BENEFITS OF REGULATORY REQUIREMENTS WITH RESPECT TO BUSINESS OPTIMIZATION

An IT-Infrastructure Compliance Maturity Model for Management, Compliance and IT Stakeholders

Michael Kranawetter
Chief Security Advisor
Microsoft Deutschland GmbH

This White Paper is for informational purposes only.
MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The conclusions on views expressed by decision makers on the German market are based on the results of the Experton Group analysis and incumbent on the Experton Group. The information and data contained in this document were researched with diligence and care; despite this no guarantees can be given for the accuracy or completeness of any information presented in it. All rights relating to the content of the survey are reserved by Experton Group AG. For data protection reasons, the data and information shall remain the property of Experton Group AG.

Citations, in part or full, must include a reference to the source.

PROLOG

Dear Reader,

I am asked time and time again by security decision makers how to handle the subject of “compliance.” But this question automatically raises a number of additional issues; why is this subject relevant to a security expert? What kind of “compliance” are we talking about? How relevant is the subject? How much will it cost (cost of compliance)?
And the question that towers above all others right from the outset is:

How do I get started with this topic?

Of course, there is a great deal of compliance literature, but in most cases it fails to propose a solution, and instead simply structures familiar requirements in different ways.

As a leading supplier of software solutions, we appreciate that our responsibility goes farther than simply providing products, it includes supporting you in the implementation of IT compliance requirements. In this context we see three aspects that – above all others – put us as a solution provider in a position to help you. For one thing, more or less all business processes are based on IT systems; all the more reason to use electronic means to ensure the effectiveness of internal control systems; for another, automation – the elementary objective of IT – helps to expedite measures, guaranteeing reproducibility and traceability. On top of this “compliance” can be integrated with IT handling to prompt for and fulfill requirements at the workplace, more or less without any active interaction, that is, IT can be set up to be compliant and autonomous (compliance at the desk). After all, the required information is immanently and inherently available on the system.

This document thus describes an approach that – like the Pareto principle – takes the phenomenon of distribution of effort into account. Keeping track of the fundamental issues and focusing on solving those takes us far closer to our goal – compliance.

The focus here will be on aspects of infrastructure compliance, which are naturally very closely linked to the topics of availability, trust, and integrity, and thus build a bridge to information security.

Does this mean that the document is for security experts only?
On the contrary: At the end of the day, the aim is to create a communications basis for mutual understanding that allows the reader to gain a foothold in the field of compliance at various levels and from various viewpoints using a variety of approaches.

The document can thus be read by managers, technical decision makers and IT experts alike. Start where you feel most at home.

Your

Michael Kranawetter

DR. CHRISTOPH CAPELLARO

In recent years and months, legal requirements have played an increasingly important role for businesses. Lawmakers at national, European and international levels aim to introduce mandatory standards for risk management in enterprises to help introduce enterprise-wide systems to manage these risks and to define internal and external reporting on the effectiveness of the control systems in question. The most famous examples are, of course, the Sarbanes Oxley Act (SOX), the Basel II Accord in the European Union, which applies to financial institutions and Germany's German Accounting Law Modernization Act (BilMoG), which implements the 8th EU Directive, also known as Euro SOX. The question of adhering to these legal requirements – commonly referred to as compliance – is becoming increasingly challenging for businesses.

In the context of compliance, IT plays a critical role in the enterprise. The close tie-in between IT and critical business processes that the majority of today's businesses has achieved, makes it possible to define workflows in a way that controlling tasks, such as approval processes, can be automated. On top of this, IT makes it possible to automatically collect and prepare relevant data for individual business cases, thus ensuring compliance with disclosure requirements. That this kind of automation puts businesses in a position to leverage huge potential savings is also evidenced by experiences with SOX. The tests required for controlling, such as compliance with change management rules, were originally implemented manually and involved considerable overhead; today, it is not uncommon to find them efficiently implemented in the form of permissions, mandatory system workflows and automated reporting. After all, data processing itself is subject to legal and regulatory requirements that are becoming increasingly strict. Data protection, or the fundamental principles of data access, and verifiability of digital documents (GDPdU) which, among other things, govern electronic access to digital data by the fiscal authorities , are just a few examples.

