



IT Risk Management requires Automation

Introduction

Risks are the salt in the soup of economic activity – too little and it tastes insipid, too much and the whole thing is inedible. In terms of enterprise-wide risk management, IT is becoming increasingly important: enterprise software products are being used more and more to perform increasingly complex functions, which means an increase in reliance and the associated risk. Companies need to prove that they have this under control. For a long time, successful companies have therefore relied on continuous automation as an important component of their forward-looking IT risk management strategy.

Seeing more than the tip of the iceberg	2
Evaluating risks correctly	2
IT as a risk factor.....	3
Benefits of automation for IT risk management	4
Trust is good, control is better.....	4
Avoiding risks through automated controls.....	5
Acting in compliance with the law and with the rules	5

It was one of the most tragic disasters in the history of civil navigation and is at the same time a classic example of incorrect or at least inadequate risk management: when the Titanic set off on her maiden voyage from Southampton to New York on 10 April 1912 under Captain Edward John Smith she was regarded as being unsinkable, which unfortunately proved to be a fallacy. An avoidance manoeuvre went wrong, leading to a collision with an iceberg in the vicinity of Newfoundland.

The list of failings which led to the disaster and above all to the high number of victims is a long one. Too few lifeboats, disregarded warnings, missed radio communications and too great a readiness to accept risk, to name but a few. A series of incorrect assessments of existing risks and a chain of unlucky circumstances led to a catastrophe which, even today, 100 years on, lives on in memory. In retrospect, the disaster could easily have been prevented. However, this would have required a clear assessment of the risks – that is to say risk management.

SEEING MORE THAN THE TIP OF THE ICEBERG

In principle, any company nowadays which uses software solutions and wishes to control corresponding processes using external tools must be aware that not only the software needs to be audit-proof, but also all tools in the data centre which are used for automation. Under the law as it currently stands, no auditor will certify annual financial statements if a retrospective manipulation of data records is possible. In the processing of mass data, for example, UC4's solutions act as a component of the internal control system, as required under the German Companies Acts [Aktiengesetz and GmbH-Gesetz].

For companies, the time has come to implement transparent and measurable IT processes and also extend their internal control systems to include IT. Companies should make use of professional external support which is familiar with the applicable rules and best practice frameworks. To return to the example of the Titanic: then as now, it is characteristic that the majority of the factors which can cause problems are not apparent at first glance. It is well-known that only the tip of an iceberg projects above the surface of the water, more than two thirds are underwater. In the world of enterprises too, the visible risks often only represent the tip of the iceberg. For this reason, managers should not rely on their own vigilance, but should implement automatic processes to ensure comprehensive risk management. Even small leaks can have major consequences – the hole torn in the hull of the Titanic during the collision with the iceberg was originally no bigger than 1.2 square metres in size.

EVALUATING RISKS CORRECTLY

But what are risks exactly? In statistical terms, a risk is the combination of the probability of an event and its consequences. Risk management, then, is the sum of all actions which serve to steer and control an organisation in terms of a risk. For example, risks can be reduced in that certain rules are complied with, for example safety precautions, material properties or maximum speeds. In the case of the Titanic, although the existing rules were largely followed, they proved to be inadequate.

A distribution of existing resources can also reduce risks: examples of this include investing funds in different classes of investment which, while minimising the risk of a total loss, also reduces the likelihood of achieving maximum



Figure 1: Risk factors in companies

returns. Risks cannot be eliminated, but entering into a risk is always an individual decision. We face such decisions extremely often in day-to-day life: we justify dangerous sports and unhealthy lifestyles to ourselves because they give us an adrenaline rush or pleasure, sometimes we feel uncomfortable boarding an aircraft or sprint across a red light to catch the bus.

Companies cannot afford to act so erratically and sometimes irrationally. When it comes to business activities, a planned approach to risks is of essential importance. By its nature, any entrepreneurial decision involves risks: the expansion into China can go wrong, a new product can prove to be a flop and a personnel decision can turn out to be a mistake. Each decision should therefore be preceded by a risk-benefits analysis which allows one to assess whether the benefit, i.e. the anticipated profit, outweighs the residual risk. In purely arithmetical terms, then, a risk is at a tolerable level if the costs of further minimising it would exceed the costs to be expected if the risk were to be realised.

