ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Règlement d'organisation du Risk Management à l'EPFL

LEX 1.4.3

La version 1.0 a été approuvée par la Direction le 22 juin 2009 et en Conférence des Doyens le 6 juillet 2009.
La version 2.0 a été approuvée par la Direction le 30 mai 2011. Version 2.30 du 3 septembre 2018

Table des matières

Liste des figures

Introduction

Bases légales

La Direction de l'EPFL

vu la Directive du Conseil des EPF concernant la gestion des risques des EPF et des établissements de recherche du 4 juillet 2006 et

vu l'Ordonnance sur l'organisation de l'Ecole polytechnique fédérale de Lausanne du 1e mars 2004, état au 1er janvier 2017,

arrête

Objet

Le présent règlement définit l'organisation du Risk Management (RM) au sein de l'Ecole polytechnique fédérale de Lausanne (EPFL), l'organisation et les compétences décisionnelles du Comité Risk Management (CRM) et des comités qui lui sont rattachés.[1]

Périmètre de la gestion des risques de l'EPFL

Le périmètre de la gestion des risques comprend l'EPFL, ainsi que le périmètre étendu (non exhaustif), soit :

Périmètre EPFL

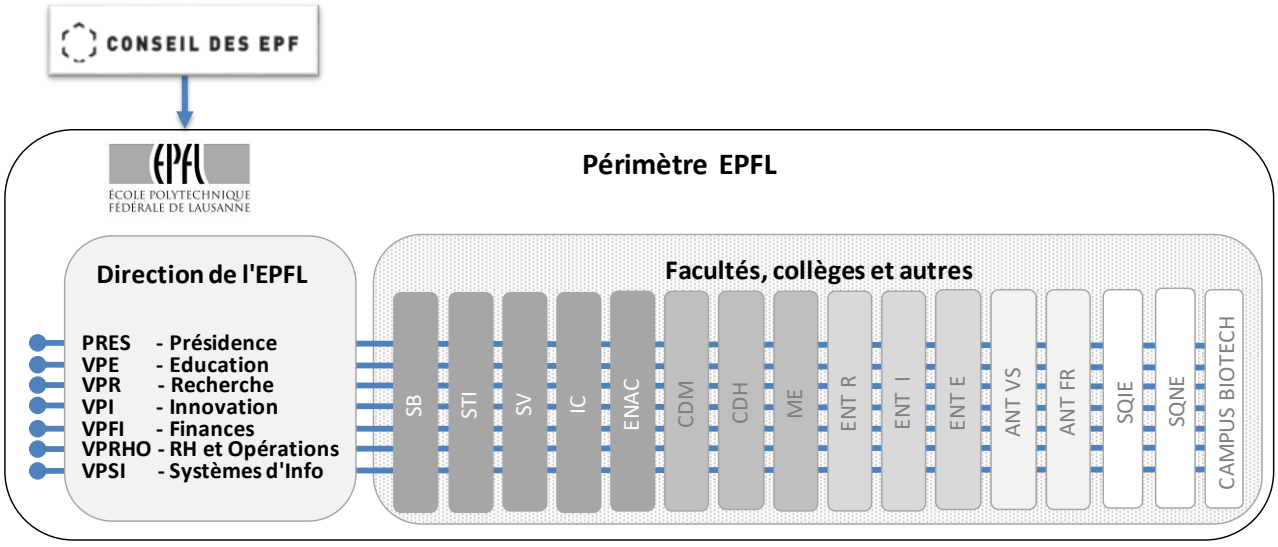

Figure 1 – Périmètre de la gestion des risques de l'EPFL

[1] Les référentiels applicables sont le COSO et le COBIT.

COSO = Le COSO est un référentiel de contrôle interne défini par le Committee Of Sponsoring Organizations of the Treadway Commission.

COBIT = Le CobiT (Control Objectives for Information and related Technology – Objectifs de contrôle de l'Information et des Technologies Associées) est un outil fédérateur qui permet d'instaurer un langage commun pour parler de la gouvernance des systèmes d'information tout en tentant d'intégrer d'autres référentiels tels que ISO 9000, ITIL.

