orell füssli
group

# Regulations

| | |
|---|---|
| Subject | **Risk Management and Internal Control System (ICS) of the Orell Füssli Group** |
| Instruction number | REK-0005 |
| Scope | OF Group |
| Valid from | 01.05.2021 |
| Release by | VR |
| Responsible | CEO |
| Author | BMU |

## 1 Purpose of the regulations

The need to set up and document risk management and the ICS is based on the following provisions or guidelines that are binding for listed companies:

- Swiss company law
- SIX Corporate Governance Directive (DCG) of 1 January 2016
- Swiss Code of Best Practice for Corporate Governance (Economiesuisse) vom 28.08.2014

Company law [1]goes one step further by requiring that the board of directors must ensure a functioning internal control system (ICS) and confirm the existence of the ICS, as far as it is relevant for financial reporting, through the external audit in the audit report.
In order to take into account the regulations on the formal design of an ICS, but also with the aim of providing an effective and efficient working tool for management, the binding principles for an ICS in the OF Group are defined here. For the organisational implementation, additional directives are issued where necessary.

## 2 Content of the regulations

### 2.1 Internal Control System ICS

The ICS in the OF Group aims to systematically control risks. The internal control system is comprehensive and also covers those areas that are not covered by the external audit. The external audit examines it within the framework of the legal requirements. The basis of the ICS is risk management, which identifies risks, evaluates and recommends measures to reduce or prevent any risks.
The description of the ICS therefore essentially focuses on the recording of risks and builds 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 the Orell Füssli Group (OFG). For this purpose, the ICS for Orell Füssli has been structured on the basis of the internationally used COSO risk and control framework.
Internal control aims to achieve the following objectives:

- The efficiency and effectiveness of the activities / processes are assessed and improved if necessary.
- The reliability and integrity of financial reporting and risk reporting are ensured.
- Compliance with the applicable standards, i.e. public laws and regulations as well as internal directives, instructions and guiding principles of the company are checked.
- Transparency about the risk situation through regular reporting and any deviations from it is created.

[1] Swiss Code of Obligations Art. 728a, b OR

## 2.2 Risk and risk management

The risk is determined on the one hand by the probability of occurrence and on the other hand by the extent of the possible damage. Accordingly, risk reduction means influencing the probability of occurrence and/or measures to reduce the potential damage. Risk reduction is the task of risk management, which is part of the management task and is monitored by the ICS.

The result of risk management is recorded in the divisions in a **risk register.** This is structured according to the risk categories mentioned above and includes important individual risks and the associated measures. At the Group level, a synthesis is drawn up on the basis of the divisional risk registers, which is supplemented by specific Group risks.

## 2.3 Compliance

Damage can also occur if applicable laws and internal directives are not complied with. Compliance is the responsibility of the CEO and the division heads, who can delegate tasks (but not responsibility) to the risk officers to support them.

## 2.4 Training

An essential element for the successful management of the risk and ICS system is regular training in ICS issues for the OFG risk officer, the risk officers of the divisions and the employees. The OFG Risk Officer ensures the training and regular further education of the target groups after having ascertained the concrete needs. He approves an adequate training concept that is appropriate to the level and needs. He is supported in this by the HR function or by external providers.

## 2.5 Compliance Reporting Offices OFG

All employees are obliged to report non-compliance with instructions or even the suspicion of non-compliance to their superiors. In cases where employees would feel uncomfortable doing so, they can report to one of the following OFG reporting offices:

- Internal: Risk Officer OFG
- External: Mr. Guido Seitz, Attorney at Law, Zurich, www.riversidelaw.ch

## 2.6 Reporting

Reporting is carried out at the appropriate level by means of:

