une TR doit être appliquée dès qu'un risque correspondant est identifié et jugé matériel. Par conséquent, dans le cadre de l'analyse des risques concernée, il convient de vérifier s'il existe des risques liés aux TR en vigueur. Si un tel thème est retenu sur la base de l'analyse des risques, d'une contribution des parties prenantes ou au cours de l'exécution d'une mission d'audit, la TR correspondante doit être appliquée.

Dès qu'un risque est classé comme matériel et qu'une TR s'applique, la fonction d'audit interne doit en tenir compte, c'est-à-dire analyser et documenter son applicabilité. Cette analyse peut conduire à l'application de la TR dans l'audit ou à la non-prise en compte partielle ou totale de certains de ses éléments. Au minimum, cette analyse doit être effectuée au niveau de la mission concernée. L'IIA recommande toutefois de tenir compte des TR de manière cohérente tout au long du cycle d'audit, tant lors de la planification périodique qu'au niveau de la mission et de son exécution. Les recommandations complémentaires de l’IIA fournissent toutefois le cadre permettant une approche globale de l’ensemble du cycle d’audit, depuis la planification périodique, en passant par la planification au niveau de la mission, jusqu’à la réalisation de celle-ci conformément aux Standards.[1] Cela vaut également dans le cas du co-sourcing ou de l’outsourcing d’une mission, le donneur d’ordre demeurant responsable du respect des exigences applicables tout au long du cycle de vie de la mission.

[1] Voir, par exemple, l’*IIA Topical Requirements – Application Guidance*, chapitre 4 : *Applying Topical Requirements in the Audit Lifecycle*

À l'appui de cette démarche, le groupe de travail de l'IIA Switzerland met à disposition un arbre de décision présentant de manière structurée le processus permettant de déterminer l'applicabilité d'une TR (voir Fig. 2). Celui-ci facilite une évaluation cohérente et concluante des facteurs pertinents. L'arbre de décision indique également les cas dans lesquels une documentation compréhensible de l'approche « comply or explain » est nécessaire (voir la section suivante).

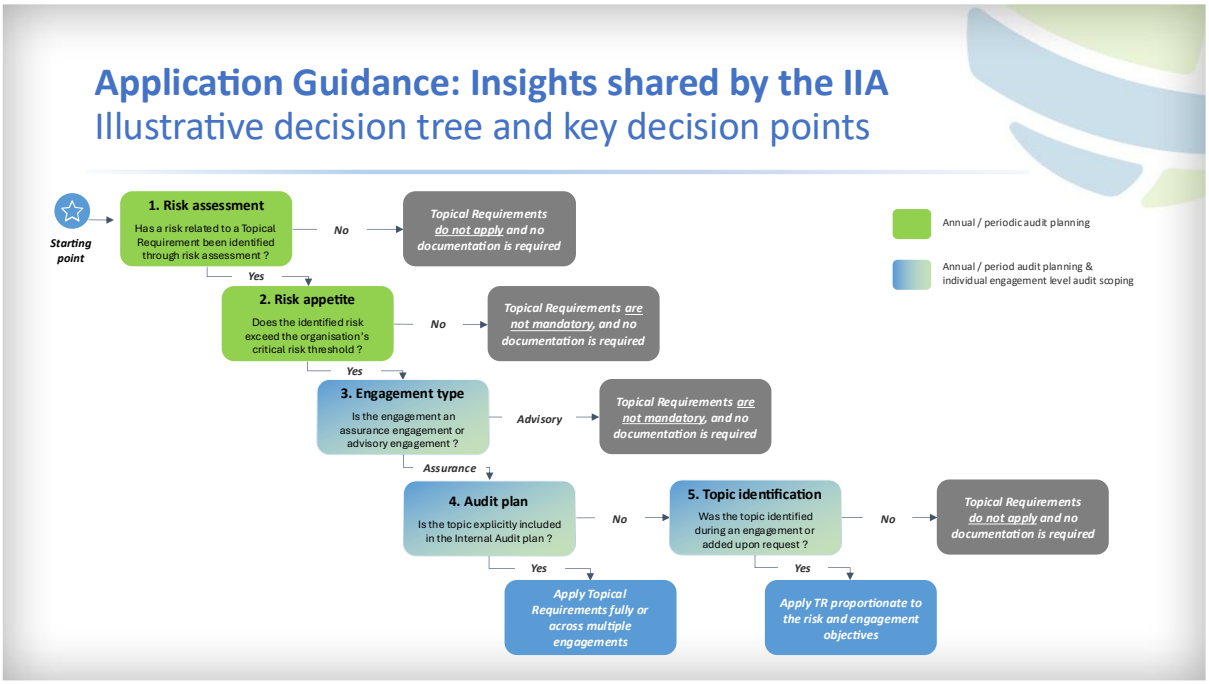

Fig. 2 : Arbre de décision pour l'application des exigences thématiques,
source : groupe de travail IIAS « Professional Services Firms »