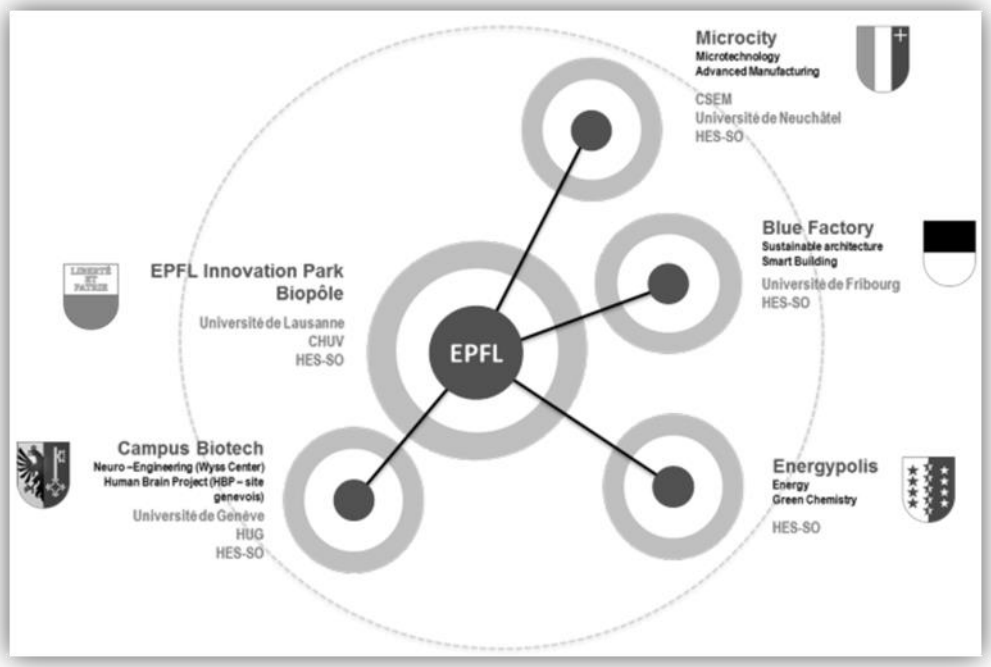

Figure 2 – Schéma des antennes cantonales EPFL

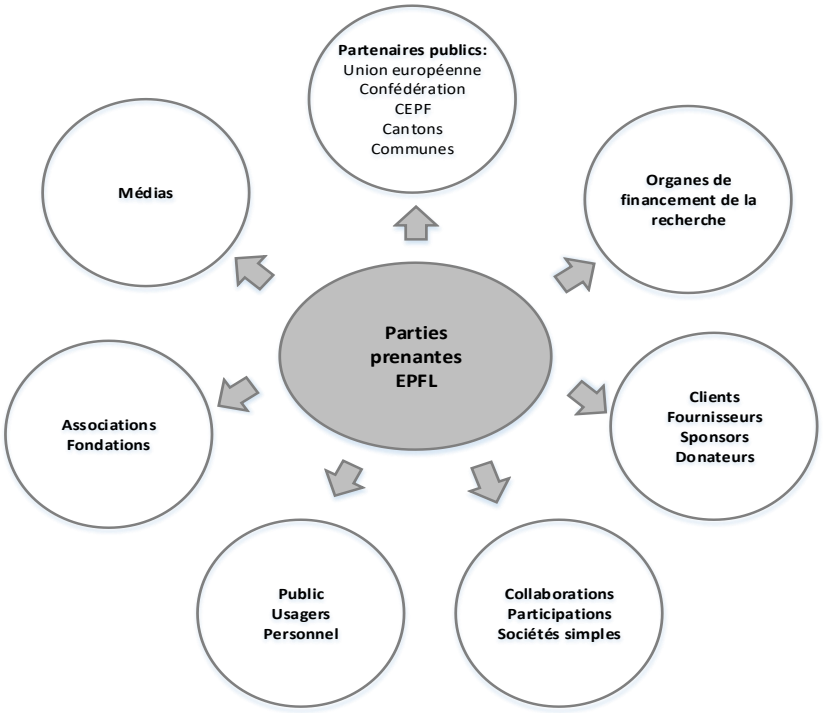

Figure 3 – Périmètre étendu de l'EPFL

Organisation du Risk Management à l'EPFL

Comité Risk Management (CRM)

Composition et rattachement

Le CRM est composé de quatre membres :

La Vice-présidente pour les finances, la General Counsel, le Délégué à la sécurité, le responsable du contrôle interne et gestion des risques.

Le CRM est conseillé par trois représentants du domaine académique. Leur rôle est d'apporter l'expertise académique, notamment dans le cadre de l'analyse des risques du périmètre EPFL (voir fig. 1)

Ce comité rapporte directement au Président de l'EPFL via la Vice-présidente pour les finances.

Le CRM coordonne les activités des six comités qui lui sont rattachés selon le schéma ci-après.

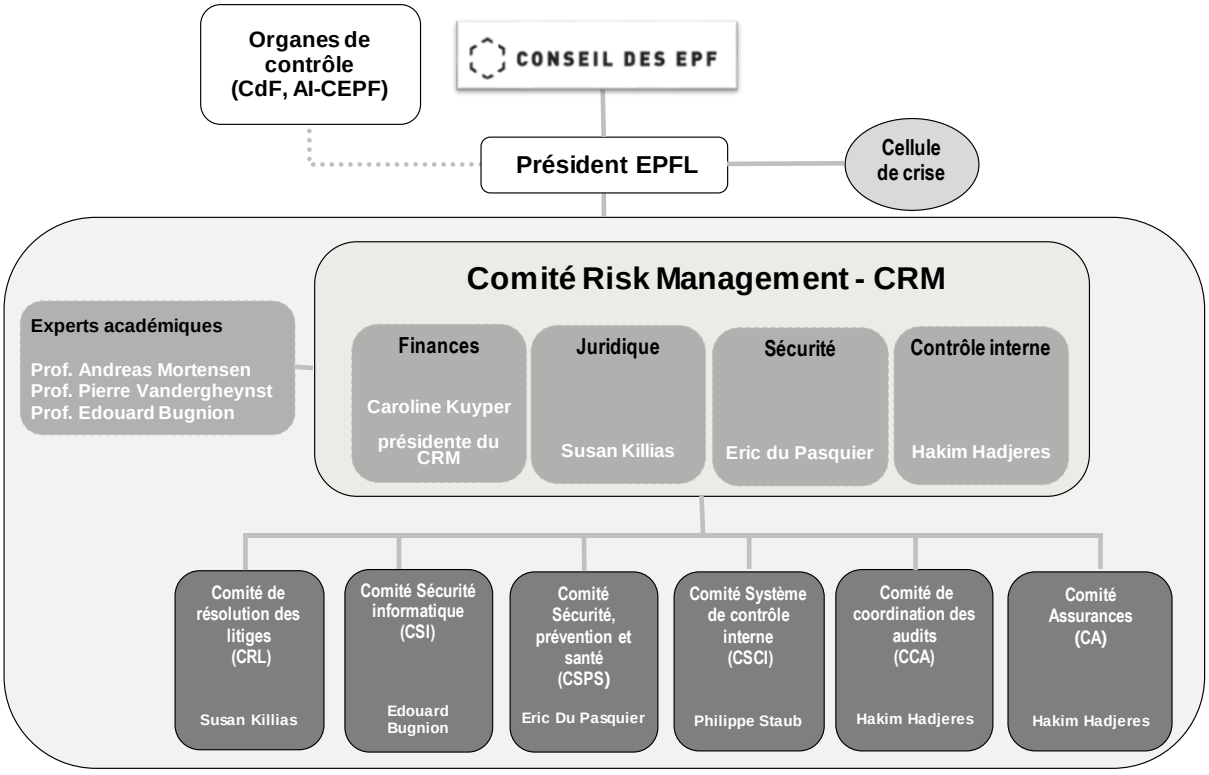

Figure 4 – Organisation du CRM et des comités

Domaines de risques et responsables

Le CRM analyse les risques de l'ensemble des domaines de l'EPFL. La liste des responsables et des domaines est présentée ci-dessous :