The developments that IT has gone through in the enterprise in recent decades are logical, but nonetheless remarkable for that fact. In the early days, the company IT department would tend to organize itself autonomously for the most part. IT had to work, and how the IT department made sure this happened was only the IT department's business. Increasing interdependence of IT and business processes later led to the rise of the service concept. The IT department mutated into an internal (and later an external) service provider. This process was accompanied by IT service definitions and the introduction of IT processes. Subjecting IT to regulatory controls was a test of IT's maturity. As an established division of the enterprise IT is subject to the same legal requirements as, say, accounting or human resources.

Understanding the regulatory environment is both a challenge and an opportunity for IT. Because it is closely tied in with business processes, IT-supported automation of controls is a logical solution. This adds value to the role of IT throughout the enterprise. IT is becoming a compliance enabler and the IT department is slowly changing from a service provider for other divisions of the company to a key function within the enterprise; a function that is subject to similar regulatory requirements, and internal and external audits as, say, accounts or human resources.

Considering the special role of IT in compliance with regulatory requirements, I sincerely hope that reading this document gives you interesting and new insights.

Dr. Christoph Capellaro has been working at Ernst & Young's Munich office since 1999. He is responsible for IT security services for Germany, Austria and Switzerland within the Technology & Security Risk Services department. The focus of these services is on auditing and consulting in all areas of secure IT deployment, paying special attention to equal weighting of legal, business and technical aspects. Dr. Capellaro manages key accounts from the private and public sectors for clients who give high priority to IT security because of their involvement in international transactions, because they are responsible for critical data processing processes, handle sensitive information, or are subject to strict regulatory controls. Dr. Capellaro is a Certified Information Security Manager (CISM), certified WebTrust auditor, basic protection auditor, ITIL Foundation certified, and an officially recognized data protection consultant. In nearly 20 years of working in IT security Dr. Capellaro has registered several patents, held many keynotes at various conferences, published articles in professional journals and contributed to three books.

DR. JYN SCHULTZE-MELLING LL.M.

What compliance means, in a nutshell, is adhering to pertinent legal and regulatory imperatives and prohibitions. However, this view ignores the enormous complexity of the challenge that enterprises face in dealing with compliance today, particularly in the context of IT deployment. It starts with the question of pertinent jurisdiction; after all, if you do not know what is expected of you, you can't fulfill the expectations. Although this sounds simple, it is typically the first major problem in daily business: Correctly identifying actual and pertinent legal and regulatory requirements for an enterprise is highly complex and it takes just as much legal and technical expertise as it does insider knowledge of the industry. The material becomes all the more complex if you take a broader perspective. Even in a purely European business environment compliance is not exactly characterized by clarity. And if you need to consider additional jurisdictions, such as those of the U.S. or the emergency economies of central and Eastern Europe, the risk of losing track increases. This, in turn, not only entails considerable financial risk and business disadvantages for the company, it can also expose the board and management to criminal prosecution.

This said, full identification of the given requirements often leads to the realization that the overhead involved in ensuring total compliance is grossly disproportionate to the resources planned or available for the task. On top of this, some IT compliance requirements are contradictory, or at least cause enormous implementation problems from a technical point of view. In these cases, companies need professional IT compliance and risk management that not only identifies the legal and regulatory requirements the company faces, but evaluates them with respect to their tangible and practical significance. When prioritizing the corresponding technical and organizational measures, the possible legal and practical damage potential plays an equally decisive role as the multifaceted benefits and opportunities that a professionally oriented IT compliance strategy implemented in a targeted manner can offer.