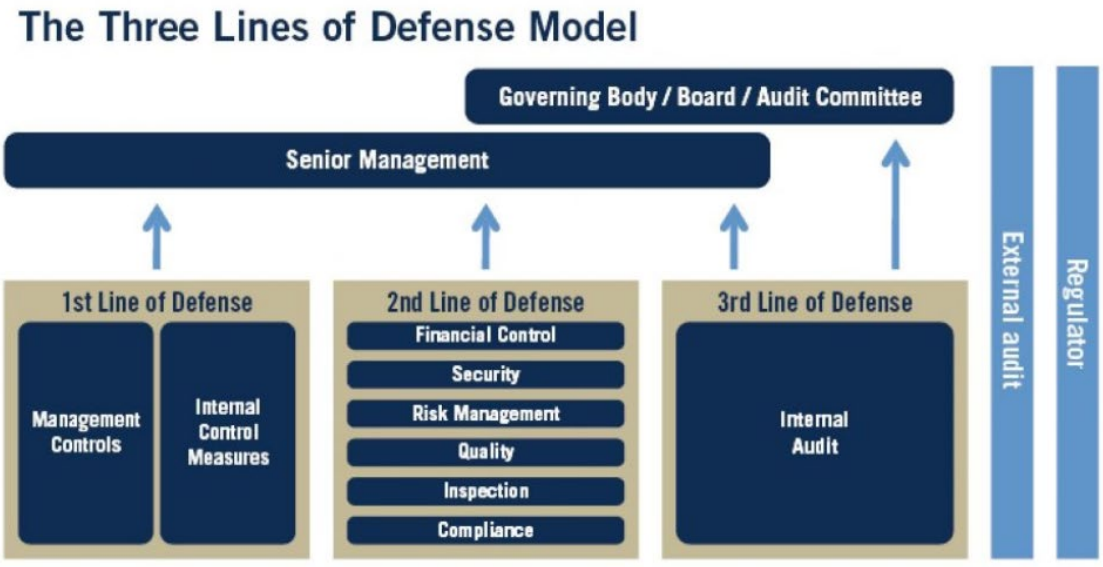
- Risk report (updated 2 times a year)
- Risk and ICS report (planning, implementation, results, measures)
- by:
- Risk Officer OFG
- for the attention of:
- Group Executive Board OFG
- Board of Directors Audit Committee
- Board of Directors (at least 1 time per year)

## 2.7 Management tools to support the ICS

Various management instruments are used at Orell Füssli to manage the risks described. These include strategic and financial controlling, quality management systems, process audits and other control instruments ranging from the four-eyes principle and signature regulations to internal and external auditing.

## 2.8 Organisation and integration in the OF assurance concept

Risk management and ICS are primarily the responsibility of the divisions. The Group provides the systematic basis, training, coordination and monitoring in accordance with the corporate governance requirements. The organisation is integrated into the "OF assurance concept". This concept is based on the well-known "Three Lines of Defence" model in order to transparently present the different roles for internal corporate management and their interaction within the OF Group.




Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*

The persons and entities actively involved in risk and ICS management are described below.
**Board of Directors (BoD):** The Board of Directors is responsible to the shareholders and the law for the effectiveness of the Group-wide risk, ICS and compliance management and must report on the functioning of the ICS in the annual report. The BoD has delegated the monitoring of the risk and ICS activities, but not the responsibility for them, to the Audit Committee. The BoD assesses the risk situation and obtains information on the status of the ICS. The BoD Audit Committee

- assesses the current risk situation and the status of the defined ICS audit projects twice a year,
- assesses the divisions' proposals for ICS audit projects for the coming year and determines them,
- identifies and determines, in collaboration with the CEO, the CFO and the Risk Officer OFG, any audit points for the internal/external audit.

**CEO and DivL:** Risk monitoring and management in the course of normal business activities is the responsibility of the CEO and the division heads. These persons in charge have to organise the controlling (incl. strategic controlling) in such a way that the requirements for a good opportunity and risk control are met. They can delegate some of the controlling tasks, but not their responsibility within the company to employees.
**Risk Officer OFG:** The Risk Officer OFG coordinates the implementation and functioning of risk, ICS and compliance management at the Group level (see section 11).
**Risk Officer Division (ROD):** The ROD is responsible for risk, ICS and compliance management within a division.
**Coordination with the Security Officer (SIBE):** The Security Officer informs the CEO, the Risk Officer OFG, the Division Heads and the ROD about relevant security issues that are important for risk and compliance management. He is informed by the Risk Officer OFG about the risk situation within the framework of reporting.

