Risk Management Regulations at EPFL

LEX 1.4.3

Version 1.0 was approved by the Direction on 22nd June 2009 and by the Deans' Conference on 6th July 2009.

Version 2.0 was approved by the Direction on 30th May 2011. Version 2.30 status as at 3rd September 2018.

Version 2.4 was approved by circular on 8th March 2021.

Contents

Introduction 3
Legal bases 3
Purpose 3
Scope of EPFL Risk Management 3

Organisation of Risk Management at EPFL 5
Risk Management Committee (CRM) 5
Security and exploitation committee (CSE) 11
Insurance Committee (CA) 15
Dispute Settlement Committee (CRL) 16
Audit Coordination Committee (CCA) 19

Introduction

Legal bases

The EPFL Direction,

based on the *Directive du Conseil des EPF concernant la gestion des risques des EPF et des établissements de recherche* of 4th July 2006, status as at 16th May 2018, and

based on the Ordinance on the Organisation of the Ecole polytechnique fédérale de Lausanne of 1st March 2004, status as at 17th December 2020,

hereby adopts the following:

Purpose

These Regulations define how Risk Management (RM) is organised within the Ecole polytechnique fédérale de Lausanne (EPFL), as well as the organisation and decision-making powers of the Risk Management Committee (CRM) and other committees reporting to the latter.[1]

Scope of EPFL Risk Management

The scope of risk management includes EPFL and its (non-exhaustive) extended scope, i.e.:

EPFL Scope

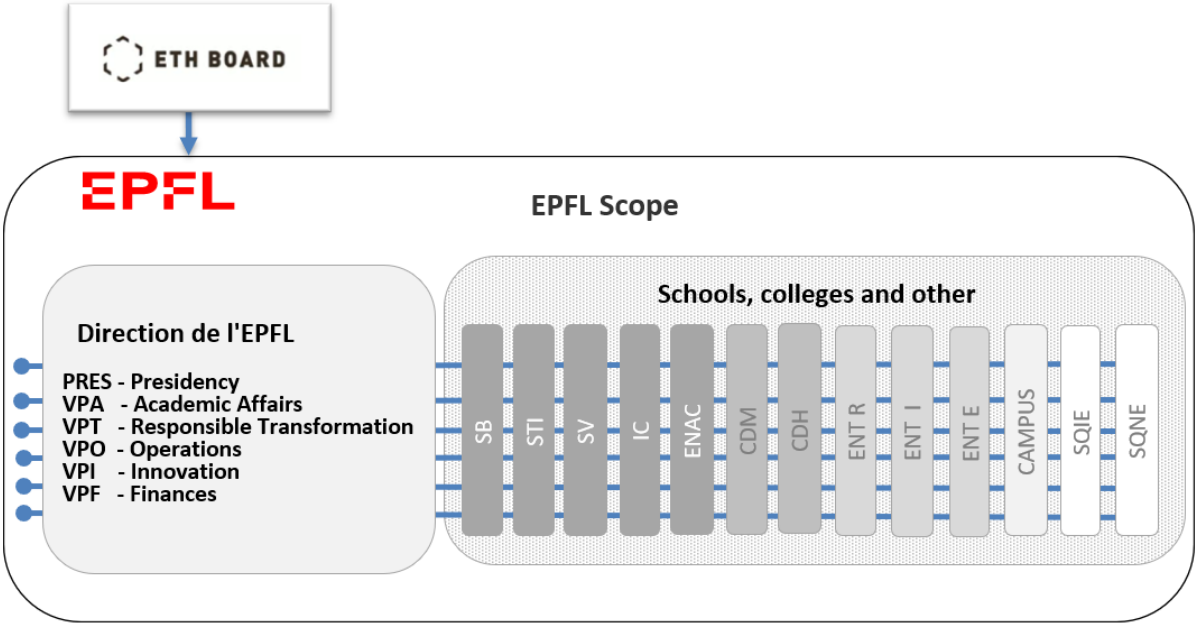

Figure 1 – Scope of EPFL Risk Management

[1] The applicable control frameworks are COSO and COBIT.