People who not only know what is expected of them, and what tangible benefits this offers, but also what is likely to happen if worst comes to worst, are likely to find it far easier to plan the next steps and establish compliant and audit-proof IT. However, the first and at the same time most difficult step is that of actually concerning oneself with the topic in a serious way. The white paper that you now hold in your hands provides an excellent basis for this. I sincerely hope that you benefit from reading it, and that it in turn helps you to successfully plan your IT compliance structures and strategies.

Dr. Jyn Schultze-Melling LL.M. is a specialist for IT compliance at the Munich office of the international corporate lawyers Nörr Stiefenhofer Lutz where he advises key accounts from the public sector, large corporate accounts and global companies in questions of IT, data protection and data security law. The focus of his work is strategic development of IT compliance models for global players. He regularly contributes to and publishes in professional and trade journals on the topic of IT compliance and other IT-related legal topics. On top of that, Dr. Schultze-Melling is the chief legal officer with the Kompetenzzentrum für Sicherheit (Competence Center for Security KoSiB e.G.), a tutor with Deutsche Anwaltakademie (German Lawyers' Academy - DAA) where he teaches IT law to ongoing specialist lawyers, a lecturer at the University of Passau, and an active member of various societies and associations, in particular the Deutschen Gesellschaft für Recht und Informatik (German Society for Law and Informatics - DGRI), the Arbeitsgruppe IT-Recht des Deutschen Anwaltsvereins (IT law working group within the Association of German Lawyers - DAVIT), the Gesellschaft für Informatik (Informatics Society - GI), and the International Association of Privacy Professionals (IAPP).

PROF. DR. MICHAEL KLOTZ

This document does an excellent job of demonstrating the benefits that IT compliance can hold for a business. To this end, the authors translate the business-oriented goals of protection, availability, traceability, transparency and due diligence into correlating fields of action (information protection, risk management, information management, internal control systems and duties to cooperate and disclose). More than anything else, the fact that the document integrates these five areas to create a maturity model proves to be highly relevant and actionable in practical applications as the systematic view reveals a path of ongoing improvement. The interactive approach with respect to the fields of risk, incident, problem, configuration and change management is also eminently suited to releasing IT compliance from its current wallflower existence. Detailed explanations provide extremely useful guidelines for anyone working in enterprise data processing.

Prof. Dr. Michael Klotz, born 1960 in Berlin, studied Economics at the Technical University of Berlin, with a degree in Business Management; more than ten years of various positions with IT consulting and sales companies as a management consultant, project manager and CEO; since 1999 at the FH Stralsund as Professor for Information Management, Enterprise Organization and Data Processing; since 2008 Head of – the Stralsund Information Management Team – (SIMAT); numerous publications on information management, IT governance and IT compliance; member of the ISACA scientific council; co-publisher of “IT-Governance” since 2007.

TABLE OF CONTENTS

EXECUTIVE SUMMARY 13-14
1. COMPLIANCE IN THE YEAR 2009 16-18
2. SUCCESSFUL ENTERPRISE MANAGEMENT? STRUCTURED! 22-25
3. PLAYING BY THE RULES? MAKE THE MOST OF IT! 28-34
4. WHAT DO I NEED TO FOCUS ON? KEY ISSUES! 38-40
5. AND NOW THE SOLUTION 43-50
6. QUO ESQUE QUO VADIS? COMPLIANCE, IMPLEMENTATION 54-78
7. AUTHORS 80-80
8. COMPLIANCE RELEVANT IT INFRASTRUCTURE SOLUTIONS 81-83
9. IT GLOSSARY 84-85

CHAPTERS 1 + 2

are designed for all interested readers. They provide an overview of the compliance status quo in Germany and explain the links between governance, risk management and compliance (GRC).

CHAPTER 3

This chapter is mainly designed for management. It reveals collates and details the mutual objectives of regulatory and business requirements.

CHAPTER 4

This chapter is designed for technical decision makers.
It focuses on a description of five key areas of compliance implementation.