**Coordination with the insurance coordinator:** At Group level, the CFO OFG acts as insurance coordinator. He bundles and coordinates the insurance needs of the divisions and ensures the optimal risk transfer from the Group to insurance companies. If risk transfer requests are identified at the divisional level, the insurance coordinator must be consulted.
**External audit:** The external audit fulfils the organ function prescribed by law. Furthermore, the external audit must confirm the existence of the internal control, as far as it is relevant for the financial reporting, in the audit report.
**Internal audit:** The internal audit (IR) supports the board of directors in the exercise of its supervisory function. The IR performs its tasks independently and autonomously. It assesses the effectiveness and efficiency of the risk management, the internal management and control systems as well as the management processes (governance) and contributes to their improvement. Internal Audit also reviews compliance with standards and provides independent and objective assurance and advisory services.

## 2.9 Tasks of the Risk Officer OFG

The Risk Officer OFG ensures the implementation and functionality of the risk and ICS management at the Group level. He is primarily responsible for coordination and control tasks, which he carries out himself or delegates to specialists. In addition, the Risk Officer OFG develops guidelines for the quality of specific processes and makes suggestions for improvement in the event of identified weaknesses. He provides technical leadership to the RODs of the divisions. The Risk Officer OFG reports to the CEO and the Audit Committee of the Board of Directors. He is responsible for the management of the ROD and for reporting to the BoD AC, GL, CEO and the Safety Officer OFG. His tasks are listed below:

| | |
|---|---|
| **Version** | **Risk management:** The Risk Officer OFG coordinates the process of periodically revising the risk registers for the Group and for the individual divisions. To this end, he directs the RODs in such a way that the process is carried out in a coordinated manner according to appropriate methodology. He assesses the divisional results and takes corrective action if necessary. He prepares the Group's risk register in cooperation with the CEO.<br><br>**ICS audits**: The Risk Officer OFG proposes an audit plan for the following year to the BoD Committee AC in the last quarter of the year. After approval by the AC BoD Committee, he ensures timely and correct implementation. He assesses the results of the audits and makes concrete proposals to the CEO for the elimination of weaknesses. He accompanies the follow-up process until the successful completion of the implementation measures. |
| **Control** | In consultation with the line managers and in cooperation with the RODs, the Risk Officer OFG shall perform the following tasks:<br><br>**Compliance:** (Compliance is understood to mean adherence to internal company directives and regulations, but also to laws, ordinances and other publicly binding, national and international provisions).<br><br>- The Risk Officer OFG monitors whether the applicable internal directives, regulations, process descriptions, etc. are complied with by the employees concerned. He ensures that, if necessary, measures are taken to ensure compliance.<br><br>- It verifies that employees are<br><br>- aware of the legal provisions affecting their activities and keep abreast of changes. |

| | |
|---|---|
| | - It ensures the regular review of specifications for clarity, completeness, appropriateness and correctness.<br><br>**Processes:** The Risk Officer OFG checks whether the risks inherent in the performance and production processes have been identified and recorded, whether fraud risks are covered by suitable control mechanisms (suitable definition of controls to be carried out as target/actual comparison, dual control principle, signature regulation, etc.), whether confidential information is clearly classified and handled and periodically examined. |
| **Reporting** | **Periodic reporting to the BoD, BoD AC, GL OFG, CEO and to the Safety** Officer OFG**:** The Risk Officer OFG ensures that documents and activities are continuously updated and that reporting is carried out at the appropriate level in accordance with the requirements.<br><br>**Event-related reporting to CEO: The** Risk Officer OFGH reports on risk management-relevant events in the Group to the CEO. |
| **Support** | **Advice:** The Risk Officer OFG advises the CEO and the GL OFG on risk management issues.<br><br>**Recommendations:** The Risk Officer OFG recommends adjustments to processes, directives, regulations and risk management to the CEO and the BoD AC.<br><br>**Consultation of experts:** If necessary, the Risk Officer consults OFG experts. |