Rattachem.	Entité / Domaine	Responsable
P	Présidence	Martin Vetterli
P	Affaires professorales	Hassan Sadeghi
P	Développement et communication	A repourvoir
P	General Counsel	Susan Killias
P	Protection des données	Eva Thélisson
P	EPFL Alumni	Leïla Ojjeh
P	Promotion des sciences	Farnaz Moser
P	Service philanthropie	Nathalie Katharina Fontana
P	Egalité	Helene Fueger
P	Accréditation et assurance qualité	William Pralong
VPE, ENT-E	Vice-présidence éducation	Pierre Vandergheynst
VPR, ENT-R	Vice-présidence recherche	Andreas Mortensen
VPI, ENT-I	Vice-présidence innovation	Marc Gruber
SI	Vice-présidence systèmes d'information	Edouard Bugnion
FI-VP	Vice-présidence Finances	Caroline Kuyper
FI-VP	Comptabilité	Bertold Walther
FI-VP	Planification, Trésorerie & données institutionnelles	Yves Allegri
FI-VP	Contrôle interne, gestion des risques & assurances	Hakim Hadjeres
FI-VP	Contrôle de gestion	Marc Bachelot
RHO-VP	Vice-présidence RHO	Etienne Marclay
RHO-VP	Ressources humaines	Susanna Swann
RHO-VP	Sécurité, prévention & santé	Eric Du Pasquier
RHO-VP	Immobilier & infrastructures	Pierre Gerster
RHO-VP	Achats	Elvis Fontaine
RHO-VP	Centre de congrès	Julianne Jammers
RHO-VP	Restauration et commerces	Roland Deléchat
RHO-VP	Campus durable	Philippe Vollichard
ANT-VS	EPFL Valais Wallis	Marc-André Berclaz
ANT-FR	EPFL Fribourg	Anne-Claude Cosandey
	Faculté / Collège	
SB	Sciences de Base	Jan S. Hesthaven
I&C	Informatique & Communications	James Larus
ENAC	Environnement Naturel, Architectural & Construit	Marilyne Andersen
SV	Sciences de la Vie	Gisou van der Goot
STI	Sciences & Techniques de l'Ingénieur (yc Antenne NE)	Ali Sayed
CDM	Collège du Management	Dominique Foray
CDH	Collège des Humanités	Béla Kapossy
EPFL ME	EPFL Middle East	Franco Vigliotti

Figure 5 – Domaines de risques et responsables

Missions du CRM

Le CRM a pour missions de :

1. mettre en œuvre la **politique de gestion des risques** à l'EPFL en conformité avec la Directive du Conseil des EPF sur la gestion des risques ;
2. proposer **une organisation et des procédures** propres à assurer la conformité légale (compliance) ;
3. garantir l'**identification des risques** et proposer la mise en place des mesures propres à les réduire à un niveau acceptable ;
4. veiller, via le CFO à ce que les **détenteurs de risques** les gèrent, les communiquent au CRM et effectuent régulièrement les **mises à jour des actions de mitigation**;
5. superviser via le **portefeuille d'assurances** et l'adapter aux besoins;
6. soutenir **les actions et initiatives individuelles** visant à améliorer la gestion des risques et des opportunités à l'EPFL ;
7. **rendre compte au Président** et à la Direction de l'EPFL sur une base annuelle et de façon régulière de l'état ainsi que de l'évolution des dossiers liés au Risk Management.

Les membres du **CRM** sont tenus au devoir de réserve. Le CRM peut prendre toute mesure utile à l'accomplissement de son mandat, notamment des mesures provisionnelles.

Membres du CRM[2]

Nom	***Fonction***	***Domaines***	***Rattachement***
Caroline Kuyper	Vice-présidente	Finances	FI
Susan Killias	General Counsel	Juridique	P-GEC
Eric Du Pasquier	Délégué à la Sécurité	Sécurité, prévention et santé	RHO
Hakim Hadjeres	Chef de service	Contrôle interne, assurances	FI

Experts académiques

Nom	***Fonction***	***Domaines***
Andreas Mortensen	Vice-président R	Risques stratégiques recherche
Pierre Vandergheynst	Vice-président E	Risques stratégiques éducation
Edouard Bugnion	Vice-président SI	Risques stratégiques informatique

Fonctionnement et rapports du CRM

Le CRM se réunit au minimum une fois par mois. Un ordre du jour et des procès-verbaux sont établis et distribués. Cette séance est généralement précédée d'une réunion avec le comité de sécurité informatique.

Le CRM édite un **rapport annuel** à l'attention du Président de l'EPFL et de la Direction EPFL. Ce rapport présente les activités du CRM et de tous les groupes et comités, ainsi que les recommandations générales. Il est approuvé par le Président. Son contenu est disponible pour les auditeurs internes du Conseil des EPF (CEPF) et les auditeurs externes du Contrôle fédéral des Finances (CdF).

D'autres rapports peuvent être transmis au Président et à la Direction EPFL pour des dossiers sensibles ou spécifiques.

[2] Note : en cas de besoin, d'autres experts peuvent être invités par le CRM

Devoir d'annonce / information

Le CRM informe :

Qui	*Thèmes*
Le CEPF	De tous les cas pouvant porter atteinte à l'image ou la réputation de l'EPFL sur proposition de la General Counsel ou de la Présidente du CRM et après validation du Président de l'EPFL : application de la Directive du CEPF sur le devoir d'annonce du 14 septembre 2001 (LEX 1.8.0.2).
Le Président et la Direction de l'EPFL	Sur la base d'un rapport annuel. Sur une base ad hoc lorsque les circonstances l'exigent.
Les responsables d'unité, les Vice-présidents, doyens de facultés et directeurs de collèges	Des bonnes pratiques en matière de Risk Management. De leurs devoirs d'annonces des risques, notamment ceux liés aux sinistres et aux projets. De l'évolution dans le domaine de la gestion des risques à l'EPFL.
Le responsable de la communication	De tous les dossiers sensibles sur une base ad hoc. De tous les thèmes en relation avec l'image de l'EPFL.

Registres des risques

Le CRM revoit au minimum une fois par année en juin, l'évolution des analyses de risques provenant des différentes bases de données.

Domaine	*Registres*	*Gestionnaire*	*Base de données*
Direction EPFL, services centraux, facultés et collèges	Registre des risques stratégiques & opérationnels	Hakim Hadjeres	Excel
Sécurité, prévention et santé	Cadastre des dangers	Eric Du Pasquier	SAP – EHS
Audits	Registre et plan des révisions et suspens	Hakim Hadjeres	Excel
SCI	Registre des risques financiers et contrôles clés	Philippe Staub	Excel
Assurances	Tableau des assurances et sinistralité	Hakim Hadjeres	Excel
Système d'information	Registre des risques de sécurité informatique	Edouard Bugnion	Excel

Gestion de crise

Le Président pilote la cellule de crise de la Direction lorsqu'un évènement majeur touche à la sécurité des personnes, de l'informatique ou des bâtiments. En cas d'absence, les remplaçants sont dans l'ordre: le Vice-président pour la recherche, puis le Vice-président pour les ressources humaines et opérations.

Le dossier de crise règle le mode de fonctionnement de la cellule de crise. Il est tenu à jour par le DSPS.

