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.
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) ..............................................................................10
IT Security Committee (CSI) ........................................................................................................123
Insurance Committee (CA) ...........................................................................................................145
Dispute Settlement Committee (CRL) ............................................................................................16
Internal Control System Committee (CSCI) ..................................................................................15
Audit Coordination Committee (CCA) ..........................................................................................19

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) ............................10
Figure 7 – DSPS Organisation Chart .............................................................................................112
Figure 8 – Organisation of the IT Security Committee (CSI) .......................................................123
Figure 9 – Organisation of the Insurance Committee (CA) .........................................................145
Figure 10 - Organisation of the Dispute Settlement Committee (CRL) .........................................16
Figure 11 – Organisation of the Internal Control System Committee (CSCI) ..............................16
Figure 12 – Organisation of the 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 and on the Ordinance on the Organisation of the Ecole polytechnique fédérale de Lausanne of 1st March 2004, status as of 1st 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

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 – 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 Vice President for Finances,
- the General Counsel,
- the Safety Delegate,
- and the Head of Internal Controls and Risk Management.

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 within the scope of EPFL (see Figure 1).

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

The CRM coordinates the work of the six 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:

<table>
<thead>
<tr>
<th>Attachment</th>
<th>Unit / Domain</th>
<th>Head of Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>P</td>
<td>Presidency</td>
<td>Martin Vetterli</td>
</tr>
<tr>
<td>P</td>
<td>Faculty Affairs</td>
<td>Hassan Sadeghi</td>
</tr>
<tr>
<td>P</td>
<td>Development Office</td>
<td>Madeleine von Holzen</td>
</tr>
<tr>
<td>P</td>
<td>General Counsel</td>
<td>Susan Killias</td>
</tr>
<tr>
<td>P</td>
<td>Data Protection</td>
<td>Eva Théliois</td>
</tr>
<tr>
<td>P</td>
<td>EPFL Alumni</td>
<td>Leïla Ojeh</td>
</tr>
<tr>
<td>P</td>
<td>Science Outreach Department</td>
<td>Farnaz Moser</td>
</tr>
<tr>
<td>P</td>
<td>Philanthropy</td>
<td>Nathalie Katharina Fontana</td>
</tr>
<tr>
<td>P</td>
<td>Equal Opportunities Office</td>
<td>Helene Fueger</td>
</tr>
<tr>
<td>P</td>
<td>Quality Assurance and Accreditation</td>
<td>William Pralong</td>
</tr>
<tr>
<td>VPE, ENT-E</td>
<td>Vice Presidency for Education</td>
<td>Pierre Vanderghynst</td>
</tr>
<tr>
<td>VPR, ENT-R</td>
<td>Vice Presidency for Research</td>
<td>Andreas Mortghynst</td>
</tr>
<tr>
<td>VPI, ENT-I</td>
<td>Vice Presidency for Innovation</td>
<td>Marc Gruber</td>
</tr>
<tr>
<td>SI</td>
<td>Vice Presidency for Information Systems</td>
<td>Edouard Bugnion</td>
</tr>
<tr>
<td>FI-VP</td>
<td>Vice Presidency for Finances</td>
<td>Caroline Kuyper</td>
</tr>
<tr>
<td>FI-VP</td>
<td>Accounting department</td>
<td>Bertold Walther</td>
</tr>
<tr>
<td>FI-VP</td>
<td>Planning, Treasury and Institutional Data</td>
<td>Yves Allegri</td>
</tr>
<tr>
<td>FI-VP</td>
<td>Internal Controls, Risk Management and Insurance</td>
<td>Hakim Hadjiere</td>
</tr>
<tr>
<td>FI-VP</td>
<td>Head of Controlling</td>
<td>Marc Bachelot</td>
</tr>
<tr>
<td>RHO-VP</td>
<td>Vice Presidency RHO</td>
<td>Etienne Marclay</td>
</tr>
<tr>
<td>RHO-VP</td>
<td>Human Resources</td>
<td>Susanna Swann</td>
</tr>
<tr>
<td>RHO-VP</td>
<td>Safety, Prevention and Health</td>
<td>Eric Du Pasquier</td>
</tr>
<tr>
<td>RHO-VP</td>
<td>Real Estate and Infrastructures</td>
<td>Pierre Gerster</td>
</tr>
<tr>
<td>RHO-VP</td>
<td>Procurement and Purchasing</td>
<td>Elvis Fontaine</td>
</tr>
<tr>
<td>RHO-VP</td>
<td>Congress centre</td>
<td>Julianne Jammers</td>
</tr>
<tr>
<td>RHO-VP</td>
<td>Catering and Merchants</td>
<td>Roland Deléchat</td>
</tr>
<tr>
<td>RHO-VP</td>
<td>Sustainable Campus</td>
<td>Philippe Vollichard</td>
</tr>
<tr>
<td>ANT-VS</td>
<td>EPFL Valais Wallis</td>
<td>Marc-André Berclaz</td>
</tr>
<tr>
<td>ANT-FR</td>
<td>EPFL Fribourg</td>
<td>Anne-Claude Cosandey</td>
</tr>
</tbody>
</table>

