



Extract from the directive on risk management and the internal control system of the Orell Füssli Group

1. Objectives

The ICS (internal control system) of the Orell Füssli Group is aimed at the systematic control of risks. It is comprehensive and also covers those areas which are not included in external audits. External audits complement the ICS and review it in the context of legal requirements. The basis of the ICS is risk management, which identifies risks, and evaluates and recommends action in order to reduce or prevent risks.

The description of the ICS therefore focuses essentially on the identification of risks and is based on divisional risk management.

In principle, responsibility for the group-wide implementation of risk and ICS management lies with the Board of Directors and the Executive Board of Orell Füssli Holding Ltd (OFH).

For this purpose, the ICS for Orell Füssli has been structured in line with the internationally customary risk and control framework (COSO¹).

The following goals are pursued with the internal control:

- The efficiency and effectiveness of activities/processes are assessed and improved where appropriate.
- The reliability and integrity of financial reporting and risk reporting are ensured.
- Compliance with applicable standards, i.e. public law and ordinances as well as internal company orders, directives and guidelines, is reviewed.
- Transparency regarding the risk situation is created by regular reporting and any deviations from this.

2. Risk and risk management

Risk is determined on the one hand by the likelihood of its occurrence and on the other by the extent of the potential damage. Correspondingly, risk reduction implies exerting influence on the likelihood of occurrence and/or action to reduce the potential damage. Risk reduction is the task of risk management, which is a component part of managerial duties and is monitored by the ICS.

With a view to simplicity of implementation, risk management is based on the following risk categories:

¹ COSO = Committee of Sponsoring Organizations of the Treadway Commission.

Risk category	Sub-category
Planning, development	- Risks arising from planning and development processes
Sales and procurement market	- Non-performance of partners and/or customers (e.g. also supply risks, supplier risks, business continuity, etc.) - Changes in the business environment: markets, consumers, customers, suppliers, competitors, technology, regulation
Performing services and production	- Quality risks (risks in service performance processes) - Process risks - Failure of means of production
Financial reporting, accounting, financing	- Financial reporting - Bases for cost calculation - Acquiring means of production - Financing - Changes in the business environment: financial markets, interest rates, currencies, investors
Personnel	- Fraud risks - Personnel deployment /Personnel selection - Accidents at the workplace - Disclosure of confidential internal information
Location & environment	- Risks of intrusion - Damage caused by natural hazards - Changes in the business environment: laws, society, politics, climate, etc.
Contracts	- Contract risks
IT	- Technology risks - Cyber risks - Failure - Security
Control environment - COSO	- Corporate culture, business conduct of management - Integrity/ethical values in the company - Organisational structure - Principles of personnel policy - Transparency & internal communication
Reputation & Image	- Perception in the media

The outcome of risk management is recorded in the divisions in a risk matrix. This is subdivided in accordance with the above-mentioned risk categories and includes material individual risks and the relevant action. A synthesis is compiled at group level on the basis of the divisional risk matrix and complemented by specific group risks.

3. Compliance and compliance reporting units at OFH

Damage can also occur if directives are not complied with. Compliance is the responsibility of the CEO and the Heads of Division, who can delegate tasks (but not responsibility) to the Risk Officers for their support. All employees are obliged to report non-compliance with directives, and even suspicion of non-compliance, to their line manager. In instances where employees feel uneasy they can contact one of the following OFH units:

- Internal: OFH Risk Officer
- External: Mr Guido Seitz, Attorney-at Law in Zurich, www.vrhc.ch.

4. Training

An essential element for the successful management of the risk and ICS organisation is regular training in ICS issues, for both the OFH Risk Officer, the divisional Risk Officers and employees. Suppliers and agents must also receive ICS-relevant information, at least as integral components of contracts. The OFH Risk Officer ensures that the target groups receive regular basic and further training. He approves an appropriate training concept and is supported in this by the HR function or external providers.

5. Organisation and incorporation in the OF Assurance concept

Risk management and the ICS are conducted primarily by the divisions. OF Holding provides the systematic principles, basic training, coordination and monitoring as defined in the corporate governance obligations. The organisation is incorporated in the "OF Assurance Concept" (cf. page 4). This concept is based on the familiar "Three Lines of Defence" model, in order to represent transparently the differing roles in internal corporate control and their interplay within the OF Group.

Those persons and units bearing active responsibility in the context of risk and ICS management are described below:

Board of Directors

The Board of Directors is responsible to the shareholders and the law for the effectiveness of group-wide risk, ICS and compliance management and has to report on the functional capability of the ICS in the context of the annual report. The Board of Directors has delegated the monitoring of risk and ICS activities, but not responsibility for them, to the Audit Committee. The Board of Directors assesses the risk situation and arranges to be informed about the status of the ICS.

The Board of Directors' Audit Committee

- assesses the current risk situation and the status of the scheduled ICS audit plans
- assesses the divisions' proposals regarding ICS audit plans for the coming year and schedules these
- identifies in cooperation with the CEO, the CFO and the OFH Risk Officer any audit items for Internal Audit and the external auditors and stipulates these.

CEO and Heads of Division

Monitoring and dealing with risks in the context of normal business activity is the responsibility of the CEO and the Heads of Division. In this process these persons have primarily to organise Controlling (incl. Strategic Controlling) in such a way that the requirements of good opportunity and risk control are satisfied. They can delegate part of the control duties, but not their responsibility, to employees within the company.

OFH Risk Officer

The OFH Risk Officer coordinates the implementation and functional capability of risk, ICS and compliance management at group level.

Divisional Risk Officer

The Divisional Risk Officer oversees the matters of risk, ICS and compliance management within a division.

Coordination with the Security Officer

The Security Officer informs the CEO, the OFH Risk Officer, the Heads of Division and the divisional Risk Officers about relevant security issues of significance for risk and compliance management. He is informed about the risk situation by the OFH Risk Officer in the context of the reporting process.

Coordination with the insurance coordinator

At group level the CFO of OFH exercises the function of an insurance coordinator. He bundles and coordinates the insurance needs of the divisions and ensures the optimal transfer of risk from the group to insurance companies. If risk transfer requirements are identified at divisional level, the insurance coordinator must be consulted.

External auditors

The external auditors fulfil the corporate function stipulated by law. The external auditors must verify the existence of the internal control system insofar as it is relevant for financial reporting and confirm this in the audit report.

Internal Audit

Internal Audit supports the Board of Directors in performing its supervisory function. Internal Audit performs its duties independently and autonomously. It assesses the effectiveness and efficiency of risk management, the internal control and monitoring systems as well as the management processes (governance) and contributes to their improvement. Internal Audit also verifies conformity with standards (compliance) and performs independent and objective assurance and advisory services.

OF – «Assurance Concept»

