Risk Management Regulations at EPFL
LEX 1.4.3

Version 1.0 was approved by the Direction on 22 June 2009 and by the Deans’ Conference on 6 July 2009.
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
Safety, Prevention & Health Committee (CSPS) ........................................................................ 111
IT Security Committee (CSI) ....................................................................................................... 144
Insurance Committee (CA) ......................................................................................................... 166
Internal Control System Committee (CSCI) ............................................................................... 177
Audit Coordination Committee (CCA) ...................................................................................... 211

List of Figures

Figure 1 – Scope of EPFL Risk Management ............................................................................. 3
Figure 2 – Diagram of EPFL Cantonal Outposts ........................................................................ 4
Figure 3 – EPFL Extended Scope ................................................................................................ 4
Figure 4 – Organisation of the CRM and Related Committees .................................................... 5
Figure 5 – Risk Domains and Persons in Charge ....................................................................... 6
Figure 6 – Organisation of the Safety, Prevention & Health Committee (CSPS) ......................... 111
Figure 7 – DSPS Organisation Chart .......................................................................................... 133
Figure 8 – Organisation of the IT Security Committee (CSI) ...................................................... 144
Figure 9 – Organisation of the Insurance Committee (CA) ......................................................... 166
Figure 10 – Organisation of the Internal Control System Committee (CSCI) ............................. 177
Figure 11 – Organisation of the Audit Coordination Committee (CCA) ..................................... 211
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 4 July 2006 and
on the Ordinance on the Organisation of the Ecole polytechnique fédérale de Lausanne of 1 March 2004, status as of 1 January 2017,
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. The initial framework called COSO 1 has evolved since 2002 toward a second version called COSO 2.

COBIT = The CoBIT (Control Objectives for Information and Related Technology) is a federating tool that allows to establish a common language for information system governance, while attempting to integrate other reference systems such as ISO 9000, ITIL.
Figure 2 – Diagram of EPFL Cantonal Outposts

Figure 3 – EPFL Extended Scope
Organisation of Risk Management at EPFL

Risk Management Committee (CRM)

Members and Reporting
The CRM is made up of four members:
The General Counsel, the Vice President for Finances, the Safety Delegate and the Head of Management Control.
The CRM is advised by three representatives from the educational field, whose task is to provide academic expertise, in particular in the context of risk analysis for strategic projects, Schools and Colleges.
The Committee reports directly to the President of EPFL via the General Counsel.

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

Figure 4 – Organisation of the CRM and Related Committees
Risk Domains and Persons in Charge

The CRM analyses the risks for all EPFL domains. The list of persons in charge of the various domains is given below:

**EPFL Direction**

- **Presidency**
  - Martin Vetterli

- **Vice Presidencies**
  - **VPE**
    - Academic Affairs
    - Pierre Vanderheyst
  - **VPR**
    - Research
    - Andreas Mortensen
  - **VPI**
    - Innovation
    - Marc Gruber
  - **VPRHO**
    - Human resources and operations
    - Etienne Marclay
  - **VPFI**
    - Finances
    - Caroline Kuyper
  - **VPSI**
    - Information systems
    - Edouard Bugnon

**Schools, Colleges & Other**

- **Schools**
  - **SB**
    - Basic Sciences
    - Pierre Vanderheyst & Andreas Mortensen
    - Thomas Rizzo
  - **STI**
    - Engineering
    - Pierre Vanderheyst & Andreas Mortensen
  - **ENAC**
    - Architecture, Civil and Environmental Engineering
    - Marlyne Andersen
  - **I&C**
    - Computer and Communication Sciences
    - Jaroslav Larus
  - **SV**
    - Life Sciences
    - Gisou van der Goot

- **Colleges**
  - **CDH**
    - College of Humanities
    - Thomas David
  - **CDM**
    - Management of Technology
    - Christopher Tucci
  - **EPFL ME**
    - EPFL Middle East
    - Franco Vignoli

**Figure 5 – Risk Domains and Persons in Charge**
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 **an organisation and procedures** in order to ensure legal compliance;
3. to guarantee **the identification of risks** and implementation of appropriate measures to reduce them to an acceptable level;
4. to ensure, via the CFO, that **risk owners** manage their risks, inform the CRM of the latter and **regularly upgrade mitigation actions**;
5. to supervise, via a staff member yet to be defined the **insurance scheme** and adapt it as necessary;
6. to encourage **individual actions and initiatives** aimed at improving risk and opportunity management at EPFL;
7. to **report to the President** and to the EPFL Direction on an annual basis and regularly 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, including precautionary measures.