Dans le domaine de la sécurité informatique, la cellule de crise informatique est intégrée à la cellule de crise de la Direction ; le dossier de crise « sécurité informatique » est tenu par le responsable de la sécurité informatique.

Protection des données et archivage

La loi sur la protection des données s'applique à tous les cas traités. Tous les dossiers, documents et fichiers électroniques sont conservés et archivés (archives > 50 ans).[3]

[3] Loi fédérale sur l'archivage (LAr) du 26 juin 1998 (RS 152.1)

Comité Sécurité, prévention et santé (CSPS)

Composition et rattachement

Le CSPS est conduit par le Délégué du DSPS de l'EPFL. Il rapporte directement au CRM.

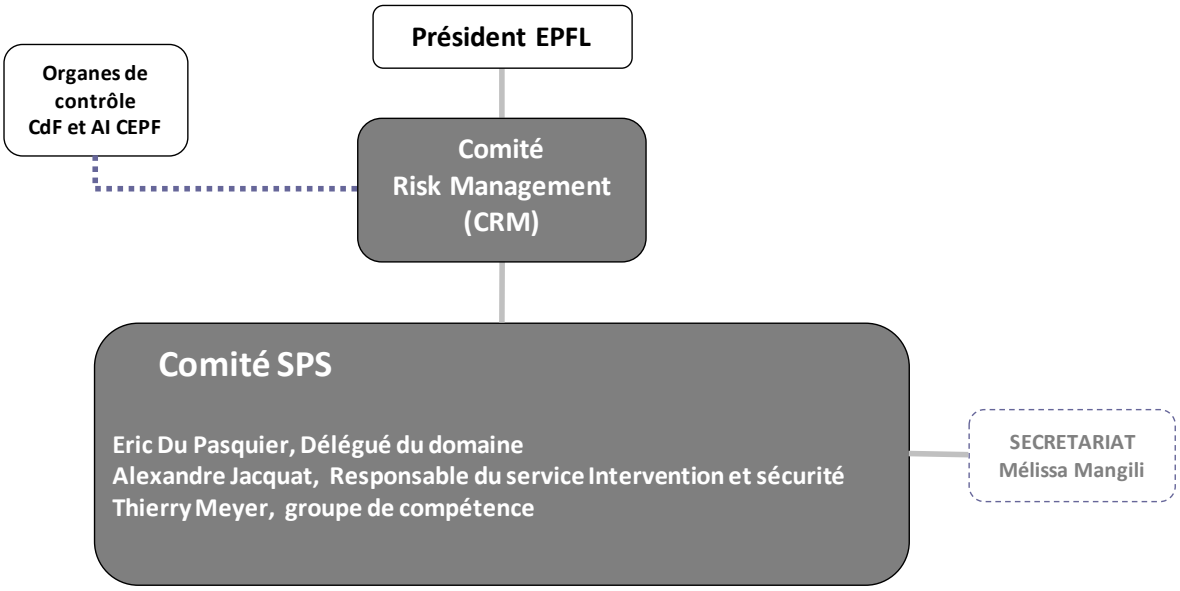

Figure 6 – Organisation du Comité Sécurité, prévention et santé (CSPS)

Missions du Comité SPS (CSPS)

En relation étroite avec les experts du DSPS, le CSPS développe et met en œuvre la politique de sécurité et santé de l'EPFL. Il coordonne les plans d'actions et de contrôles de sécurité spécifiques aux différentes facultés, collèges et antennes de l'EPFL.

Il veille notamment :

- au développement et à la formation du réseau des correspondants de sécurité (COSEC);
- au cadastrage des risques et au suivi des mesures d'atténuation de ceux-ci;
- à la formation de l'ensemble des collaboratrices et collaborateurs dans le domaine de la prévention;
- au reporting et au suivi des actions de mise en conformité;
- à la collaboration et aux échanges d'expériences avec les différents réseaux de sécurité, tant dans le monde académique qu'avec les secteurs public et privé.

Fonctionnement du Comité SPS

Le CSPS se fixe des objectifs annuels, et tient des tableaux de bord liés au cadastrage des risques, aux sinistres et aux MSST, intégrés dans le rapport du CRM. Il collabore étroitement avec le Service de l'emploi et assurance-chômage (SECO), tout particulièrement lors des audits, ainsi qu'avec les instances cantonales :

- Les services de la Santé Publique (Vaud, Valais, Neuchâtel, Genève)
- Les services de l'environnement (Vaud, Valais, Neuchâtel, Genève)
- Les Etablissements d'assurance contre l'incendie (ECA-Vaud et ECA-Neuchâtel)
- Les polices cantonales (Vaud, Valais, Neuchâtel, Genève)
- La protection civile (PC).

Rôle et responsabilités

Le Délégué du DSPS de l'EPFL dirige le DSPS (Domaine sécurité, prévention et santé) en étant subordonné à la VPRHO. Les coordinateurs de sécurité en faculté et collège lui sont, soit directement, soit fonctionnellement rattachés. Il fait partie de la Cellule de crise et a la compétence de l'activer. Cette fonction fait partie intégrante de son cahier des charges.