COSO = The COSO is a framework of internal controls defined by the Committee of Sponsoring Organizations of the Treadway Commission.

COBIT = The CoBIT (Control Objectives for Information and Related Technology) is a federating tool that establishes a common language for information system governance, while attempting to integrate other reference systems such as ISO 9000, ITIL.

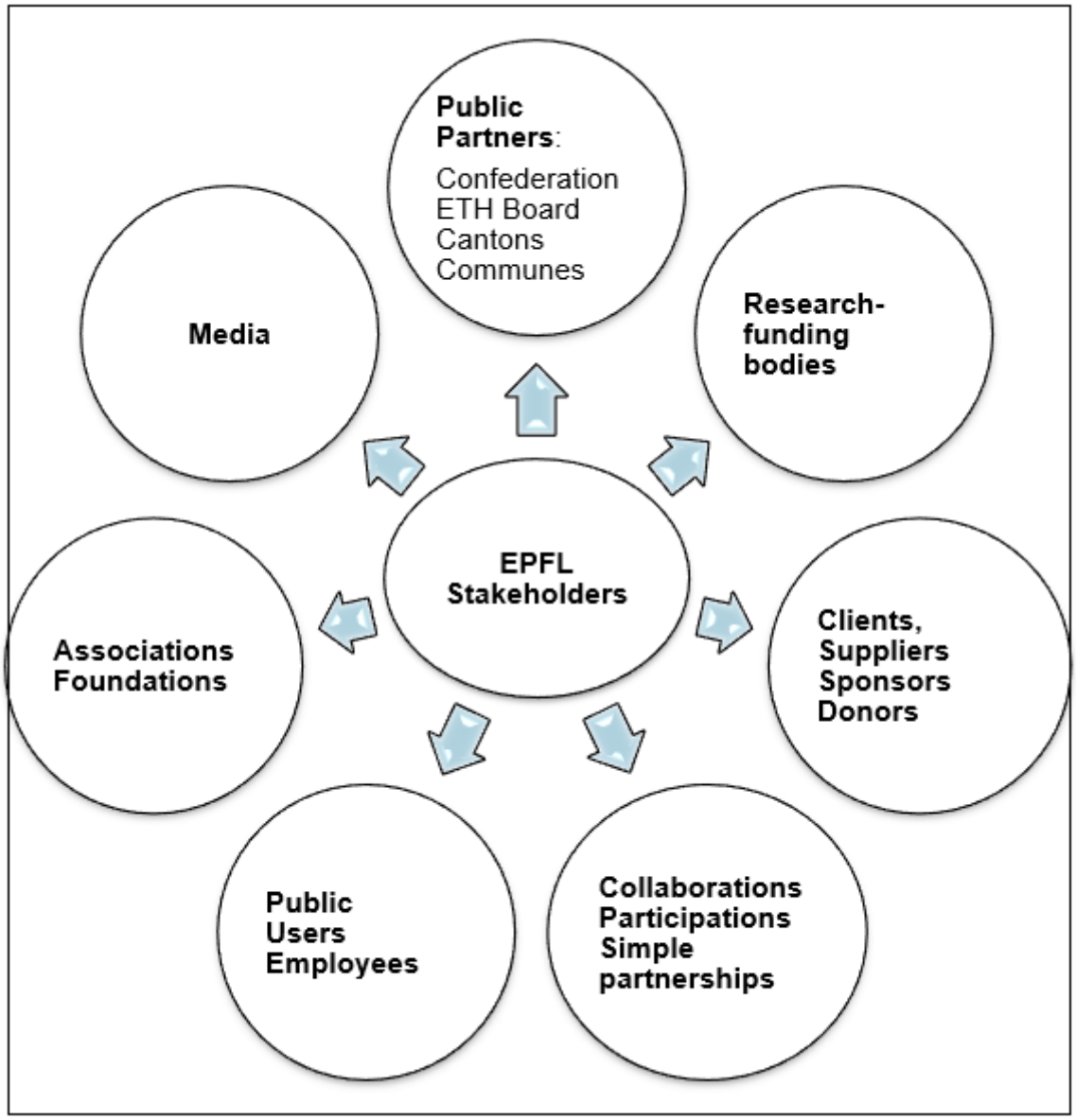

Figure 2 – EPFL Extended Scope

Organisation of Risk Management at EPFL

Risk Management Committee (CRM)

Members and Reporting

The reduced CRM is made up of a President and six members.