CRM Members

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
<th>Domains</th>
<th>Reporting to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Susan Killias</td>
<td>General Counsel</td>
<td>Legal</td>
<td>P-GEC</td>
</tr>
<tr>
<td>Caroline Kuyper</td>
<td>Vice President</td>
<td>Finances</td>
<td>FI</td>
</tr>
<tr>
<td>Marc Chambaz</td>
<td>Head, Management Control</td>
<td>Audit</td>
<td>P-GEC</td>
</tr>
<tr>
<td>Eric Du Pasquier</td>
<td>Safety Delegate</td>
<td>Health/Safety/Prevention</td>
<td>RHO</td>
</tr>
<tr>
<td>TBN</td>
<td>TBD</td>
<td>Insurance</td>
<td>TBD</td>
</tr>
</tbody>
</table>

Academic Experts

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
<th>Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>Andreas Mortensen</td>
<td>Vice President R</td>
<td>Strategic risks – Research</td>
</tr>
<tr>
<td>Pierre Vandergheynst</td>
<td>Vice President E</td>
<td>Strategic risks - Education</td>
</tr>
<tr>
<td>Edouard Bugnion</td>
<td>Vice President SI</td>
<td>Strategic risks - Computing</td>
</tr>
</tbody>
</table>

CRM Operation and Reporting

The CRM meets once a week. An agenda and minutes are drawn up and distributed.

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, the list of cases dealt with in the course of the year, 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).

---

2 Note: additional experts may be invited by the CRM as necessary
Further reports may be submitted to the President and EPFL Direction on sensitive or specific issues.
Reporting Obligations
The CRM shall notify:

<table>
<thead>
<tr>
<th>Whom</th>
<th>Subjects</th>
</tr>
</thead>
<tbody>
<tr>
<td>The ETH Board</td>
<td>Of any case potentially detrimental to the image or reputation of EPFL, following a proposal by the General Counsel and subject to validation by the EPFL President – pursuant to the relevant ETH Board Directive sur le devoir d’annoncer of 14 September 2001 (LEX 1.8.2).</td>
</tr>
<tr>
<td>The EPFL President and Direction</td>
<td>On the basis of an annual report. On an ad hoc basis when circumstances so require.</td>
</tr>
<tr>
<td>The Head of Communications</td>
<td>Of any sensitive issue on an ad hoc basis. Of any subject relating to the EPFL image.</td>
</tr>
<tr>
<td>The Unit Heads</td>
<td>Of best practice with regard to risk management. Of their reporting obligations concerning risks, especially those relating to hazards (fire, flood, etc.) and projects. Of developments in the area of risk management at EPFL.</td>
</tr>
</tbody>
</table>

Risk Registers
At least once per year in June the CRM reviews the development of risk analyses obtained from the various databases.³

<table>
<thead>
<tr>
<th>Domain</th>
<th>Register</th>
<th>Administrator</th>
<th>Database</th>
</tr>
</thead>
<tbody>
<tr>
<td>EPFL Direction, Central Services, Schools and Colleges</td>
<td>Register of strategic &amp; operational risks</td>
<td>Marc Chambaz</td>
<td>Excel</td>
</tr>
<tr>
<td>Safety, Prevention &amp; Health</td>
<td>Hazard survey</td>
<td>Eric Du Pasquier</td>
<td>SAP – EHS</td>
</tr>
<tr>
<td>Audits</td>
<td>Audit register and planning of audits and points in abeyance</td>
<td>Marc Chambaz</td>
<td>Excel</td>
</tr>
<tr>
<td>ICS</td>
<td>Register of financial risks and key controls</td>
<td>Caroline Kuyper, Philippe Staub</td>
<td>Excel</td>
</tr>
<tr>
<td>Insurance</td>
<td>Insurance scheme and table of claims</td>
<td>TBN</td>
<td>Excel</td>
</tr>
<tr>
<td>Information System</td>
<td>Register of IT security risks</td>
<td>Edouard Bugnion</td>
<td>Excel</td>
</tr>
</tbody>
</table>

³ The information managed by the CRM originates from several databases not integrated to date.
Crisis Management
The 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 Research and the Vice President for Human Resources and 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 (DSPS).

