

### Title of Paper

# Flirting with Disaster or How Can Cruise Ships Affect Your IT Risk Management

---

### Presenter

Hans G. Siebert, Product Manager, TÜV Informationstechnik GmbH (D)

---

### Instructional Skill Level

Introductory     Intermediate     Advanced

---

### Target Group

CEOs, CIOs, Risk Managers

---

### Keywords

- Risk Management
  - Quality Management
  - Compliance
  - IT Governance
- 

### Abstract

#### Background

Today, nearly all business processes, activities and decisions in companies require support from IT systems and communication infrastructure. Therefore availability and reliability of these IT systems are much more important than a few years ago. Even short breakdowns or malfunctions of IT systems can cause severe damage to companies or in the worst case cause bankruptcy.

#### IT-Disasters

In November 2006, a famous shipyard in the northern area of Germany performed the transfer of a big cruise ship to the Northern Sea via a small river. During this transfer a planned circuit breaking caused a power blackout in big areas of Western Europe.

Suddenly, everybody who has to take care of redundant power supply for important technical equipment realized that such a wide-ranging power disaster could severely put a new risk on every disaster recovery (and business continuity) plans.

This disaster might seem a little bit „exotic“ but it really happened and everybody who runs one or more data centers has to take care how to avoid damages for companies even in such rare cases.

#### How important is IT for your company? Is this only a problem for big companies?

The worst case disaster in IT is the complete outage of a data center and its offered services for a longer time. To speak of „data centers“ might imply that this might be only a problem for big companies with mainframes but this is not true. Even if your „data center“ consists only of a room with one

---

---

server or only of one PC alone you have to think about it what would happen if your „data center“ had a blackout.

The size of your „data center“ or the size of your company doesn't really matter. Critical is how important a running IT is for your business. The investment in disaster recovery and business continuity depends on the risks and costs you would have in case your „data center“ has a complete blackout.

### **IT risk management: Do we really need more than a reliable data backup?**

In many companies data backup (and restore!) and data archiving are the only processes to take care of IT risks but these are not enough. You have to start risk management (RM) by checking which risks exist and then take care of the most important ones at first. Otherwise you might improve a lesser important weakness and a big risk remains in place.

### **Some examples from everyday life (neither complete nor representative)**

Some examples from everyday life shall give an impression of possible challenges

- Important data were accidentally deleted?  
*No problem, we could restore all data from our backup.*
- A crash of a hard disk?  
*No problem, too. We backup all data at regular intervals.*
- Eight year old files of engineering data are required in a legal procedure?  
*Hm, back in those days we had this other backup system (what was its name?) with its own file format. I hope someone could still read those cartridges?*
- A fired employee changed important company data during the last 12 months?  
*Hm, until now that never happened in our company. Would be unpleasant.*
- In a small but important part of the company, a very „optimized“ software code is used for production control. The only one who could handle this code is Mr. Mayer who soon will be retired.  
*Well, we have such a case, too. Could be a real problem if something happened to his man.*
- Due to an error in reasoning, backup procedures in a company worked only for the user hard disks but not for the system disks. But an important data base stored its data only on a system disk. The error was detected after a severe data loss when data backup was tried in vain.  
*Oh oh, poor admin!*
- The server room burnt down completely?  
*No problem, this is fully covered by insurance. We have only to buy new hardware, make the operation systems running, the database running and all other software running, configure them properly, restore all data, look whether everything works fine...  
Hm hm we never tested this completely. I think we would need some time to recover completely. Should not happen! Would cause some problems.*
- A serious fire destroyed your data center. Your backup data center in the same area is also affected?  
*This would be a real disaster! How could we provide for such a risk? There must be a limit for this. Should we take care of a meteor impact?*
- During the transfer of a big cruise ship to the Northern Sea via a small river in Northern Germany a planned circuit breaking caused a power blackout in big areas of Western Europe.  
*Hard to believe! Wide area power blackouts might happen elsewhere but not here!!*
- Due to very exotic weather conditions in winter (a once in a century event) nearly all power poles in a wide area were destroyed. Some towns remained without power for a week.  
*Hm, hm, I heard about this. It was near the city of Münster, wasn't it? Would be very unpleasant. One week? Our uninterruptible power supply (UPS) would not last that long!*
- Due to an epidemic 60% of your employees could not work for several weeks. Because you

---

offer services, you make only money, when your employees could work. Soon you would run into liquidity problems.