## 2.10 Tasks of the Divisional Risk Officers

The ROD ensures the implementation and functionality of the risk management and ICS at the Division level. In addition to maintaining the systems, he ensures reporting to the Risk Officer OFG. The ROD also performs division-specific tasks as instructed by the DivL. His tasks are listed below:

| | |
|---|---|
| **Version** | **Risk register:** The ROD compiles the Division's risk register in accordance with the specifications of the Risk Officer OFG and ensures on an ongoing basis that the description and evaluation of risks are up-to-date.<br><br>**Risk management:** The ROD ensures the completeness and appropriateness of divisional risk management within the framework of Group-wide requirements.<br><br>**ICS projects**: The ROD identifies and proposes which topics and items are to be audited in the coming calendar year. It ensures on an ongoing basis that the status of the documentation of the work in progress is up to date.<br><br>All tasks are carried out in coordination with the Risk Officer OFG and the Division Heads. |
| **Control** | **Compliance:**<br><br>The ROD checks whether the applicable internal directives, regulations, process descriptions, etc. are complied with by the employees con- |

| | |
|---|---|
| | cerned. In the event of misconduct, he clarifies whether this is due to ignorance of the directive, outdated regulations, negligence or other reasons. It defines measures to ensure compliance with the requirements.<br>- It verifies that employees are aware of the legal provisions affecting their activities and keep abreast of changes.<br>- It ensures the regular review of specifications for clarity, completeness, appropriateness and correctness.<br>**Processes:** The ROD checks whether the risks inherent in the performance and production processes have been identified and recorded, whether fraud risks are covered by suitable control mechanisms (precise definition of controls to be carried out as target/actual comparison, dual control principle, signature regulation, etc.) and whether information worth protecting is adequately classified and handled. |
| **Reporting** | **Periodic reporting to DivL (copy to Risk Officer OFG):** The ROD continuously updates documents and activities on the shared repository and reports regularly to the DivL.<br>**Event-related reporting to DivL:** The ROD keeps a log of risk management-relevant events in the division and ensures that the DivL and the Risk Officer OFG are informed. |
| **Support** | **Advice:** The ROD advises the DivL and Division cadre on risk management issues.<br>**Recommendations: The** ROD recommends adjustments to processes, directives and risk management to the DivL and the Risk Officer OFG.<br>**Involvement of experts:** If necessary, the ROD consults experts in consultation with the OFG Risk Officer and the DivL. |

**Organisation ROD**

**Requirements**: The ROD may perform his function on a part-time basis, provided that the DivL ensures that the ROD has sufficient capacity and expertise to perform the risk management and ICS tasks. As a rule, he is an employee of the Division. The ROD must be available for the tasks assigned to him/her, have analytical and business management skills and be characterised by independence of judgement and action.

**Subordination:** The ROD reports directly to the DivL and is appointed by him in consultation with the Risk Officer OFG. The ROD is technically led by the Risk Officer OFG.

**Cooperation with DivL**: The ROD supports the DivL significantly in the implementation of risk management. As a rule, the ROD acts on his own initiative, but he can also act on behalf of the DivL. The ROD discusses his activities in advance with the Risk Officer OFG and the DivL and reports to both.

**Cooperation with the Risk Officer OFG:** The ROD supports the Risk Officer OFG in the execution of his tasks. The Risk Officer OFG provides technical leadership to the ROD, has the right to issue instructions to the ROD on technical matters and monitors the quality and efficiency of the ROD's work through controls in consultation with the DivL.