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.

Logistical support to the CRM
In fulfilling its missions the CRM is supported by a coordinator to guarantee the confidentiality and security of (paper-based) information and manage access rights to the various databases and documents.

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).4

---

4 Loi fédérale sur l’archivage (LAr) of 26 June 1998 (RS 152.1)
Safety, Prevention & Health Committee (CSPS\textsuperscript{5})

Members and reporting
The CSPS is headed by the EPFL DSPS Delegate and reports directly to the CRM.

In close cooperation with the DSPS experts, the CSPS 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 CSPS 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;
- 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.

\textsuperscript{5} Formerly CSHE
Operation of the SPS Committee
The CSPS sets annual objectives to be validated by the CRM 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 EPFL DSPS Delegate heads the Safety, Prevention & Health Domain and reports to the VPRHO. School and College Safety Coordinators report to the Delegate either directly or operationally. The Delegate is part of the Crisis Unit and is competent to initiate the latter. This task is an integral part of the Delegate’s terms of reference.

EPFL Security, Health & Safety Committee
In order to best meet the needs of EPFL users as well as to inform them, an EPFL Security, Health & Safety Committee has been established, which formally meets twice a year. An extraordinary session may be requested from the Committee Chair. The Committee is made up of:
- The Vice President for Resources & Infrastructures (acting) as the Chair;
- The Delegate of the Safety, Prevention & Health Domain in charge of operating the Committee;
- A Dean representing all School Deans;
- The EPFL General Counsel;
- The Real Estate & Infrastructure Delegate;
- The Delegate for Academic Affairs;
- A representative of each of the three EPFL constituents (teaching staff, students, administrative and technical staff) appointed by the EPFL Assembly.
This Committee has an advisory capacity.
DSPS organisation chart

Figure 7 – DSPS Organisation Chart
IT Security Committee (CSI)

Members and reporting
IT Security is the responsibility of the Vice President for Information Systems, who exercises this through an IT Security Committee.6

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 centre)
   c. access (firewall, access security, data security, archiving);
2. Deploy a network of IT security Delegates in all Schools and Colleges as well as in the cantonal outposts7, according to the action plan proposed by the VPSI and approved by the EPFL Direction;
3. Monitor measures to mitigate such risks;
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 DSPS on crisis management.

6 The external expert will be subsequently appointed by the CSI.
7 The VPSI will develop a plan of action to be submitted to the EPFL Academic Direction (summer 2015).
Roles and responsibilities
IT security is under the responsibility of the Vice President for Information Systems, who chairs the CSI.

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
- Cooperate with other groups engaged in the field of general security
- Draw up the CSI annual report
- Prepare the weekly meetings of the CRM as regards IT security, i.e.:
  - Attend the weekly meetings of the CRM
  - Draw up the IT security report.

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 infrastructure, people and information.

Reports
The CSI issues an annual report whose content is integrated into the CRM annual report.
Insurance Committee (CA)

Members and reporting
The CA reports to a Vice Presidency (which will be selected at a later point). It interacts directly with the CRM in the framework of the ETH Board/EPFL insurance policy. The CA is made up of a representative of this Vice Presidency, the legal counsel in charge of insurance management and the insurance broker (external adviser to EPFL)\(^8\).

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 looking for specific insurance coverage.

Operation
The CA meets several times a 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.

---

\(^8\) As from 2017, this Committee will have to be strengthened with additional expertise in the field of insurance.
Internal Control System Committee (CSCI)

Internal Control System
The EPFL internal control system (ICS9) focuses on the financial impact of management processes and implements key controls to guarantee an acceptable risk level. This system serves to guarantee that financial operations at EPFL are carried out in accordance with existing rules and regulations. The system is managed by the ICS Committee, hereinafter “CSCI”.

Members and reporting
The CSCI is headed by the acting Vice-President for Finances. It is made up of the main ICS process managers. The CSCI reports directly to the CRM.

---

Figure 10 – Organisation of the Internal Control System Committee (CSCI)

---

9 See the Directive on the Internal Control System (ICS) at EPFL – September 2010
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 implemented,
   - the documentation for processes and controls is kept up-to-date and stored,
   - internal auditing recommendations on ICS are acted on;
2. to encourage the identification and mitigation of risks in financial processes, according to a consistent and effective document database, by all administrative employees;
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.
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.
Minutes of meetings are drawn up and distributed for information to all process managers as well as to the CRM.