Schéma d'organisation DSPS

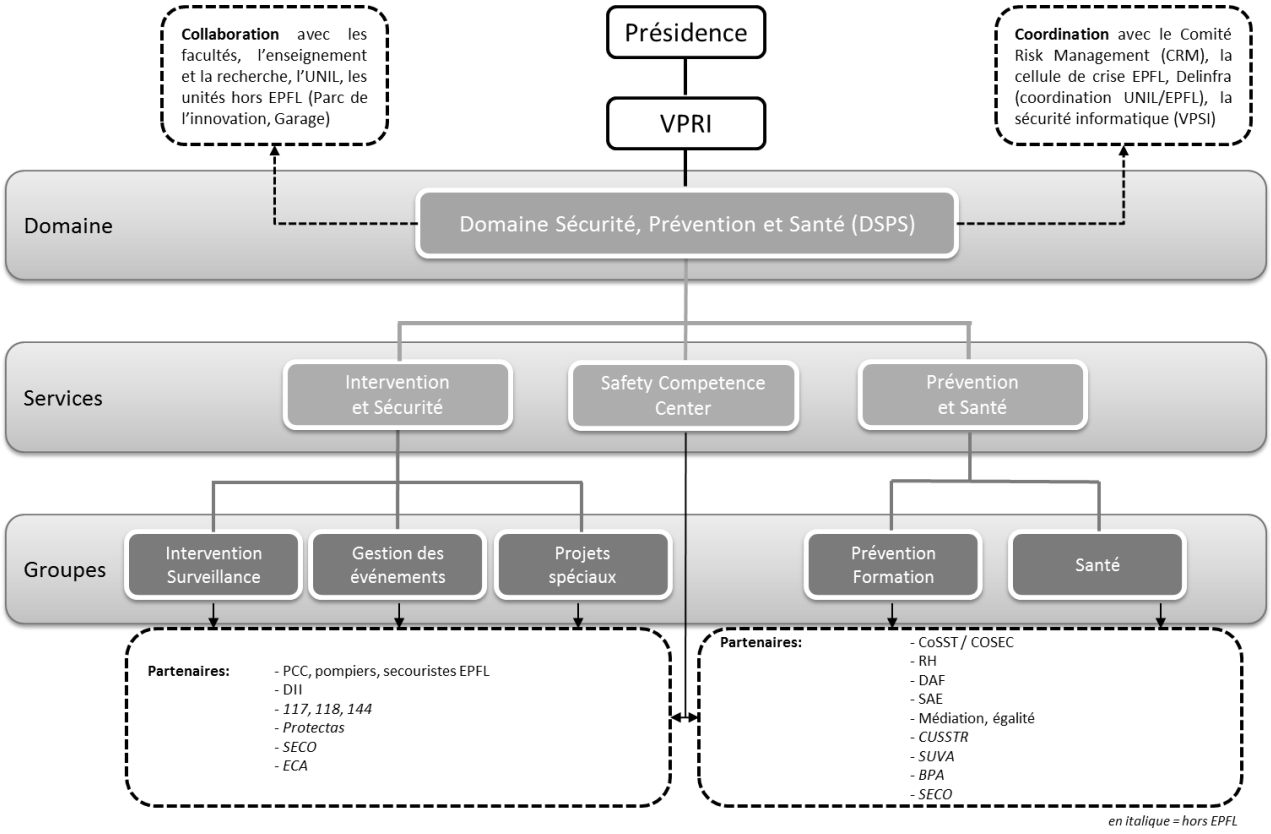

Figure 7 – Schéma d'organisation du DSPS

Comité Sécurité informatique (CSI)

Composition et rattachement

La sécurité informatique est une compétence du Vice-président pour les systèmes d'information, qui l'exerce par le biais d'un Comité de Sécurité Informatique.

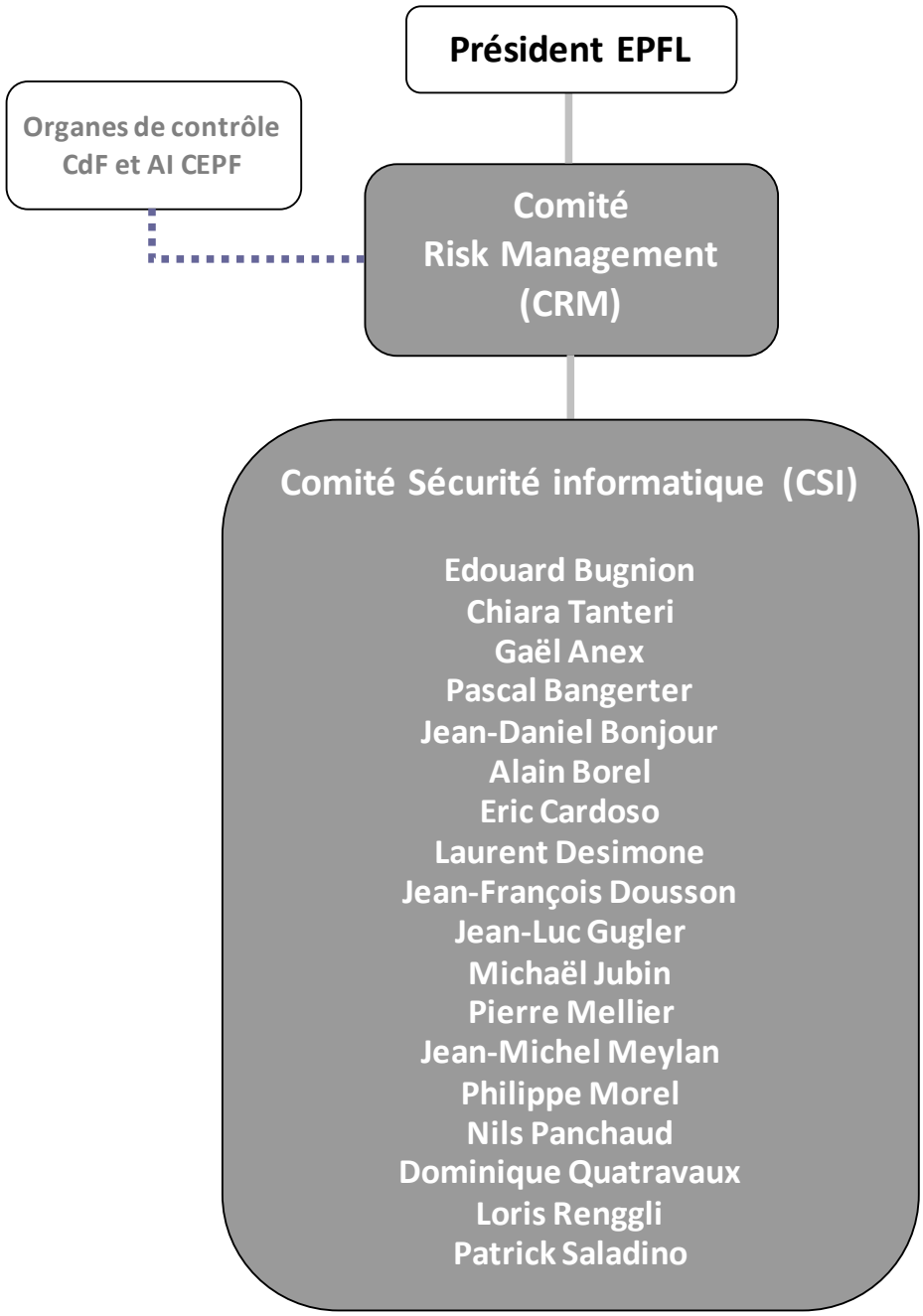

Figure 8 – Organisation du Comité Sécurité informatique

Missions du CSI

La mission principale du CSI est de développer et mettre en œuvre la politique de sécurité informatique de l'EPFL, ce qui se traduit par :

1. Etablir et maintenir à jour un inventaire des risques liés :
    a. à la sécurité informatique de l'EPFL,
    b. aux infrastructures et aux réseaux (data center),
    c. aux accès (firewall, sécurité d'accès, sécurité des données, archivage) ;
2. Suivre les mesures de mitigation de ces risques ;
3. Déployer un réseau de correspondants « sécurité informatique » via le rattachement fonctionnel IT (Heads of IT, Admin IT) dans l'ensemble des facultés et collèges ainsi que dans les antennes cantonales ;.
4. Agir de manière proactive dans la sensibilisation de l'ensemble des collaborateurs et étudiants dans le domaine de la sécurité informatique;
5. Mettre en place des métriques de suivi des actions de mise en conformité;
6. Collaborer avec d'autres groupes de l'Ecole actifs dans le domaine de la sécurité en général, notamment avec le DSPS pour la gestion de crise.