Application du jugement professionnel

Le jugement professionnel est central dans toutes les décisions relatives à l'application d'une TR. L'IIA fait explicitement référence à l'approche « conform or explain » ou « comply or explain » lorsqu'un risque matériel identifié rend l'application d'une TR obligatoire et que la fonction d'audit interne ne l'inclut néanmoins pas, ou seulement partiellement, dans l'audit :

- si certaines exigences d'une TR ne sont pas applicables en raison de la nature, du contexte ou de la cause d'un risque, cela doit être clairement justifié et documenté ;
- si, par exemple, un risque découle d'une faiblesse de contrôle opérationnel, les exigences spécifiques relatives aux contrôles peuvent être principalement pertinentes, tandis que certains éléments de gouvernance de la TR peuvent ne pas s'appliquer.

Le Guide d'application souligne que des circonstances exceptionnelles, telles que des contraintes de ressources ou des caractéristiques propres à un secteur, peuvent également justifier des écarts. Dans de tels cas, l'auditeur interne devrait définir des mesures alternatives répondant à l'objectif de l'exigence concernée. Les travaux d'autres prestataires d'assurance internes ou externes peuvent aussi être pris en considération. Une documentation transparente et compréhensible demeure alors indispensable.

Couverture des exigences des TR sur plusieurs années ou plusieurs missions

Lorsqu'un thème d'audit est examiné sur plusieurs années, la TR correspondante doit être prise en compte à nouveau pour chaque mission et son applicabilité doit être vérifiée. Les exigences peuvent être réparties sur plusieurs missions, voire sur plusieurs années, pour autant que les éléments suivants soient clairement documentés :

- quels éléments ont été couverts et quand,
- quelles parties ont été délibérément reportées à des années ou missions ultérieures, et
- pour quelle raison cette décision est techniquement justifiable.

Cela signifie que toutes les exigences ne doivent pas nécessairement être couvertes dans une seule mission d'audit.

Le Guide d'application exige que toutes les décisions relevant du jugement professionnel (par exemple application partielle ou non-application) soient documentées dans les documents de planification, les papiers de travail ou les matrices d'applicabilité, et présentées de manière compréhensible lors des contrôles de qualité.

Attentes en termes de documentation

L'application de la TR, de même que l'omission partielle ou totale de certains éléments sur la base de décisions relevant du jugement professionnel, doivent être documentées de manière à permettre à un tiers indépendant de comprendre les décisions prises. La documentation peut être établie aux étapes du cycle de vie de l'audit où l'applicabilité est analysée (voir « Arbre de décision pour l'application des TR », Fig. 2).

Pour documenter l'application de la TR examinée, les guides d'utilisation de chaque TR mettent à disposition, en annexe, un outil ou un tableau de documentation optionnel.

Dans le cadre d'une évaluation, par exemple lors d'une évaluation externe de la qualité (EQA), il est essentiel que les décisions prises et leurs justifications soient suffisamment documentées et compréhensibles pour des tiers. Les TR, en tant que partie intégrante du CRIPP (IPPF), sont prises en compte dans l'évaluation des principes concernés, notamment en lien avec la planification, la réalisation et la communication des missions. Il n'existe pas d'évaluation distincte de chaque TR.

Lorsqu'une TR est pertinente pour une mission donnée, une Norme ne peut être considérée comme « pleinement conforme » dans le cadre d'une EQA que si tous les éléments de la Norme sous-jacente sont satisfaits.

Application en lien avec des exigences réglementaires

Comme l'explique le Guide d'application officiel de l'IIA, les principes suivants s'appliquent :

- si des dispositions légales ou réglementaires imposent des exigences plus strictes ou plus étendues que la TR, ces exigences déterminent le périmètre de l'audit.

Dans de tels cas, l'audit interne doit adopter une approche fondée sur les risques et comparative, en mettant en balance les exigences réglementaires, la TR et d'autres cadres de référence reconnus.

Il convient de souligner que les TR ne prescrivent pas la manière dont les thèmes audités doivent être organisés ; elles définissent l'approche d'audit. Leur objectif est de garantir une approche cohérente dans les domaines d'audit critiques et de respecter les exigences de qualité de base.

Communication des aspects liés aux TR

La conformité aux TR doit être documentée dans le cadre de la planification et de l'exécution de l'audit. Elle est également suivie au moyen du programme d'assurance et d'amélioration qualité (QAIP) de la fonction d'audit interne.