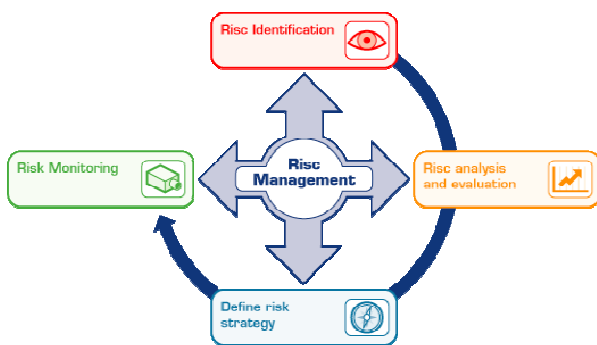


Figure 2: The risk management process

IT AS A RISK FACTOR

Before it can approach risks in a planned way, a company must determine the total extent of all risks, i.e. the overall risk. To do this, the risk is subjected to a standardised procedure: first it is identified, then analysed and evaluated, addressed and finally kept under control. Management are only slowly coming to appreciate that the entire complex of the information technology being used must be included in this risk-aggregation process. In the past, when it came to IT it was above all the risk factors "failure" and "data protection" which were considered, and measures for improving these introduced. Nowadays, measures for authorisation (access control, identity management), data back-up or protection of hardware (e.g. through redundant data centres,

climate control, no-break power supplies etc.) are regarded as common sense.

However, the actual risks go far beyond these: within a company, unclearly defined areas of responsibility or communication channels can lead to problems just as much as failure to comply with legal requirements or poor documentation. The heterogeneity of the IT landscape can present problems, the same goes for unsecured software and hardware. Other sources of danger include outdated applications with poor or inadequate documentation (especially mainframe solutions which may be decades old) or lack of adaptability or incompatibility. For a company, these can have serious consequences, ranging from the loss or manipulation of important data or unreliable or untimely availability up to the failure of systems required for operational business.

One risk which is often not recognised and which is therefore not safeguarded against involves the process chains which run in the background of any organisation and which have evolved over a period of years or decades in virtually all companies. Nowadays, most of these process chains take place fully automatically and control enterprise-wide processes, for example in SAP. Due to the increasing automation and linking of processes, the persons responsible often no longer even know which steps are followed and how the results come about. Nor is this a problem, as long as everything runs smoothly – however, it does become a problem when a complex process chain grinds to a halt for one reason or another. One example from the financial sector involves the preparation of annual insurance statements. In some cases this involves processing thousands of individual jobs/processes before the statements are finally printed out. To make things more difficult, automated processes frequently still require manual interventions which in turn often cannot be traced. In practical terms this means that, if the worst happens, it is very difficult to identify the source of errors. In particular, it is hard to localise the source of an error where interdependencies exist between individual processes. A central process management product makes it easier to maintain an overview of the interdependencies between the processes.

BENEFITS OF AUTOMATION FOR IT RISK MANAGEMENT

In addition to the general advantages of automation, it is also an important foundation for IT risk management. Automation increases reliability and thus significantly reduces various forms of risks. Used properly, it always serves to save on costs. Optimised processes make better use of hardware resources, so that new acquisitions can be avoided, or at least deferred. Companies can get by for longer with the existing resources because idle time, e.g. when waiting for user entries, does not occur.

Surveys repeatedly show that more than half of the IT budget is spent on current operation. These high operating costs act as a brake on innovation for IT, and thus for the entire company. Automation reduces operating costs, since fewer personnel are required for routine activities and better use is made of the existing infrastructure. The costs saved through automation are available for innovative projects. The risk for the company as a whole of missing out on current market developments due to outdated IT systems is reduced.

Better use of resources and optimised processes reduce overall processing time. This significantly reduces the risk of delays. As a rule, the results are available sooner. The management can respond more quickly to developments, and invoices can be sent off earlier – a direct financial advantage resulting from automation.

Other advantages include the optimisation of all processes and an increase in the reliability of processing. This means that the risk of infringing Service Level Agreements can be drastically reduced.