Rôles et responsabilités

La sécurité informatique est sous la responsabilité du Vice-président pour les systèmes d'information, qui préside le CSI.

Le CSI s'organise pour assurer les rôles et responsabilités suivants :

- Mettre en place un processus structuré et systématique de gestion des risques lié aux systèmes d'information ;
- Collaborer avec d'autres groupes actifs dans le domaine de la sécurité en général ;
- Rédiger le rapport annuel du CSI ;
- Préparer et participer aux séances mensuelles du CRM en ce qui concerne la sécurité informatique.

Compétences spécifiques

Le CSI est compétent pour :

- prendre toute décision relative à la sécurité informatique, tant physique que logique, des infrastructures de l'EPFL;
- émettre des directives en relation avec ladite sécurité;
- prendre également toute mesure visant à garantir l'intégrité physique des infrastructures, des personnes et des informations.

Rapports

Le CSI édite un rapport annuel, dont le contenu est intégré au rapport annuel du CRM.

Comité Assurances (CA)

Composition et rattachement

Le CA est subordonné à la Vice-présidence pour les finances. Il interagit directement avec le CRM dans le cadre de la politique d'assurances CEPF / EPFL.

Il se compose de la Vice-présidente pour les finances, du responsable du contrôle interne et gestion des risques et d'une juriste du service des Ressources Humaines.

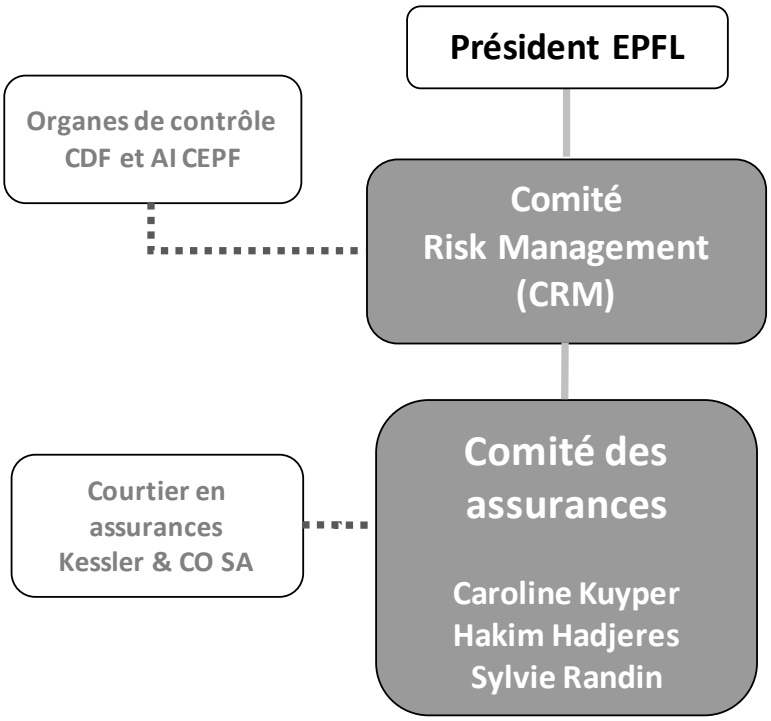

Figure 9 – Organisation du Comité Assurances (CA)

Missions, rôle et responsabilités

Le Comité des assurances :

1. participe au cadastrage des risques;
2. élabore le programme d'assurances de l'EPFL en coordination avec le CEPF;
3. gère les sinistres, notamment dans le domaine des risques non-assurés;
4. informe, conseille et soutient les unités ou les personnes en terme de couvertures d'assurances spécifiques.

Fonctionnement

Le CA se réunit au minimum une fois par année.

Rapports

Le Comité Assurances édite un rapport annuel, dont le contenu est intégré au rapport annuel du CRM. Celui-ci comprend la liste des polices ou contrats d'assurances ainsi que le tableau de la sinistralité EPFL.

Comité Résolution des litiges (CRL)

Composition

Le CRL est composé de la General Counsel ainsi que de juristes de l'EPFL et d'un support de coordination.