Role of the Head of the CSCI
The Vice-President for Finance heads the CSCI, with the following tasks:
1. to check that key controls are performed. In addition, he/she shall
   - check the control environment,
   - lead the group of process managers,
   - plan activities and the schedule for their completion;
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. plan and manage the communication of ICS processes within EPFL, particularly among Schools and Colleges (via GT14), by transmitting and commenting on the annual programme;
5. ensure consistency and conformity of the ICS document database and standards;
6. regularly inform the CRM about work progress, at least on a quarterly basis;
7. prepare the CSCI activity report to be included in the annual report of the Risk Management Committee.
8. Role of Process Managers

Each Process Manager shall:
- maintain and develop the documentation, processes and key controls in accordance with the standards defined by the Head of the CSCI and communicate these to staff members involved in the process;
- ensure that the specified key controls are duly performed and documented;
- ensure that the processes under his/her responsibility are certified without qualification;
- answer requests by the ETH Board internal auditing body or by CdF;
- initiate action in line with the aims of his/her process throughout the EPFL scope; responsibility for this gives him/her authority to do so;
- organise the necessary resources within his/her unit towards the continuous improvement and maintenance of an effective ICS;
- establish a plan of action.

Processes and Process Managers

<table>
<thead>
<tr>
<th>Manager</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Albert Meyer</td>
<td>Human Resources</td>
</tr>
<tr>
<td>Pierre Magnin</td>
<td>Planning &amp; Budget</td>
</tr>
<tr>
<td>Bertold Walther</td>
<td>Income</td>
</tr>
<tr>
<td></td>
<td>Closing</td>
</tr>
<tr>
<td></td>
<td>Petty cash</td>
</tr>
<tr>
<td></td>
<td>Cash flow</td>
</tr>
<tr>
<td></td>
<td>Fixed assets</td>
</tr>
<tr>
<td></td>
<td>Expense claims</td>
</tr>
<tr>
<td></td>
<td>Stocks</td>
</tr>
<tr>
<td></td>
<td>Accounts payable</td>
</tr>
<tr>
<td></td>
<td>Camipro electronic payment</td>
</tr>
<tr>
<td>Sandra Henrich</td>
<td>Mortgages</td>
</tr>
<tr>
<td>Elvis Fontaine</td>
<td>Purchasing</td>
</tr>
<tr>
<td>Thierry Crocoll</td>
<td>Opening/closing of third party funds</td>
</tr>
<tr>
<td></td>
<td>Management of FP7 funding</td>
</tr>
<tr>
<td></td>
<td>Management of SNSF funding</td>
</tr>
<tr>
<td>Philippe Staub</td>
<td>Signatures</td>
</tr>
<tr>
<td>Emma Dorée</td>
<td>SQIE</td>
</tr>
<tr>
<td>Julianne Jammers</td>
<td>SQNE</td>
</tr>
<tr>
<td>Franco Vigliotti</td>
<td>EPFL Middle East</td>
</tr>
</tbody>
</table>
Reports

The CSCI issues:

1. a monitoring dashboard distributed quarterly to CRM members, including:
   - a status of processes,
   - a summary of ongoing actions;

2. an annual activity report setting out:
   - the activities undertaken in the ICS framework,
   - the list of revised processes,
   - the list of new activities (sub-processes).

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

---

10 The information processed by the ICS originates from several databases. All data are grouped on the document management website “khety.epfl.ch”. 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 acting Vice President for Finances, the General Counsel, the Vice President for Human Resources and Operations and the Head of Management Control.

This Committee reports operationally to the Vice President for Finances. It reports to the CRM on a monthly basis.

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.
Operation of the Audit Coordination Committee
The CCA meets at least quarterly, based on a schedule, depending on the progress in audits. At least one CCA member attends all closing meetings for each type of audit.

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

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.

This is an integral part of the Audit Coordinator’s terms of reference.

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, at least on a quarterly basis;
• prepare an activity report for the CCA, which will include this in the CRM annual report.

This is an integral part of the Thematic Audit Head’s terms of reference.

Reports
The CCA Coordinator issues:

3. 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;

4. 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.

---

11 The information processed by the ICS originates from several databases. All data are grouped on the document management website “khety.epfl.ch”. The framework for the EPFL ICS is COSO. The applicable auditing standard is NAS 890.