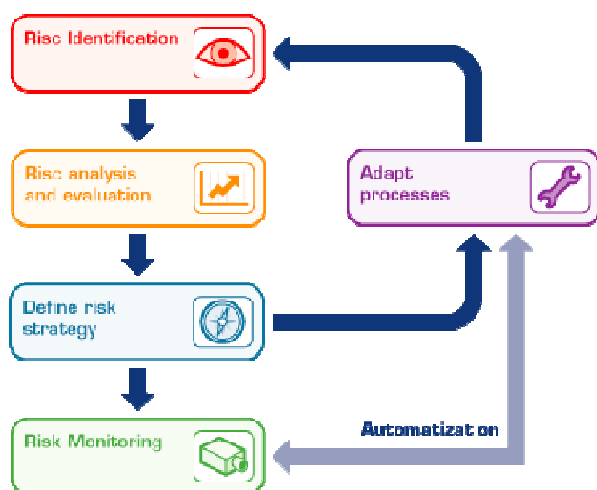


Figure 3: Possibilities offered by automation in IT risk management

TRUST IS GOOD, CONTROL IS BETTER

However, automation doesn't only bring advantages in terms of process control. It also contributes significantly to increasing efficiency in terms of controls. As early as 1998, the IT Governance Institute (www.itgi.org) was founded in order to foster "the development of international ideas and standards for the administration and control of internal information systems within companies. According to the Institute, effective control of IT systems contributes to "realising business objectives with the support of IT, deriving the full benefits from IT investments and managing IT-specific risks and opportunities". Within the context of enterprise-wide IT Governance strategies, the aspect of IT risk management is continually gaining in importance. IT Governance views a company's IT from a process perspective and governs the company management's measures for the organisation, steering and control of IT as well as the consistent alignment of the IT process to the company's strategy (IT Alignment).

This is necessary because information plays an increasingly important role, which means that IT processes represent a significant success or failure factor. As a first step towards setting up an enterprise-wide IT risk management, the best method for the company in question needs to be selected. Proven standards for the implementation of IT Governance are "Best Practice" methods such as ITIL (IT Infrastructure Library) or Cobit (Control Objectives for Information and Related Technology). ITIL describes the processes on which IT operations are based. These are oriented not around the technology, but the services provided. Cobit, in contrast, divides the functions of IT into processes and control objectives. It thus defines not the way a process is implemented, but simply the objective of a process.

IT Governance must maintain the balance between risk and performance. A succession of new laws and regulations require measures to minimise the risk, while increasing competitive pressure necessitates an increase in the efficiency of an organisation. Within this complex of priorities, the company's management must ensure that the IT processes are at least as clearly defined, transparent and measurable as each individual step of a modern production plant. Control systems must ensure that IT is not a "black box".

AVOIDING RISKS THROUGH AUTOMATED CONTROLS

Automated process management also includes automatic documentation of all processes which take place, an important prerequisite for later controls and audits. Another aspect of risk management is the computer-controlled performance of controls. Application settings, processes, log files etc. can be checked automatically for risk factors. These processes are easier to keep track of.

Any risk management strategy requires corresponding control mechanisms which allow risks to be identified and avoided in good time. The controls usually take the form that a report is generated, and the resulting list checked manually. This check is documented manually and filed. In most cases this form of control must be restricted to the checking of random samples in order to keep costs as low as possible. These controls take place at intervals of weeks or even months; after all each check takes up a certain amount of working time. Automation thus makes possible more exact checking at lower costs. The advantage of automated controls lies in their efficiency.

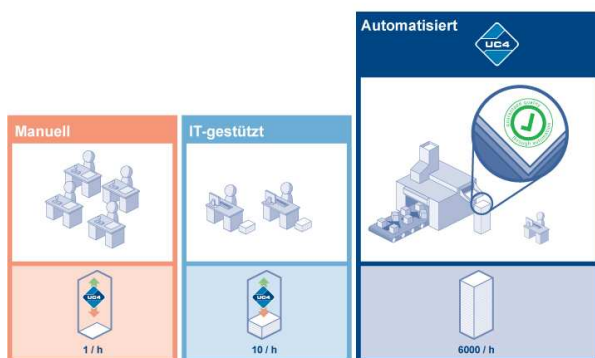


Figure 4: Increase in efficiency through automation

MORE EXACT CHECKING

Automated controls don't take up any working time. If computing time is available, the controls can be significantly more detailed without causing additional costs.

GREATER NUMBER OF RANDOM SAMPLES

The number of random samples can be significantly increased through automation; even 100% checking is possible.

GREATER DEPTH OF CHECKING

Naturally, automation also makes a greater depth of checking possible.

CHECK MORE OFTEN

If controls are carried out automatically, these can take place significantly more often, namely whenever resources are available. In most cases these controls are not particularly time-critical, and can therefore take place in the early hours of the morning without any problem.

UP-TO-DATE CHECKING

In most cases, manual controls cannot be carried out at any time. Organisational prerequisites are often lacking, operational activities usually have priority. Automated controls can be carried out at virtually any time, as long as sufficient computing resources are available. This means that risks are identified earlier and more quickly, because naturally an identified risk leads to immediate reporting to the person responsible for the process.

AUTOMATIC DOCUMENTING

A significant share of the work involved in risk management relates to the documentation of controls which have been carried out. A precise documentation must be kept of which random samples are selected, how the control was carried out and what the result looks like. This documentation must then be stored in an audit-proof way and kept for several years.

NO WORKLOAD

If the controls are automated, the workload involved in documentation is saved. The automation solutions from UC4 Software automatically keep records of the controls, including their performance and the result. An archiving tool which is included can be used to archive this data automatically for long-term storage. The process documentation complies with the requirements of the Sarbanes-Oxley Act.

