


Systematic Integration of ORM and ICS



Marcel Stalder
 Certified Public Accountant
 Partner
 Industry Leader Insurance
 Audit Services
 marcel.stalder@ch.ey.com



Stephanie Furger
 Master's degree in economics, HSG
 Senior Manager
 Advisory Services
 stephanie.furger@ch.ey.com

 **Swiss law requires the use of internal control systems and risk management. If these two disciplines, which until now have often been applied independently, are systematically implemented and integrated, many synergies can be realized.**

With the inclusion of an internal control system (ICS) and risk management requirements in Swiss legislation (Code of Obligations from mid-2007 and Insurance Supervision Act since 1 January 2006), two important components of corporate governance are becoming compulsory. The new provisions are Switzerland's way of responding to the changed environment for insurers. Financial scandals and the stock market slump of a few years ago have spurred rating agencies, legislators and regulators into action all over the world. Internationally, the demand of stakeholders

for internal control systems and risk management has grown substantially. Examples:

- New requirements for internal control systems (e.g. Sarbanes-Oxley Act, SOX, in the US; Loi sur la sécurité financière in France; EU Directives 4,7 and 8; the Code of Obligations and the Insurance Supervision Act in Switzerland).
- New solvency requirements (Swiss Solvency Test in Switzerland and Solvency II in the EU).
- Enterprise risk management (Standard & Poor's).

ORM and ICS: previously independent ...

Historically, risk management concepts, particularly operational risk management (ORM) and internal control systems, were regarded as an independent discipline:

- ORM evolved from risk management, for which a chief risk officer is often responsible and which at many companies is monitored by a risk management committee.
- ICS developed as an aspect of management and corporate governance in the context of management concepts. It com-

Historically, risk management concepts, particularly operational risk management (ORM) and internal control systems (ICS), were regarded as an independent discipline.

prises several areas of responsibility: financial reporting, which is headed by a chief financial officer and monitored by an audit committee; operations, which is headed by a chief operations officer; and

compliance, which is headed by a chief compliance officer. After the financial scandals, the legislatures of many countries made only one aspect of ICS compulsory: financial reporting (e.g. SOX in the USA and new provisions of the CO in Switzerland). Consequently, many companies placed the responsibility for ICS as a whole with the CFO with oversight at the board level by the audit committee.

The parallel development of these two complementary disciplines has resulted in redundancies. In spite of their different provenances and functions, ORM and ICS overlap in many areas, because both disciplines are based on the process structure of a given company and support the management in its steering activity. Numerous companies are therefore faced with the following challenges:

- Managers are complaining about the increasingly onerous duty to document key activities. In many cases, they are required to document their processes, risks and controls vis-à-vis various corporate bodies (e.g. ICS, ORM, quality management) several times a year.
- At many companies, a control culture has developed which is incompatible with risk-based management.
- Frequently, substantial expenditures are considered for improving control, but no cost-benefit analysis is performed.

... now to be harmonized

These challenges, in combination with steadily increasing cost and performance pressure, are making efficient risk management a more and more important competitive factor. The latest developments, therefore, are aimed at integrating and harmonizing ICS, ORM and other initiatives such as quality management (EFQM, ISO, etc.).

Existing practices form the basis while at the same time operational efficiency, effectiveness and consistency are promoted. The key objectives of this harmonization and integration process are as follows:

- No significant overlaps or gaps between the various control and risk management functions: all major risks, controls and tasks must be identified and addressed in a uniform manner.
- Allotment of tasks to those persons and departments best suited to perform them: identified key risks must be assigned to a risk taker, a risk controller and a risk owner and be managed by means of appropriate tasks.
- Inclusion of the framework in the business, because risk management cannot

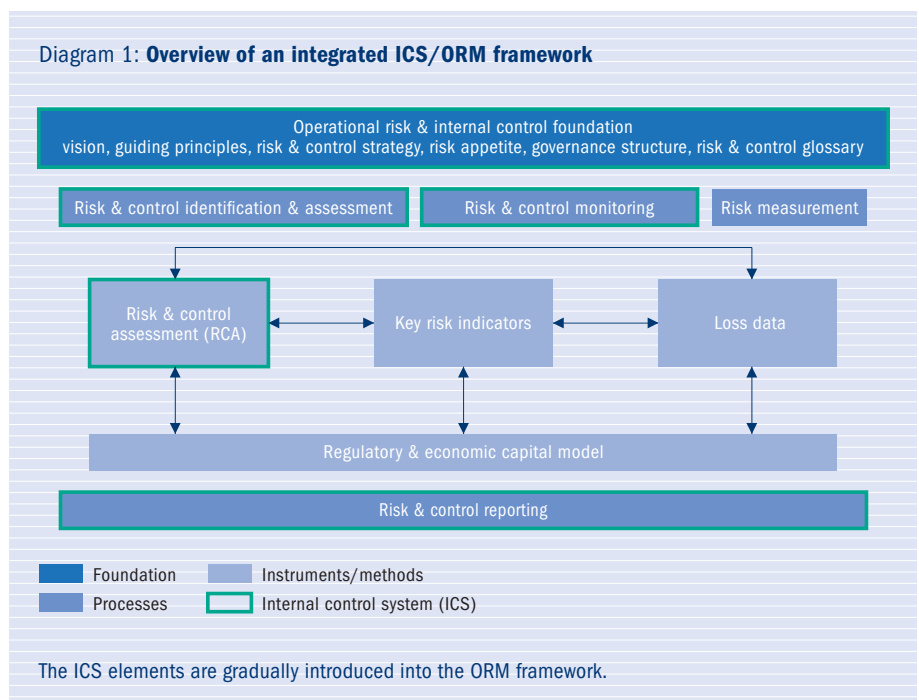
carry out this responsibility on its own (risk taker function).