The extended CRM is made up of the members of the limited committee, plus the Vice President for Academic Affairs and the Vice President for Operations.

Status within the CRM	EPFL role
President	Vice President for Finances
Reduced committee member	Director of the department of Security, Safety and Facilities Operations
Reduced committee member	Director of Legal Affairs
Reduced committee member	Head of Internal Controls and Risk Management
Reduced committee member	Data Protection Officer
Reduced committee member	Director of Information Systems
Reduced committee member	Director of Human Resources
Extended committee member	Vice President for Academic Affairs
Extended committee member	Vice President for Operations

The Committee reports directly to the President of EPFL via the Vice President for Finances.

The CRM coordinates the work of the six committees reporting to it as shown in the diagram below.

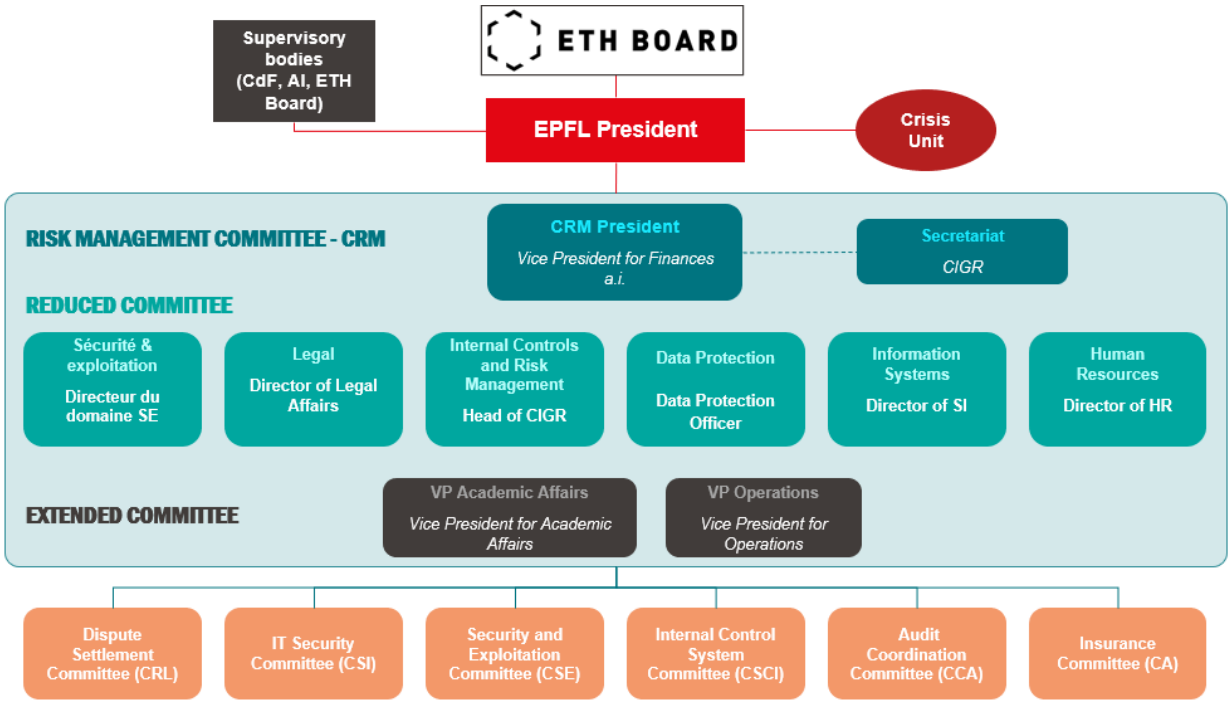

Figure 3 – Organisation of the CRM and Related Committees

Risk Domains and Persons in Charge

Using risk assessments carried out by the persons in charge of the domains defined below, the CRM creates a catalogue of risks at EPFL. The list of domains is given below:

Presidency
MEDIACOM
International Affairs
Philanthropy
General Secretary
Legal Affairs
Quality assurance and accreditation
Vice Presidency for Academic Affairs
Associate Vice Presidency for Postgraduate Education
Associate Vice Presidency for Student Affairs and Outreach
Associate Vice Presidency for Education
Associate Vice Presidency for Research
Associate Vice Presidency for Centers and Platforms
Basic Sciences
Computer and Communication Sciences
Architecture, Civil and Environmental Engineering
Life Sciences
Engineering (inc. NE outpost)
College of Management of Technology
College des Humanities
Vice Presidency for Responsible Transformation
Inclusion and diversity
Sustainability
Vice Presidency for Innovation
SQNE
SQIE
Vice Presidency for Operations
Development & Construction
Safety, Security & Operations
Human Resources
Information Systems

Procurement
Wallis Campus
Fribourg Campus
Neuchâtel Campus / Microcity
Geneva Campus / Biotech Campus
Middle East Campus
Vice Presidency for Finances
Controlling
Accounting
Planning, Treasury and Institutional Data
Internal Control and Risk Management
Program Management Office

Missions of the CRM

The CRM has the following missions:

1. to implement **risk management policy** at EPFL in accordance with the ETH Board Directive on Risk Management;
2. to develop **a system of organisation and procedures** to ensure legal compliance;
3. to guarantee **the identification of risks** and suggest the implementation of appropriate measures for reducing them to an acceptable level;
4. to ensure, via the Vice President for Finances, that **risk owners** manage their risks, inform the CRM of the latter and **regularly upgrade mitigation actions**;
5. to supervise using the **insurance portfolio** and adapt it as necessary;
6. to support **individual actions and initiatives** aimed at improving risk and opportunity management at EPFL;
7. to **report to the President** and to the EPFL Direction regularly and on an annual basis on the status and progress of issues related to risk management.

CRM members are bound by a duty of confidentiality. The CRM may take all necessary measures to fulfil its mandate, in particular provisional measures.

CRM Operation and Reporting

The CRM meets a minimum of once a month. An agenda and minutes are drawn up and distributed. This event is generally preceded by a meeting with the IT Security Committee.

The CRM issues an **annual report** for the EPFL President and EPFL Direction. This report presents the activities of the CRM and all related groups and committees, as well as general recommendations. The report is approved by the President. Its content is available to the internal auditors of the ETH Board (CEPF) and the external auditors of the Swiss Federal Audit Office (CdF).

Further reports may be submitted to the President and EPFL Direction on sensitive or specific issues.

Reporting Obligations / Information

The CRM shall notify:

Whom	***Subjects***
The ETH Board	Of any case potentially detrimental to the image or reputation of EPFL, following a proposal by the Director of Legal Affairs or the President of the CRM and subject to validation by the EPFL President – pursuant to the ETH Board *Directive sur le devoir d'information* of 5th July 2017 (LEX 1.8.0.2*)*.
The EPFL President and Direction	Via an annual report. On an ad hoc basis when circumstances so require.
The Heads of Units, the Vice Presidents, School Deans and College Directors	Of best practice regarding risk management. Of their reporting obligations concerning risks, especially those relating to hazards and projects. Of developments in risk management at EPFL.
The Head of Communications	Of any sensitive files on an ad hoc basis. Of any subject relating to the EPFL image.

Risk Registers

At least once per year in June, the CRM reviews the development of risk analyses obtained from the various databases.