CHAPTER 5

This chapter mainly addresses IT experts, but also technical decision makers interested in more detail. Chapter 5 gives a detailed description of the tangible implementation of regulatory requirements by means of IT controls.

CHAPTER 6

Chapter 6 explains the IT compliance infrastructure maturity model. Thanks to this overview, each target group can evaluate its own position and develop a strategy to ensure appropriate ongoing development. A case study will help to present the material in a plausible way.

CHAPTER 1

EXECUTIVE SUMMARY

1. COMPLIANCE IN THE YEAR 2009

EXECUTIVE SUMMARY

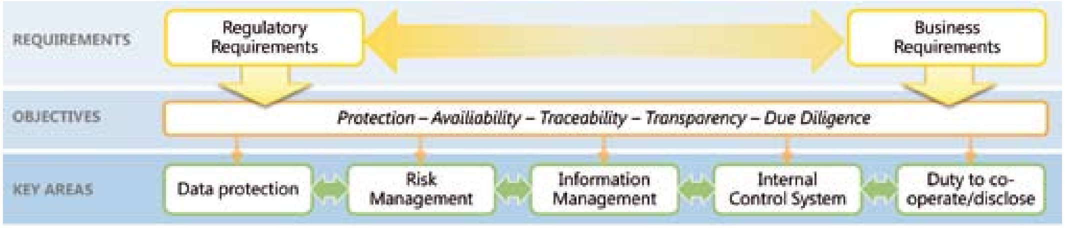
Compliance as the driving force behind a dynamic IT infrastructure

The need for action in the implementation of compliance requirements continues to grow inexorably. A survey of German companies performed by the Experton Group and commissioned by Microsoft revealed that nearly 40 percent of all respondents are only moderately satisfied with this field. The results also show that dissatisfaction among IT decision makers tends to be higher than among business decision makers. Quite obviously, IT sees the need for compliance measures more clearly than management. This raises the question of what advantages and benefits compliance solutions can have for business decision makers.

The answer lies in solving this problem:
If regulatory requirements need to be implemented, how can I leverage this process to optimize business processes?

To be able to discuss this issue, all the stakeholders need to establish a **mutual language** and a **mutual understanding**. Every stakeholder needs to be aware of the aspects to be taken into consideration, how "must" and "can" are interrelated, and how to realize that "must" becomes a "plus".

IT INFRASTRUCTURE COMPLIANCE MATURITY MODEL



What steps do we need to take to achieve this objective?
To make things easier, we have developed an **IT infrastructure compliance model** unlike any previous model. It lowers the barriers for concerning oneself with such a complex topic and contributes towards a better understanding of compliance.

In this context it is important to realize that regulatory and business requirements – with respect to information – actually pursue five common goals: **protection, availability, traceability, transparency, and due diligence.** These objectives are based on legal and regulatory principles which we need to understand as they are the basis for the majority of rules in one form or another, although their character may differ from country to country, and from rule to rule.

Regulatory and business requirements are not necessarily contradictory. On the contrary: **Both can be traced back to common objectives and intentions.** Enterprises can use regulatory requirements as a starting point for leveraging synergies between mandatory duties and their own objectives.

IT can more easily attain business and regulatory targets and objectives via the following five key areas: **information protection, risk management, information management, internal controlling and duty to cooperate and disclose.**

These are the common grounds that arise from legal/regulatory and economic/business requirements.

An enterprise that is well positioned in these key areas will also find it easier to fulfill **future compliance requirements.** In other words, companies that focus on the five areas mentioned above actually use compliance to drive a dynamic IT infrastructure.

On top of this value is added to business requirements such as the ability to calculate and mitigate business and IT risks, fraud avoidance, improved efficiency and transparency thanks to the automation and optimization of processes, a boost to the image of the entire company, and last but not least, optimization of investments in protective measures.