Un rapport distinct sur la conformité aux TR (par exemple à la Direction générale et/ou au Conseil d'administration) n'est pas nécessaire. Ces aspects doivent plutôt être pris en compte implicitement dans le reporting global relatif au QAIP.

Aide aux évaluateurs EQA

Pour les évaluateurs EQA, les contenus officiels de l'IIA - en particulier les documents disponibles sur le site web - constituent un point de référence essentiel. Ils définissent les attentes de l'IIA en matière de mise en œuvre des TR et d'évaluation de la conformité dans le cadre des évaluations de qualité. Le document « Assessing Topical Requirements Conformance » (Insights to Quality), qui fournit des indications détaillées, est particulièrement pertinent.

Les TR constituent un élément obligatoire du CRIPP (IPPF) et sont donc évaluées, comme les autres éléments de l'IPPF tels que les Normes, dans le cadre des évaluations internes et externes de la qualité. Le Quality Assessment Manual 2024 de l'IIA indique que les évaluateurs devraient examiner le plan d'audit fondé sur les risques afin de s'assurer que les TR en vigueur durant la période d'audit ont été correctement prises en compte. Cet examen s'effectue généralement, entre autres, par l'inspection des papiers de travail au niveau des missions individuelles.

Le document « Assessing Topical Requirements Conformance » clarifie la manière dont les fonctions d'audit interne et les évaluateurs devraient procéder pour évaluer la conformité aux TR. Dans ce contexte, l'IIA recommande notamment aux fonctions d'audit interne de :

- intégrer les TR dans les processus de planification et d’audit,
- documenter de manière transparente l'applicabilité des TR et les justifications en cas de non-application,
- veiller à ce que les processus d’audit, les papiers de travail et les autres documents reflètent la conformité aux TR de manière compréhensible.

Ainsi, selon la manière dont les TR sont mises en œuvre dans les différentes fonctions d’audit interne, les assesseurs prendront en compte les différents éléments du processus d’audit dès l’analyse de l’univers d’audit, l’analyse des risques et le processus de planification de l’audit interne, et évalueront si des thèmes couverts par les TR sont présents.

Les documents faisant autorité pour les évaluateurs comprennent notamment :

- l'analyse des risques et le plan d'audit (planification périodique ainsi qu'au niveau de la mission),
- le mémorandum de planification et les papiers de travail au niveau de la mission,
- Matrices de contrôle des risques,
- le guide d’utilisation de la TR, l’outil de documentation ou la checklist correspondante,
- Couverture des TR dans le QAIP.

Focus Cyber-TR : Aperçu des domaines à examiner

- **Gouvernance :** évaluation de la gestion stratégique et de l'ancrage organisationnel. Les éléments suivants sont examinés :
  - existence d'une stratégie formelle de cybersécurité, régulièrement mise à jour et soumise à l'examen du Conseil d'administration (y compris l'approbation du budget) ;
  - établissement de directives claires et définition des rôles et responsabilités au sein de l'organisation ;
  - garantie et évaluation des connaissances et compétences spécialisées nécessaires des collaborateurs responsables ;
  - gestion des parties prenantes : implication active de la Direction générale, des ressources humaines, du service juridique, de la conformité et des fournisseurs dans le dialogue sur les menaces et les vulnérabilités.
- **Gestion des risques :** examen des processus de gestion des risques cyber. Les éléments suivants sont examinés :
  - identification, analyse, atténuation et surveillance systématiques des cybermenaces dans toutes les unités organisationnelles ;
  - attribution claire des responsabilités en matière de suivi et de reporting continus de la situation de risque ;
  - mise en place de processus d’escalade rapide en cas de dépassement de seuils, ainsi que de mesures visant à promouvoir la sensibilisation générale aux risques ;
  - validation d'un processus de réponse et de rétablissement (détection, confinement, suivi) régulièrement exercé.
- **Processus de contrôle :** vérification de l'existence de contrôles internes et de contrôles liés aux fournisseurs destinés à protéger la confidentialité, l'intégrité et la disponibilité des systèmes et des données. Cela inclut notamment :
  - gestion du cycle de vie de tous les actifs informatiques (matériel, logiciels, services externes), de la sélection au déclassement ;
  - surveillance continue des vulnérabilités et gestion des talents afin de développer les compétences techniques ;
  - processus de renforcement de la sécurité informatique, incluant le chiffrement, la gestion des correctifs, la gestion des accès, le développement logiciel (DevSecOps) et la configuration ;
  - contrôles réseau, tels que la segmentation réseau, les pare-feux, l'accès VPN/Zero Trust (ZTNA), les contrôles IoT et les systèmes de détection et d'atténuation des intrusions (IDS/IPS) ;
  - sécurité des terminaux pour des services tels que la messagerie électronique, les navigateurs, la visioconférence et les applications cloud.