- Flexibility of the framework so that new risks, organizational changes and local needs can be attended to.
- Ability to review the framework and, consequently, ensure transparency in activities; this requires documentation.

The following is a description of a proven approach to the integrated management of ORM and ICS.

Integrated ICS/ORM approach

The ORM framework into which the ICS elements are gradually introduced is the starting point for integrating ICS, ORM and other control functions (see Diagram 1).



The basis of the framework is the operational risk and internal control foundation, whose purpose is to complement existing components such as the vision, the guiding principles, the risk and control strategy, the risk appetite, the governance structure and the risk and control glossary with the components of ICS. Loss data (pertaining to the past) as part of risk measurement will be adopted without any changes as ICS does not set out any new requirements. Key risk indicators (pertaining to the future) as part of risk and control monitoring do not necessarily have to be implemented in Switzerland from a purely regulatory point of view. Risk and control assessments (pertaining to the present) are at the center of these two approaches. It is here that the most overlaps have developed, so this is where the most synergy can be gained. The following section will therefore discuss these components in detail. In Switzerland, there are no regulatory requirements for insurance companies as far as regulatory and economic capital models in the area of ORM are concerned. This component will, however, be relevant for companies that have to meet the Solvency II requirements. Risk and control reporting has to be expanded by the information needs of all areas of ICS (financial reporting, operations and compliance) and incorporated into ORM.

Risk and control assessments

The most synergy can be gained from risk and control assessments (RCA). The ICS method forms a basis for the ORM elements. The RCA process can be broken down into eight steps (see Diagram 2):

1. Scoping: in scoping, the corporate processes are linked to the annual financial statements (financial reporting), the company and performance goals (opera-

Diagram 2: An overview of risk and control assessment



The greatest synergetic effect is obtained in the risk and control assessments process, which is built on the ICS method and complemented by the ORM elements.

tions) and the compliance provisions (compliance). This results in the identification of the corporate processes that determine the company's goal achievement in the indicated areas. These core processes form the basis for an integrated ICS/ORM system (see Diagram 3).

2. Process documentation: the processes identified as relevant in Step 1 (scoping) are documented on the basis of existing process documentation (if available).
3. Risk identification: the main risks in

connection with goal achievement in the areas of financial reporting, operations and compliance are identified and docu-

Because efficient risk management is becoming a more and more important competitive factor, the latest developments are aimed at integrating and harmonizing ICS, ORM and other initiatives.

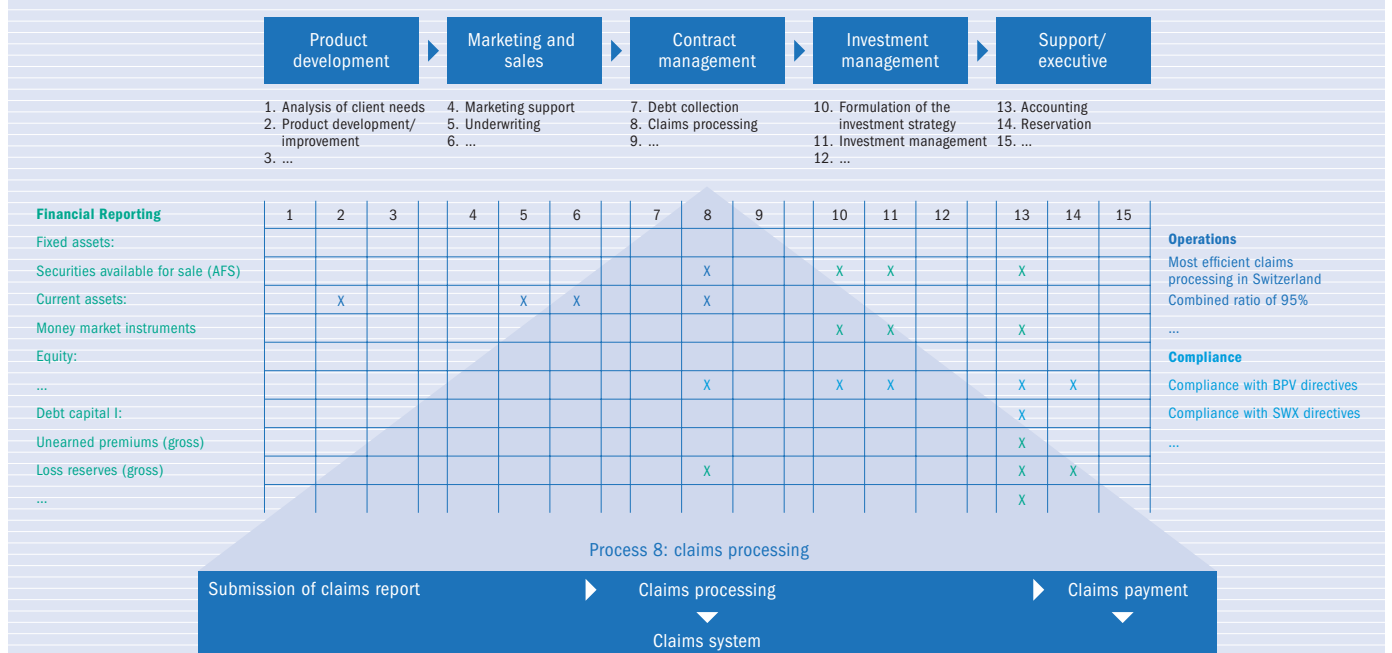
mented at the process level. They are broken down into four categories – people, processes, systems, external influences – on the basis of the risk catalogue, which is defined for the entire company.