*Hm hm, we thought about bird flu, too, but nothing happened after that. If this happened we would not be the only ones who were affected (but would that help us?).*

If you recognize your company in one or more of the examples above, maybe you should think about RM in another way than in the past.

### **One of the major risks: contingency plans not tested!**

A lot of companies do not have any contingency plans. It is strange to see, that a lot of companies have contingency plans but never really had the heart to test the expensive parts of them: "To shut down our data center merely for a test? You're surely joking?"

Obviously there are financial and other limitations to the testing of major disasters but they should be checked very carefully. Especially if it is impossible to test them in real life you should think about to simulate contingency plans as good as possible.

### **Risk management: top priority!**

(Strictly speaking, the following statements are valid only for German law (i.e. KonTraG). But a lot of other countries have similar regulations, i.e. SOX in USA, J-SOX in Japan)

The top management of a company (§ 43 GmbHG, § 93 AktG) is responsible to implement a RM to prevent business risks. According to a famous verdict (ARAG) from the German Federal Court of Justice (BGH) top management is liable in case of an act of gross negligence

- personal (!)
- unlimited (!) and
- with private property (!)

Directors & Officers insurances (D&O) were made for such "accidents" in USA and became very popular in Germany, too.

### **Do you know your business?**

RM tries to handle incidents and risks that endanger a company to reach its major goals. To do so you have to know the major goals of your company. In most cases that are not the goals you find in the corresponding chapters of your quality manual! You need to know the most important processes of your company and your business. When you know them the most important risks are the ones which endanger your most important processes. Everybody knows them? No!

Top management is responsible for RM but only employees know some of the major risks. So RM should include them in the risk finding processes.

### **An example of bad practice!**

RM is required by law and an essential process within a company. To establish RM processes only in a formal way is wide spread but not very helpful: "RM time again? Miss Schlusser, please print the Excel file with the list of risks from last year and update the year!"

RM should be seen as a chance to improve your company. Otherwise you have a bad ratio between costs and benefits. This often happens when a company approaches a formal process model in a wrong way.

### **Sense (and nonsense) of formal QM or RM systems**

One major task of a formal process model like RM or QM is to reduce the dependency of processes from individual human beings and to gain a standardized, repeatable level of quality. This could only be achieved when a RM works effectively.

---

---

If top management does not stand behind RM, you will lose effectiveness: "A RM manual? Of course we do have it. Do we act according to it? Well, it is okay; we pass the yearly audits!"

Process models usually try to define the minimal effort to reach a certain goal. You could also do too much of a good thing. In some companies the "continuous improvement process" is so extensive that the employees cannot see the benefits of it any more. That is the worst case. If the employees do not support those systems they could only fail or have a bad ratio between costs and benefits.

### **Can you outsource risks? Or do you create new risks?**

The above mentioned risks cannot be minimized via outsourcing. A lot of companies paid much money in the last years for gaining this experience. To outsource certain processes effectively and efficiently you must know those processes, their risks and their critical success factors very well. You must do your homework before you can outsource something. Then you can define the interfaces precisely and negotiate service level agreements successfully. Otherwise you create new risks and do not solve any of the old ones.

### **State of the art RM?**

The presentation will describe approaches which work in certain environments

- ISO 20000 (ITIL, IT services)
- ISO 27000 (security management)
- BSI baseline protection, especially BSI-100-4 (to be published)
- TSI (requirements for data centers with high availability).

---

### **Biography**

Short description Dipl.-Phys. Hans G. Siebert

Born 1954, studied physics and computer science at Dortmund university, several years software development, headed 10 years development of complex software systems. DEKIZ assessor in the area of „CAD/CAM interfaces“, responsible for the accreditation (first worldwide) of the usability-Labor of TÜV Informationstechnik GmbH (TÜViT) according to ISO 9241. Several Management functions within TÜViT. Today product manager at TÜViT, responsible for IT Governance in the division project & quality management. Leader of working committee „Software Quality Management“ in the German BITKOM.

---

### **Contact information of Presenter**

Hans G. Siebert  
TÜV Informationstechnik GmbH  
Langemarckstr. 20  
45141 Essen  
Germany

E-Mail: [h.siebert@tuvit.de](mailto:h.siebert@tuvit.de)  
Phone: +49 201 8999 420  
Fax: +49 201 8999 666  
Mobile: +49 160 8885 420  
URL: [www.tuvit.de](http://www.tuvit.de)

---