Investigating the theory may help to develop a better understanding for the problem, however, implementation necessitates taking tangible steps that depend on the current situation. How can an enterprise evaluate its current compliance status and identify its objectives?

Our IT infrastructure compliance maturity model picks your company up wherever it is right now. It helps you identify the degree of maturity and to define measures to achieve better compliance maturity **and a more dynamic IT infrastructure.** The model shows you how to optimize your IT infrastructure in 19 fundamental solution areas. These areas derive from international and established IT standards and best practices.

Typically, this leads to a realization that implementation is possible based on the existing infrastructure.

Ascertaining its degree of maturity makes it easier for the company to identify its own status quo, and to identify and communicate its own risk situation. It adds visibility to the current status, and illustrates how an interdisciplinary cooperation between the stakeholders can lead to improvements.

The model discussed in this white paper explains in simple steps how to approach the subject of compliance and how to establish a mutual basis for communication. Obviously, a simplified model cannot hope to be exhaustive. However, the model will help to provide a basis for understanding compliance and its contribution to business optimization. Naturally, any in-depth evaluation will need to take the company‘s individual situation into account.

However, establishing the basis paves the way for a more granular adaptation.

1. COMPLIANCE IN THE YEAR 2009

Status quo of businesses, challenges for business and IT decision makers

2008 was the year in which the hype concerning compliance gradually gave way to a more sober discussion. While German companies now follow some regulations in a more or less consistent manner, others are only monitored, or totally ignored. Despite this, the number of regulations to be observed continues to grow. They range from compliance-related laws in the stricter sense of the word, standards, reference models and industry-specific requirements to internal enterprise policies. Global players are also facing country-specific regulations that are not necessarily harmonized even within the European Union.

An analysis, commissioned by Microsoft and performed by the Experton Group, of German IT and business decision makers in corporations with at least 1000 employees reveals that currently the Federal Data **Protection Act** (Bundesdatenschutzgesetz) or regulations imposed by individual federal states are primarily being implemented, followed by various commercial laws and internal standards, or non-binding standards such as the ISO 27001 standard and IT basic protection (IT-Grundschutz).

In contrast to this, **Basel II** contains specific requirements with respect to the management of operative risks which seem to make sense both from the perspective of the economy as a whole and from the perspective of the individual enterprise. In addition to this, bank credit ratings now take their customers' operative IT risks into consideration – with the potential consequence of more favorable lending terms for businesses with solid IT processes. However, a serious rating requires time-consuming IT and process audits. This has led to Basel II dropping off the roadmap of German businesses outside the finance industry. In practical terms, audits are more typically based on "checklists." However, the mere existence of, say, a virus scanner says nothing about a company's overall security status.

Companies really do face considerable challenges in implementing regulations. The Experton Group analysis reveals that user satisfaction with the implementation of compliance requirements by companies is "moderate." Almost 40 percent of respondents stated that they are moderately satisfied or tend to be unsatisfied as Figure 1 shows. IT decision makers tend to be less satisfied with the implementation of regulations in their fields than the management. Thus, considerable **scope for optimization and action** exists, especially in the field of IT.

Almost 40 percent of respondents are just moderately satisfied or even dissatisfied with the implementation of compliance in their companies.

"The need to act is obvious: Existing infrastructure and IT services and processes simply need to be optimized to reflect compliance requirements, but how? Chapters 4 and 5 give tangible recommendations and make the topic more accessible."