ACTING IN COMPLIANCE WITH THE LAW AND WITH THE RULES

The list of laws and rules which a company has to comply with in terms of its IT processes is a long one: it starts with the perfectly normal requirements of record-keeping and due care in accounting, which in Germany are set forth in the Commercial Code (quite similar legal texts exist in Austria and Switzerland). According to this, all documentation must, for example, be kept for seven years. Against the background of spectacular accounting scandals involving companies such as Enron or Worldcom, the Sarbanes-Oxley Act (SOX) was passed in the USA in 2002, which defines requirements in relation to corporate reporting. The law applies, without exception, to all companies listed in the

USA, as well as their subsidiaries, including those in the EU.

Of particular interest is Section 404, according to which each annual financial statement must include an assessment of the effectiveness of the internal control system by the management as well as an auditor's certification to this effect. This means that the management assume responsibility for the effectiveness of the internal control systems, and this also includes the IT systems used in the presentation of accounts. SOX has huge implications in terms of IT, because its implementation requires the implementation, documentation and checking of control mechanisms. It will not be long before similar regulations are introduced in the EU.

In Germany, the "Law on Control and Transparency within the Corporate Sector", or KonTraG for short, was passed in 1998 in order to improve corporate governance in German companies. This primarily makes more precise and extends regulations under the Commercial Code and Companies Act. In particular, the liability of the management board, supervisory board and auditors within companies was extended. Company managements are practically forced to introduce and operate a company-wide risk early-warning system, and to publish statements on risks and risk structure in the situation report of the annual financial statements. In Germany, the "basic principles governing data access and the auditability of digital documents" (AO §147/ GdPDU) are regulated in the Fiscal Code (AO). The revenue authorities' auditors can cite these paragraphs if they wish to access a company's computer systems during a company audit.

The existence and functioning for a company-wide risk management system is also examined when it comes to ratings, which the banks have to carry out according to Basel II. The available financial resources of a company can thus depend on an appropriate and comprehensive risk management system which also covers IT. Companies' IT systems will become increasingly transparent to the control authorities, and it is vital that they should also be so to those responsible within the company. Control software for the entire infrastructure helps those responsible achieve this. With their products, UC4 Software offer continuous IT process automation with maximum transparency and flexibility. Automation reduces the risk of errors and failures in the area of IT-based business processes. An important contribution to risk management.

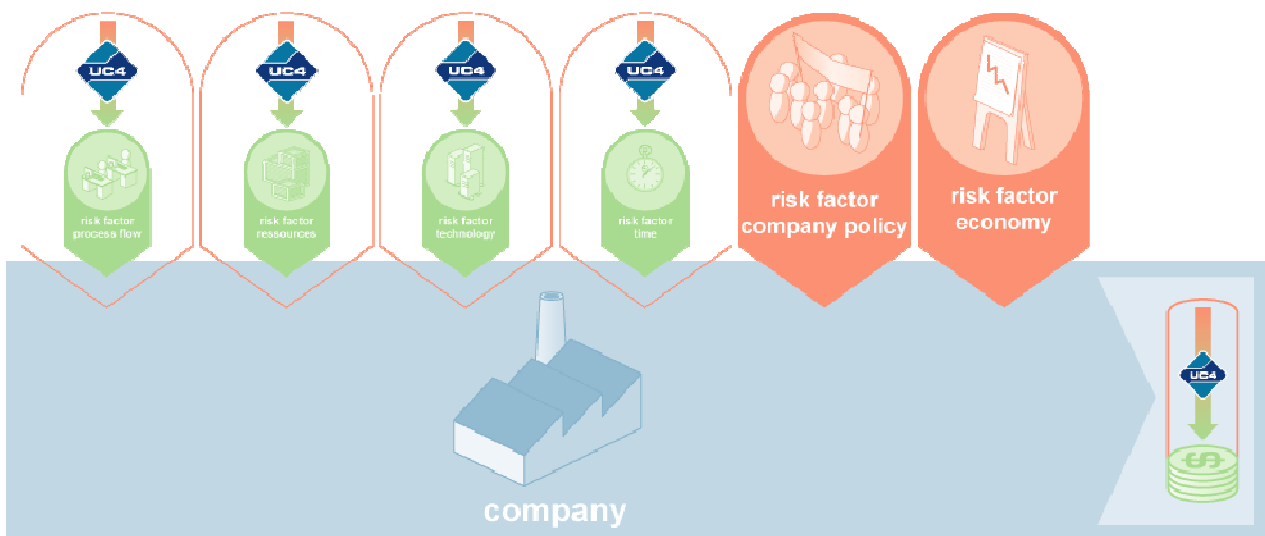


Figure 5: Avoiding risk through the use of UC4 automation solutions