Domain	***Register***
EPFL Direction, Central Services, Schools and Colleges	Register of strategic & operational risks
Safety, Prevention & Health	Hazard survey
Audits	Audit register and planning of audits and points in abeyance
ICS	Register of financial risks and key controls
Insurance	Insurance scheme and table of claims
Information System	Register of IT security risks

Crisis Management

The EPFL President heads the Direction Crisis Unit when a major event affects the safety and security of persons, IT or buildings. In his absence, the substitutes are the Vice President for Academic Affairs then the Vice President for Operations, in that order.

The crisis report defines the Crisis Unit's operating mode. The report is kept up-to-date by the Safety, Prevention and Health Domain.

In the field of IT security, the IT Crisis Unit is integrated with the Direction Crisis Unit; the IT security crisis report is kept by the Head of IT Security.

Data protection and storage

The Federal Act on Data Protection applies to all cases dealt with. All dossiers, documents and electronic files are kept and archived (archives > 50 years).[2]

[2] *Loi fédérale sur l'archivage (LAr)* of 26th June 1998 (RS 152.1)

Security and exploitation committee (CSE)

Members and reporting

The CSE is made up of the Director of the department of Security, Safety and Facilities Operations and four other members. It reports directly to the CRM.

Status within the CSE	EPFL role
President	Director of the department of Security, Safety and Facilities Operations
Member	Head of the Safety, Prevention and Health service
Member	Head of the Occupational Health and Safety service
Member	Head of the Facilities Operations service
Member	Occupational Health Specialist

Missions of the Committee

In close cooperation with the department of Security, Safety and Facilities Operations, the CSE develops and implements the EPFL's safety and health policy. It coordinates the planning of safety actions and controls specific to each EPFL School, College and outpost.

In particular, the CSE ensures:

- the development and training of the network of Safety Delegates (COSECs);
- a survey of hazards and follow-up of hazard mitigation actions;
- training of all staff members in the field of prevention of dangers at EPFL;
- reporting and follow-up of compliance measures;
- cooperation and exchange of experience with various safety networks in academia as well as with the public and private sectors.

Operation of the Committee

The CSE sets annual objectives and keeps dashboards on hazard surveys, incidents and occupational health and safety measures to be integrated into the CRM report. The CSPS works closely with the employment service and unemployment insurance of the State Secretariat for Economic Affairs (SECO), particularly during audits, as well as with cantonal authorities:

- Public health services (Vaud, Valais, Neuchâtel, Geneva)
- Environmental services (Vaud, Valais, Neuchâtel, Geneva)
- Fire insurance (ECA-Vaud and ECA-Neuchâtel)
- Cantonal police (Vaud, Valais, Neuchâtel, Geneva)
- Civil Protection (PC).

Role and responsibilities

The Director of the department of Security, Safety and Facilities Operations directs the department and reports to the Vice Presidency for Operations (VPO). The School and College Safety Coordinators report to the Director either directly or operationally. He/She is part of the Crisis Unit and is competent to initiate the latter. This task is an integral part of his/her terms of reference. He/She represents EPFL before official bodies and in particular for the filing of complaints, of which he/she also notifies the Director of Legal Affairs.

IT Security Committee (CSI)

Members and reporting

IT Security is the responsibility of the Vice President for Operations, who exercises this responsibility through an IT Security Committee.

The CSO is made up of the EPFL Director of the department of Information Systems (DSI), who acts as the committee President, the head of IT Security, who pilots the meetings, and the members listed below.