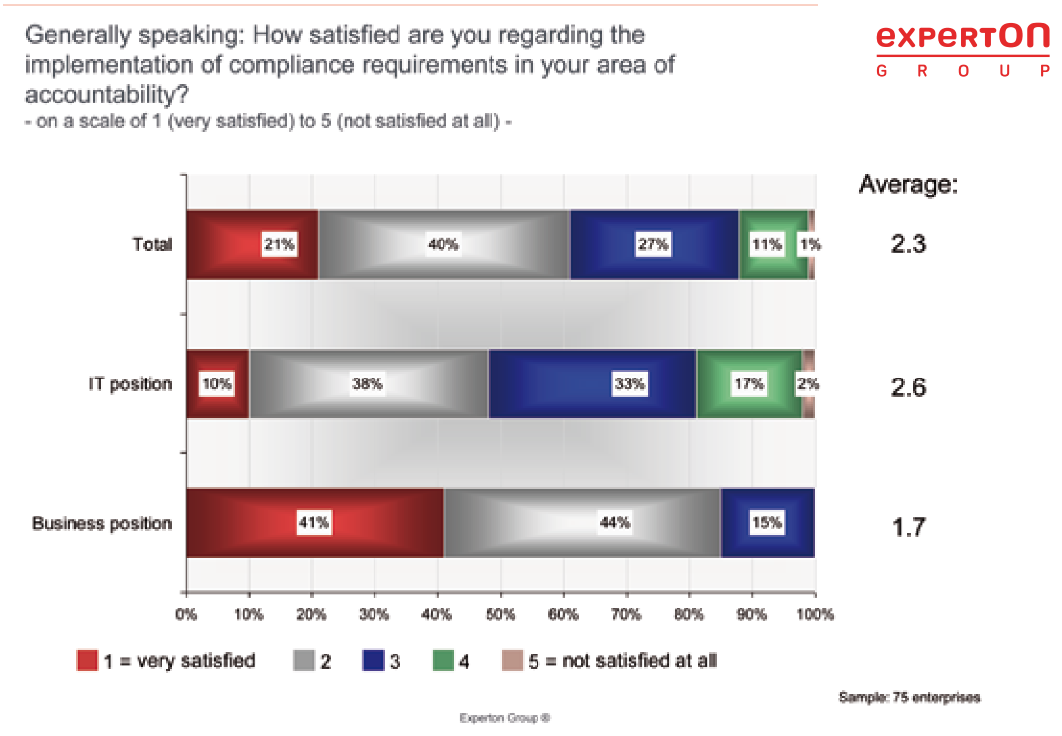


Figure 1 Experton Group survey: Satisfaction with the implementation of compliance requirements

Difficulties often occur in implementing regulatory requirements. For example, IT and business decision makers often complain that the **benefits** of implementing regulatory requirements are difficult to demonstrate and/or measure. Almost half of the companies surveyed by the Experton Group are of the opinion that this is an obstacle, or even a major obstacle. And threat-only scenarios in the sense of penalties and sanctions have little effect where individual enterprises anticipate only minor repercussions from external sources.

Must we therefore regard “compliance” as a “necessary evil”? By no means, because there are tangible **synergy effects** with general and pre-existing tasks in the field of enterprise management and information technology. Examples of this include:

- **ability to calculate and mitigate business and IT risks,**
- **avoidance of fraud,**
- **more efficiency and**
- **transparency**

thanks to the automation and optimization of processes and finally the

- **image of the company as a whole.**

In other words, it is a question of how best to **leverage the potential added value** in fulfilling regulatory requirements. One critical goal is that of resolving tension between business and IT management, risk management and regulatory requirements.

> *"The need to comply with regulatory requirements is often regarded as a necessary evil. However, it also offers opportunities. If companies are prepared to look beyond the box, they can actually benefit from this opportunity to optimize business processes."*

Decision makers at all levels must develop a **mutual understanding** of compliance. An ongoing flow of information based on comprehensible metrics between business decision makers (executive board, compliance stakeholders, divisions) on the one hand and IT decision makers on the other is a must. This necessitates **a communication platform** that enables all stakeholders to view the topic from different perspectives and discover possible solutions.