### School / College

| SB         | Basic Sciences                                     | Jan S. Hesthaven                |
| I&C        | Computer and Communication Sciences                | James Larus                     |
| ENAC       | Architecture, Civil & Environmental Engineering   | Marilyn Andersen                |
| SV         | Life Sciences                                      | Gisou van der Goot             |
| STI        | Engineering science & technology (inc. Neuchâtel Outpost) | Ali Sayed            |
| CDM        | College of Management                              | Dominique Foray                 |
| CDH        | College of Humanities                              | Thomas David                    |
| EPFL ME    | EPFL Middle East                                    | Franco Vigliotti                |

*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 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 CFO, 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 Members

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
<th>Domains</th>
<th>Reporting to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Caroline Kupyer</td>
<td>Vice President</td>
<td>Finances</td>
<td>FI</td>
</tr>
<tr>
<td>Susan Killias</td>
<td>General Counsel</td>
<td>Legal</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>Hakim Hadjeres</td>
<td>Head of Service</td>
<td>Internal Controls, Insurance</td>
<td>FI</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 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.

2 Note: additional experts may be invited by the CRM as necessary
Reporting Obligations / Information

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 or the President of the CRM and subject to validation by the EPFL President – pursuant to the ETH Board <em>Directive sur le devoir d’annonce</em> of 14th September 2001 (LEX 1.8.0.2).</td>
</tr>
<tr>
<td>The EPFL President and Direction</td>
<td>Via an annual report. On an ad hoc basis when circumstances so require.</td>
</tr>
<tr>
<td>The Heads of Units, the Vice Presidents, School Deans and College Directors</td>
<td>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.</td>
</tr>
<tr>
<td>The Head of Communications</td>
<td>Of any sensitive files on an ad hoc basis. Of any subject relating to the EPFL image.</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.

<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>Hakim Hadjeres</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>Hakim Hadjeres</td>
<td>Excel</td>
</tr>
<tr>
<td>ICS</td>
<td>Register of financial risks and key controls</td>
<td>Philippe Staub</td>
<td>Excel</td>
</tr>
<tr>
<td>Insurance</td>
<td>Insurance scheme and table of claims</td>
<td>Hakim Hadjeres</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>
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.

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).³

³ Loi fédérale sur l’archivage (LAr) of 26th June 1998 (RS 152.1)
Safety, Prevention & Health Committee (CSPS)

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

Missions of the SPS Committee (CSPS)
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.
Operation of the SPS Committee

The CSPS 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 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.

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 responsibility through an IT Security Committee.

Figure 8 – Organisation of the IT Security Committee (CSI)

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 DSPS on crisis management.

Roles and responsibilities
IT security is 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 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, the Head of Internal Controls and Risk Management and a legal counsel from the Human Resources department.

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 General Counsel, EPFL legal counsels and support staff for coordination.

Figure 10 – Organisation of the Dispute Settlement Committee (CRL)

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) 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 headed by the Head of Internal Controls and Risk Management. It is made up of the main ICS process managers. The CSCI reports directly to the CRM.

Figure 11 – Organisation of the Internal Control System Committee (CSCI)

---

* See the Directive on the Internal Control System (ICS) at EPFL (LEX 1.7.1)
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.
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
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.

---

5 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.

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

Figure 12 – Organisation of the Audit Coordination Committee (CCA)

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 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.