Status within the CSI	EPFL Role
President	Director of the department of Information Systems (DSI)
Pilot	Head of IT Security
Member	Data Protection Officer
Member	Head of the IT Operations Service
Member	Head of the SI Governance Service
Member	Head of the Engineering and Development Service
Member	School IT Managers
Member	Representative for the Technical Supervision of Infrastructures
Member	Representative for Infrastructure Safety
Member	Members of the IT Security team, appointed by the DSI
Member	Head of Telecommunications
Member	Director of High Performance Computing
Participant by invitation	Director of SISB

Missions of the CSI

The main mission of the CSI is to develop and implement the EPFL IT security policy, and in particular to:

1. Establish and keep up-to-date an inventory or risks related to
    a. EPFL IT security,
    b. infrastructure and networks (data center)
    c. access (firewall, access security, data security, archiving);
2. Monitor the mitigation measures for such risks;
3. Deploy a network of IT security Delegates via the IT functional reporting line (Heads of IT, IT Admin.) in all Schools and Colleges as well as in the cantonal antenna;

4. Proactively raise awareness to IT security among all staff members and students;
5. Implement metrics to follow up compliance measures;
6. Cooperate with other EPFL groups engaged in the field of general security, in particular with the Direction of the department of Security, Safety and Facilities Operations on crisis management.

Roles and responsibilities

IT security and the CSI are the responsibility of the Direction of Information Systems, which reports to the Vice President for Operations.

The CSI organises its activities so as to assume the following roles and responsibilities:

- Implement a structured and systematic process for IT security risk management linked to Information Systems;
- Cooperate with other groups engaged in the field of general security;
- Draw up the CSI annual report;
- Prepare and participate in the monthly meetings of the CRM regarding IT security.

Specific powers

The CSI has authority to:

- make any decision relating to the IT security - both physical and logical - of EPFL infrastructure;
- issue directives relating to said security;
- take any additional measure to guarantee the physical integrity of infrastructures, people and information.

Reports

The CSI issues an annual report, the content of which is integrated into the CRM annual report.

Insurance Committee (CA)

Members and reporting

The CA reports to the Vice Presidency for Finances. It interacts directly with the CRM in the framework of the ETH Board/EPFL insurance policy.

The CA is made up of the Vice President for Finances and the Head of Internal Controls and Risk Management service.

Status within the CA	EPFL role
President	Vice President for Finances
Member	Head of the CIGR service
Participant by invitation	Insurance broker

Missions, role and responsibilities

The Insurance Committee:

1. contributes to the survey of hazards;
2. develops the EPFL insurance scheme in coordination with the ETH Board;
3. manages hazards, in particular in the field of non-insured risks;
4. informs, advises and supports units or individuals regarding specific insurance coverage.

Operation

The CA meets a minimum of once per year.

Reports

The Insurance Committee issues an annual report whose content is integrated into the CRM annual report. The CA report includes the list of insurance policies and contracts as well as a table of EPFL claims.

Dispute Settlement Committee (CRL)

Members

The CRL is made up of the Director of Legal Affairs and EPFL legal counsels. The CRL also receives support from internal and external experts (lawyers).

Status within the CRL	EPFL role
Coordinator	Director of Legal Affairs
Member	Senior Legal Counsel, Student Affairs and Outreach
Member	Senior Legal Counsel, Student Affairs and Outreach
Member	Senior Legal Counsel, Direction of Human Resources
Member	Senior Legal Counsel, Direction of Human Resources

Role

The role of the CRL is to:

- Record disputes in the Themis database;
- Supervise the development of disputes;
- Determine dispute provisions.

Operation

This group meets quarterly in accordance with a schedule set out at the beginning of the year. The group operates as a collegial body.

Information System

The Themis database is accessible uniquely to those persons who legitimately need to consult it.

Internal Control System Committee (CSCI)

Internal Control System

The EPFL internal control system (ICS[3]) focuses on management processes with a financial impact and ensures the implementation of key controls to guarantee an acceptable risk level. This system serves to guarantee that operations are carried out in accordance with existing rules and regulations. The system is managed by the ICS Committee.

Members and reporting

The CSCI is piloted by a representative for the Internal Controls and Risk Management service. It is made up of the main ICS process managers. The CSCI reports directly to the CRM.