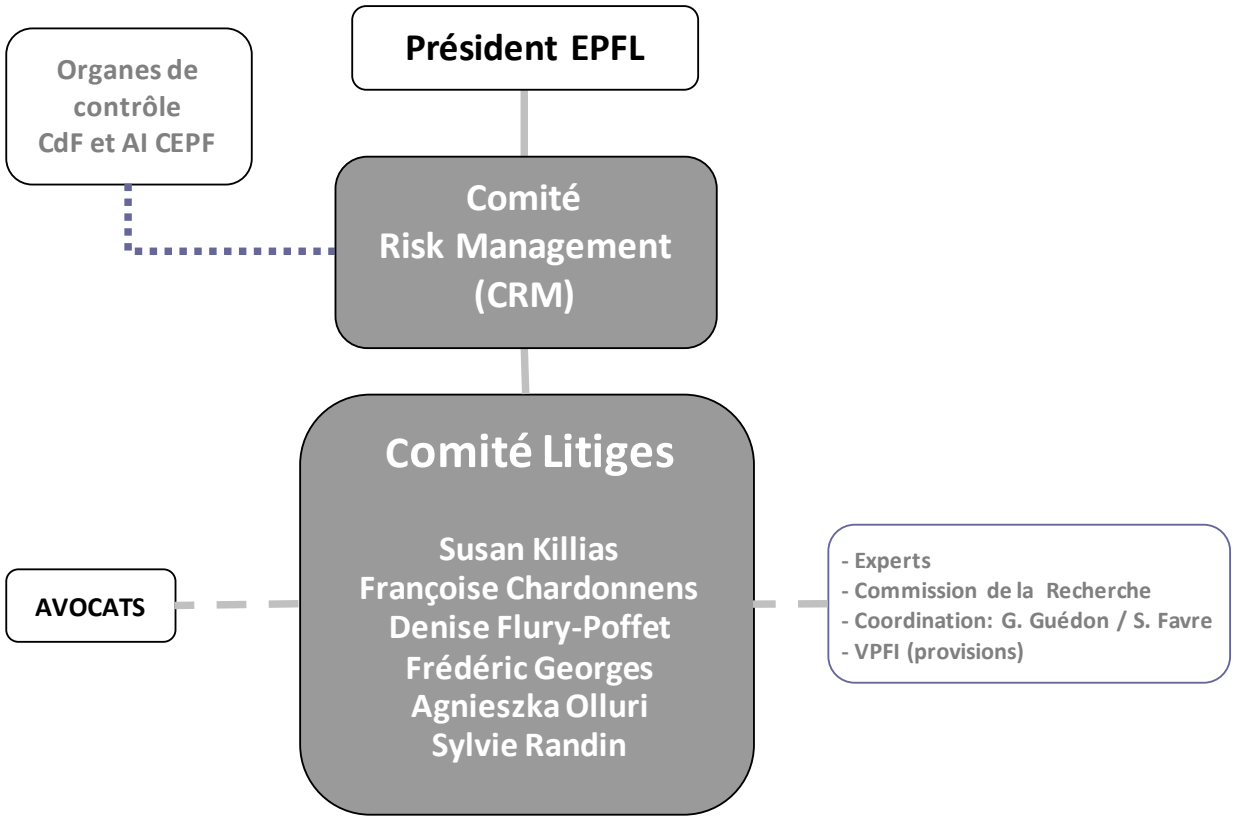

Figure 10 – Organisation du Comité Résolution des litiges (CRL)

Rôle

Le rôle du CRL consiste à :

- recenser les litiges de l'EPFL dans la base de données thémis ;
- superviser l'évolution des litiges ;
- chiffrer les provisions

Fonctionnement

Ce groupe se réunit trimestriellement selon un calendrier établi en début d'année. Il fonctionne selon le principe de la collégialité.

Système d'information

La base de données thémis est accessible uniquement aux personnes ayant un besoin légitime de la consulter.

Comité Système de contrôle interne (CSCI)

Le système de contrôle interne

Le système de contrôle interne de l'EPFL, (SCI)[4], se concentre sur les processus de gestion ayant une incidence sur les états financiers et assure la mise en place de contrôles clés garantissant un niveau de risque acceptable. Ce système permet d'assurer un déroulement conforme des opérations. Il est piloté par le Comité SCI.

Composition et rattachement du Comité SCI

Le Comité SCI est dirigé par le responsable du contrôle interne et gestion des risques. Il est composé des principaux responsables des processus du SCI. Le CSCI rapporte directement au CRM.

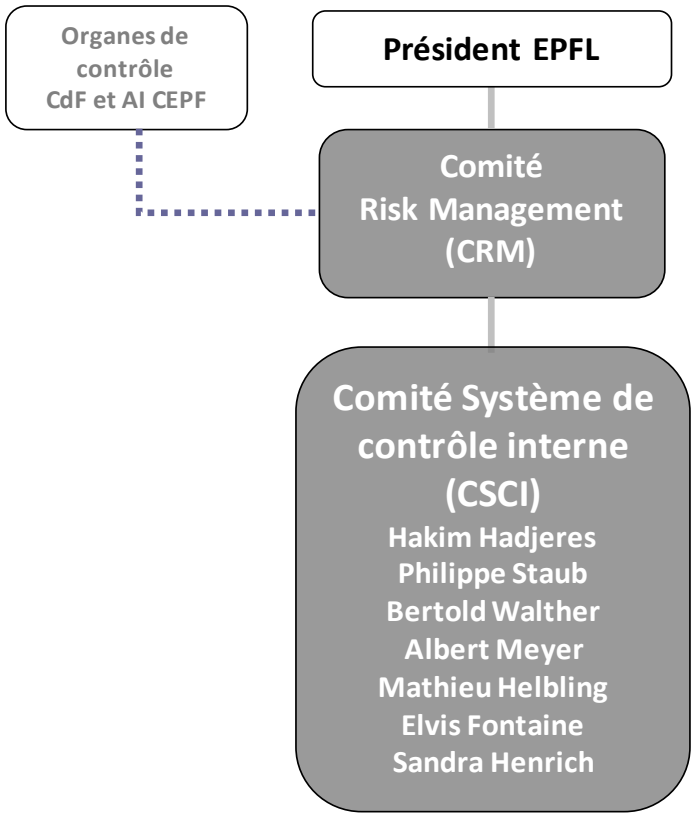

Figure 11 – Organisation du Comité Système de contrôle interne (CSCI)

Missions

Le CSCI a pour mission de :

1. piloter globalement la **mise en œuvre et la maintenance du SCI** à l'EPFL et notamment de vérifier que :
   - chaque processus ait un responsable,
   - l'analyse des risques et les contrôles clés soient bien effectués,
   - les boucles d'amélioration soient assurées,
   - la documentation des processus et des contrôles soit mise à jour,

[4] Voir la Directive sur le système de contrôle interne (SCI) à l'EPFL (LEX 1.7.1)

- les recommandations d'audit en matière de SCI soient suivies;

2. encourager l'identification des risques sur les processus financiers et leur traitement, selon une base documentaire cohérente et efficace, auprès de tous les collaborateurs des services administratifs concernés;
3. établir le programme annuel des travaux dans le domaine du SCI;
4. répondre au CRM de l'évolution du SCI.

Fonctionnement du Comité SCI

Le CSCI se réunit au minimum trimestriellement, selon un calendrier, en fonction de l'état d'avancement des travaux ou selon les besoins.

Il traite ponctuellement les cas de dysfonctionnement et propose des actions correctrices en coordination avec le CRM.

Le CSCI travaille sur la base d'un tableau de bord des activités maintenu à jour par son responsable. En outre il a pour tâche d'informer sur la qualité de l'environnement de contrôle, ainsi que de planifier les travaux et le calendrier de réalisation.

Rôle du responsable du Comité SCI

Le responsable du Comité SCI a pour tâche de :

1. vérifier que les contrôles clés soient effectués ;
2. produire le tableau de bord de suivi et le rapport d'activité;
3. coordonner et préparer les travaux de révisions du SCI avec les organes de contrôle dans le but d'obtenir une certification SCI sans réserve;
4. assurer la cohérence et conformité de la base documentaire et les standards du SCI;
5. informer régulièrement le CRM concernant l'avancement des travaux;
6. préparer le rapport d'activités du Comité SCI à inclure dans le rapport annuel du Comité Risk Management.