4. Inherent risk assessment: the identified risks are assessed in terms of the probability of their occurring and the ensuing damage if they do.
 5. Control identification: existing controls that address the identified risks are identified and documented.
 6. Control assessment: the identified controls are assessed in terms of the effectiveness of their design and performance.
 7. Residual risk assessment: the residual risk is defined by means of an inherent risk assessment (Step 4) in combination with a control assessment (Step 6).
 8. Mitigation/remediation: the residual risk is compared to the company's risk tolerance. If the residual risk exceeds the risk tolerance limit, mitigation action must be defined in order to further reduce the existing risk.
- The integrated model described above is summed up in Diagram 4 (see page 12).

Benefits and challenges

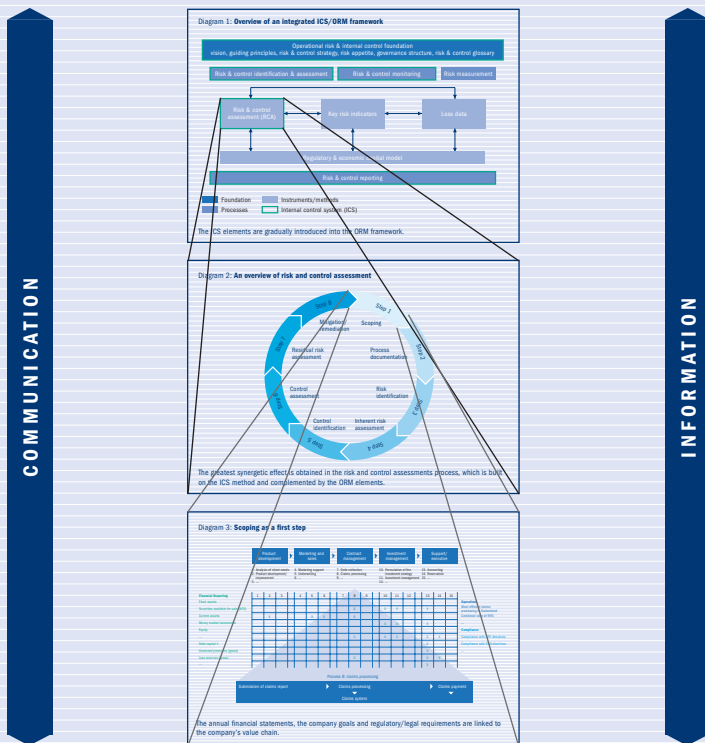
The advantage of an integrated ICS/ORM model lies in the systematic linking of the various governance, risk and control functions of a given company. The risk and control processes are uniformly defined and assessment and reporting processes are harmonized. This eliminates redundancies, fills gaps and allows reports to offer inclusive statements. What matters is overall assurance rather than fragmented views of individual functions. At the center of this approach lies the creation of added value, which increases acceptance within the

Diagram 3: Scoping as a first step



The annual financial statements, the company goals and regulatory/legal requirements are linked to the company's value chain.

Diagram 4: integrated ICS/ORM framework



Information and communication are key elements of the implementation process.

management and the hierarchy, and not isolated instances of compliance with regulatory provisions.

There are various challenges associated with this integrated ORM and ICS approach. It requires the merging of previously independent areas and disciplines. Isolated knowledge of a specific discipline is not sufficient in the context of this integrated approach. In order to implement it successfully, specialist teams are required

that are equally knowledgeable in all areas and have several years of experience within the insurance sector. 🇩🇪