Status within the CSCI	EPFL role
Coordinator	ICS and Risk Manager
Member	Head of Accounting
Member	Head of Salaries and Pensions
Member	Director of the department of Procurement
Member	Head of Finance Projects and Accounting Consolidation
Member	Support and controlling PMO-SC

Missions

The CSCI has the following missions:

1. to oversee the overall **implementation and maintenance of the ICS** at EPFL and, in particular, ensure that:
   - each process has a manager,
   - risk analysis and key controls are duly performed,
   - improvement cycles are ensured,
   - the documentation for processes and controls is kept up-to-date,
   - auditing recommendations on ICS are acted on;
2. to encourage the identification and mitigation of risks in financial processes by all administrative employees concerned, according to a coherent and effective documentary base;
3. to draw up the annual work programme in the ICS field;
4. to report ICS developments to the CRM.

Operation of the CSCI

The CSCI meets at least quarterly, according to a schedule, depending on the progress of work or as needed.

[3] See the Directive on the Internal Control System (ICS) at EPFL (LEX 1.7.1)

It deals with instances of malfunction on an ad hoc basis and proposes corrective actions in coordination with the CRM.

The CSCI works based on a dashboard of activities kept by the CSCI Head.

In addition, the CSCI must provide information regarding the quality of the control environment and plan any related work and the schedule for its completion.

Role of the Head of the CSCI

The Head of the **CSCI** has the following tasks:

1. to check that key controls are performed;
2. produce the monitoring dashboard and activity report;
3. coordinate and prepare ICS auditing work with the supervisory bodies in order to obtain unqualified ICS certification;
4. ensure the coherence and conformity of the ICS documentary base and standards;
5. regularly inform the CRM about work progress;
6. prepare the CSCI activity report to be included in the annual report of the Risk Management Committee.

Reports[4]

The CSCI issues **an annual activity report** setting out:

1. the activities undertaken within the ICS framework,
2. the list of revised processes,
3. the list of new activities (sub-processes).

This report provides evidence of key controls performed and an overview of the results obtained, particularly in terms of added value for EPFL. Its content is integrated into the CRM annual report.

[4] The framework for the EPFL ICS is COSO. The applicable auditing standard is NAS 890.

Audit Coordination Committee (CCA)

Members and reporting

The CCA is made up of the Vice President for Finances and the Head of Internal Controls and Risk Management service. It reports to the CRM on a monthly basis.

Status within the CCA	EPFL role
President	Vice President for Finances
Member	Head of the CIGR service

Missions

The **CCA** has the following missions:

1. to monitor the planning and implementation of all audits at EPFL and ensure their smooth operation;
2. to ensure that audited units or sectors are prepared and able to respond professionally to any questions from the auditors;
3. to control the schedule of major audits at EPFL;
4. to ensure follow-up of audit recommendations;
5. to report audit findings to the CRM and the EPFL Direction.

Scope

The CCA ensures the accomplishment of audits and their results via the various managers of the following domains:

- financial previsions (CdF / AI ETH Board);
- financial previsions (research projects);
- security audits (SECO);
- safety audits;
- quality audits;
- academic audits.

Operation of the Audit Coordination Committee

The CCA meets depending on the progress of audits.

The CCA works on the basis of a schedule of audits and an activity monitoring table maintained by the EPFL Audit Coordinator.

The EPFL Audit Coordinator is in charge of:

- updating and distributing the **annual audit schedule** and the audit recommendation follow-up table;
- preparing the CCA activity report to be included in the annual CRM report.

Role of Thematic Audit Heads

Each Thematic Audit Head shall:

- notify their audit schedule to the CCA;
- coordinate and prepare auditing work with the auditing bodies;

- regularly inform the CRM about work progress;
- prepare an activity report for the CCA; the CCA will include this report in the CRM annual report.

Reports

The Audit Coordinator issues:

1. a monitoring dashboard distributed quarterly to CRM members, including:
   - an up-to-date schedule of audits,
   - a follow-up of audit recommendations by audit,
   - a summary of ongoing actions;
2. an annual activity report setting out:
   - the list of audits conducted per year,
   - actions completed and pending.

Its content is integrated into the CRM annual report.