Rapports[5]

1. Le CSCI délivre un rapport d'activité annuel qui présente : les activités entreprises dans le cadre du SCI,
2. la liste des processus révisés,
3. la liste des nouvelles activités (sous-processus).

Ce rapport atteste des contrôles clés réalisés et fournit également un état des lieux des résultats obtenus, notamment en matière de plus-value pour l'EPFL. Son contenu est intégré au rapport annuel du CRM.

[5] Le référentiel du SCI de l'EPFL est le Coso. La norme d'audit applicable est la NAS 890.

Comité Coordination des audits (CCA)

Composition et rattachement

Le CCA est composé de la Vice-présidente pour les finances et du responsable du contrôle interne et gestion des risques.

Ce comité est rattaché fonctionnellement à la Vice-présidente pour les finances. Il rapporte sur une base mensuelle au CRM.

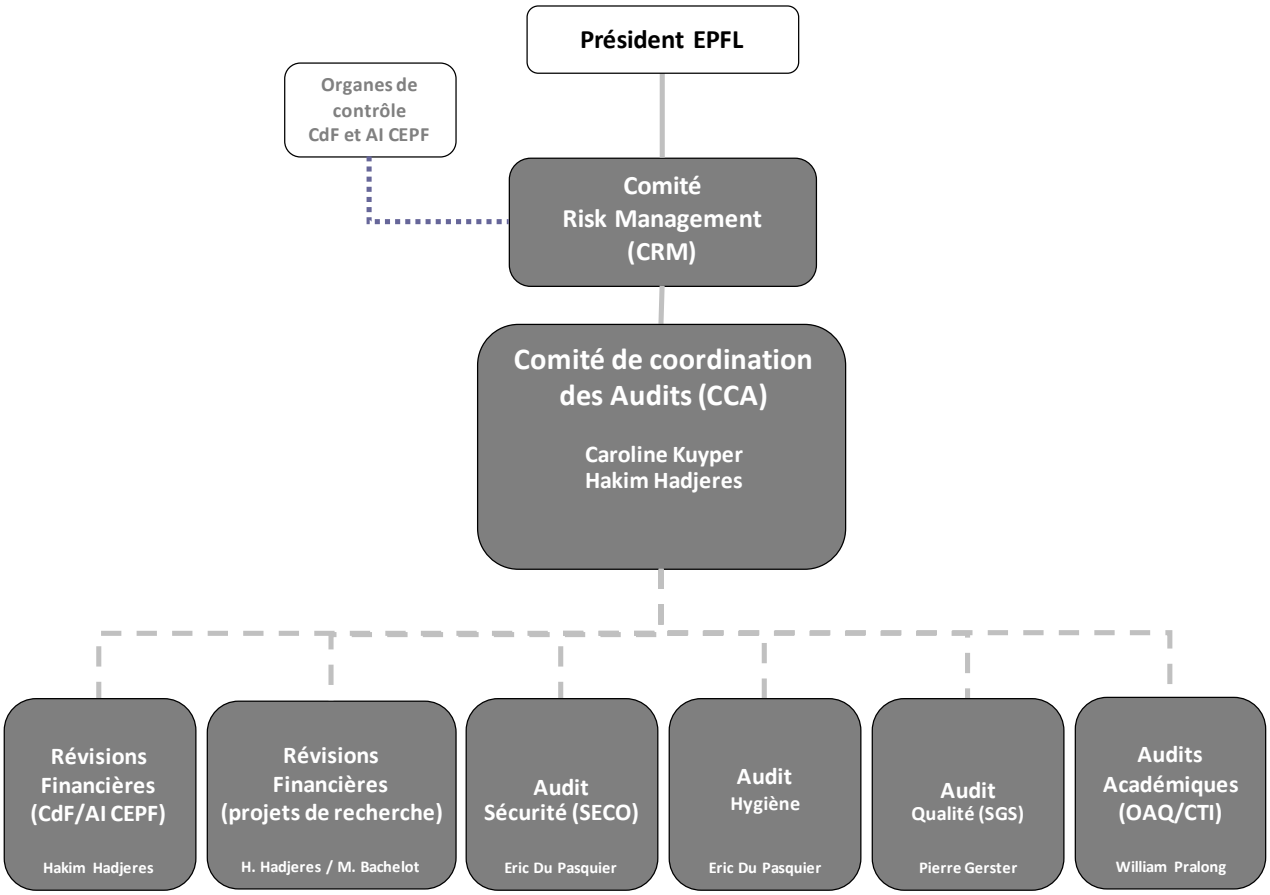

Figure 12 – Organisation du Comité Coordination des audits (CCA)

Missions

Le CCA a pour missions de :

1. suivre la planification et la réalisation de l'ensemble des audits à l'EPFL et d'en assurer le bon déroulement;
2. veiller à ce que les unités ou secteurs audités soient préparés et puissent répondre de manière professionnelle aux questions des auditeurs;
3. piloter le calendrier des principaux audits à l'EPFL;
4. assurer le suivi des recommandations d'audits;
5. rendre compte des résultats d'audits au CRM et à la Direction de l'EPFL.

Fonctionnement du Comité de coordination des audits

Le CCA se réunit en fonction de l'état d'avancement des audits.

Le CCA travaille sur la base d'un planning des audits et d'un tableau de suivi des activités maintenu par le coordinateur des audits à l'EPFL.

Le coordinateur des audits à l'EPFL est responsable de :

- mettre à jour et distribuer **le planning des audits annuels** et le tableau de suivi des recommandations par audit;
- préparer le rapport d'activités du CCA à inclure dans le rapport annuel du CRM.

Rôle des responsables d'audits thématiques

Chaque responsable d'audit thématique doit :

- communiquer le planning de ses audits au CCA;
- coordonner et préparer les travaux d'audits avec les organes mandatés;
- informer régulièrement le CRM concernant l'avancement des travaux;
- préparer le rapport d'activités pour le CCA qui l'inclura dans le rapport annuel du CRM.

Rapports

Le coordinateur des audits délivre :

1. un tableau de bord de suivi distribué trimestriellement aux membres du CRM contenant :
   - le calendrier des audits à jour,
   - le suivi des recommandations par audit,
   - un récapitulatif des actions en cours;
2. un rapport d'activité annuel qui présente :
   - la liste d'audits réalisés par année,
   - les actions terminées et les suspens.

Son contenu est intégré au rapport annuel du CRM.