Organisation et planification d'une mission d'audit à l'exemple de la TR Cybersecurity

Déclencheur de la mission

En principe, les exigences des TR doivent être appliquées dès que la cybersécurité est identifiée comme un risque matériel dans le cadre de l'analyse périodique des risques et qu'une mission d'assurance est prévue à ce sujet. Cela s'applique lorsque le thème est expressément inclus dans le plan d'audit, lorsqu'il apparaît comme risque matériel dans le cadre d'une autre mission d'audit ou lorsque les parties prenantes demandent une mission d'audit supplémentaire non planifiée.

Dans la planification détaillée de la mission d'audit, il doit être démontré que les exigences individuelles de la TR ont été examinées quant à leur applicabilité. Si certains éléments ne sont pas inclus, ou ne le sont que partiellement, cet écart doit être justifié et documenté. L'écart peut également être résumé, par exemple pour l'un des trois domaines de la TR - gouvernance, gestion des risques, processus de contrôle - lorsque, pour une raison compréhensible, les aspects de gouvernance ne doivent pas faire partie de l'audit prévu (par exemple parce qu'ils ont été vérifiés par un autre prestataire d'assurance ou qu'ils sont inclus dans la planification pluriannuelle).

Il n'est pas obligatoire qu'un audit unique couvre simultanément toutes les exigences relatives à la cybersécurité. Au contraire, un audit ciblé est recommandé pour plusieurs raisons, car un audit complet de la thématique est difficile à réaliser sur les plans logistique et technique, en particulier dans le cas de la TR Cybersecurity. La fonction d'audit interne peut répartir les exigences sur plusieurs audits et sur plusieurs années. Cette organisation suppose toutefois que soient documentés les thèmes traités et leur calendrier, les aspects délibérément reportés à plus tard ainsi que la justification technique correspondante. L'application des exigences doit en outre être présentée de manière transparente et compréhensible pour les tiers dans les documents de planification et les papiers de travail.

Planification de la mission

Du point de vue du contenu, l'IIA s'appuie fortement sur des standards établis. La TR Cybersecurity cite dès le début le National Institute of Standards and Technology (NIST) afin d'établir les définitions de base de la cybersécurité et de la sécurité de l'information. En outre, la TR exige que la fonction d'audit interne adopte une approche comparative, en particulier lorsqu'il existe déjà des exigences réglementaires ou que les audits sont réalisés sur la base de cadres reconnus au niveau international. Aligner la planification de l'audit sur le cadre du NIST s'inscrit donc pleinement dans cette logique.

Exemple de plan d'audit sur une période de trois ans selon les exigences minimales :

Année	Fonction clé NIST	Focus selon la TR-Cyber	Objectifs spécifiques de l'audit et exigences TR
Année 1	Identifier (identify)	Gouvernance et fondements (éléments de gestion des risques et de contrôle)	Stratégie et rôles : Existence d’une stratégie formelle, définition des rôles et responsabilités, et implication des parties prenantes. Identification des risques : Processus d'analyse des cybermenaces dans l'ensemble de l'organisation.

			Gestion des actifs : Cybersécurité dans le cycle de vie de tous les actifs informatiques (matériel, logiciels, fournisseurs).
Année 2	Protéger (Prevent)	Processus de contrôle préventifs (contrôles et gestion spécifique des risques)	Sécurité système et réseau : Gestion des accès, chiffrement, gestion des correctifs, DevSecOps. Infrastructures : Contrôles réseau (pare-feux, ZTNA, segmentation) et sécurité des terminaux (messagerie électronique, cloud, navigateur). Facteur humain : Gestion des talents afin de maintenir les compétences techniques et de sensibiliser les collaborateurs.
Année 3	Détecter, répondre, rétablir (Détecter, réagir, restaurer)	Surveillance et gestion des événements (contrôles résiduels et gestion des risques)	Surveillance : Surveillance continue des vulnérabilités et utilisation de systèmes de détection/prévention des intrusions (IDS/IPS). Escalade : Processus permettant de signaler rapidement les risques inacceptables à la Direction. Gestion des incidents : Mise en œuvre et tests réguliers d'un processus de réponse aux incidents et de rétablissement (détection, confinement, rétablissement, suivi).

Ce livre blanc a été élaboré par le groupe de travail « Professional Services Firms Group » de l'IIA Switzerland. Les coauteurs Urgent Azizi, Markus Berger, Christian Jung et Markus Pfeiler ont recueilli et intégré les avis d'autres personnes ainsi que ceux de l'IIA Switzerland. Ce livre blanc vise à soutenir les auditrices et auditeurs internes dans la mise en œuvre des Topical Requirements et doit servir de guide d'orientation.