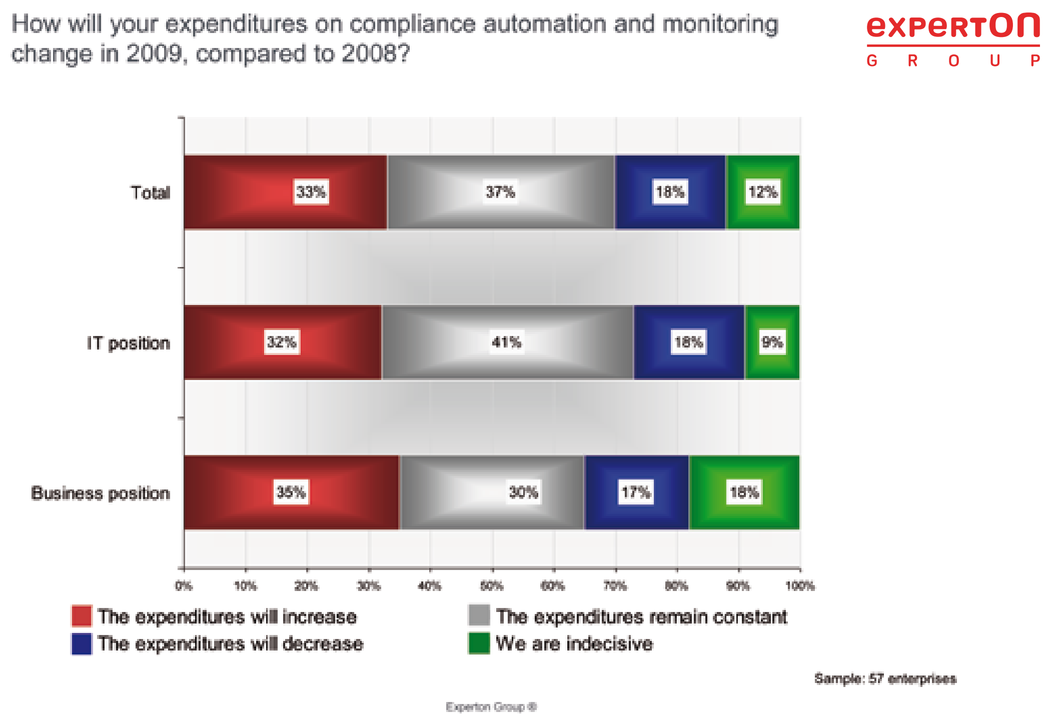


Figure 2: Development of expenditure on automation and monitoring of compliance targets

At the same time decision makers in IT, and even more so in management, anticipate rising or at least unchanged expenditure on the automation and monitoring of compliance targets in 2009 (see figure 2). Again, this shows the responsibility of IT. According to half of all respondents, investments are allocated to the IT budget. Only a few are prepared to allocate a dedicated compliance budget for this purpose. The others finance these sums from divisional budgets. By bundling and coordinating these enterprise-wide activities in the form of a **holistic approach** to governance, risk management and compliance (GRC) – thus identifying and analyzing common interests – an enterprise can achieve an optimum solution.

”This document offers more than a concise overview of the subject, it helps find a mutual communication platform and a simple approach model.“

CHAPTER 2

SUCCESSFUL ENTERPRISE MANAGEMENT? STRUCTURED!

2. SUCCESSFUL ENTERPRISE MANAGEMENT? STRUCTURED!

The role of governance, risk management and compliance (GRC)

Adherence to rules (compliance in the broader sense) is not an isolated measure but an integral part of the broader context of **governance, risk management and compliance.** GRC is the strategic bracket for a variety of tasks that bridges the gap between enterprise strategies and targets on the one hand, and the day-to-day operative business on the other. GRC is not a technology but an approach and a process that helps achieve synergies between enterprise targets and regulatory requirements.

Technologies give companies the ability to automate and implement some aspects of GRC. In information technology, many companies have already deployed stand-alone components suitable for GRC.

experton GROUP

"It is typically not necessary to completely redesign the IT infrastructure at the initial stage. On the contrary, existing components can typically be used. They simply need to be identified and, if needed, networked."

GRC OVERVIEW

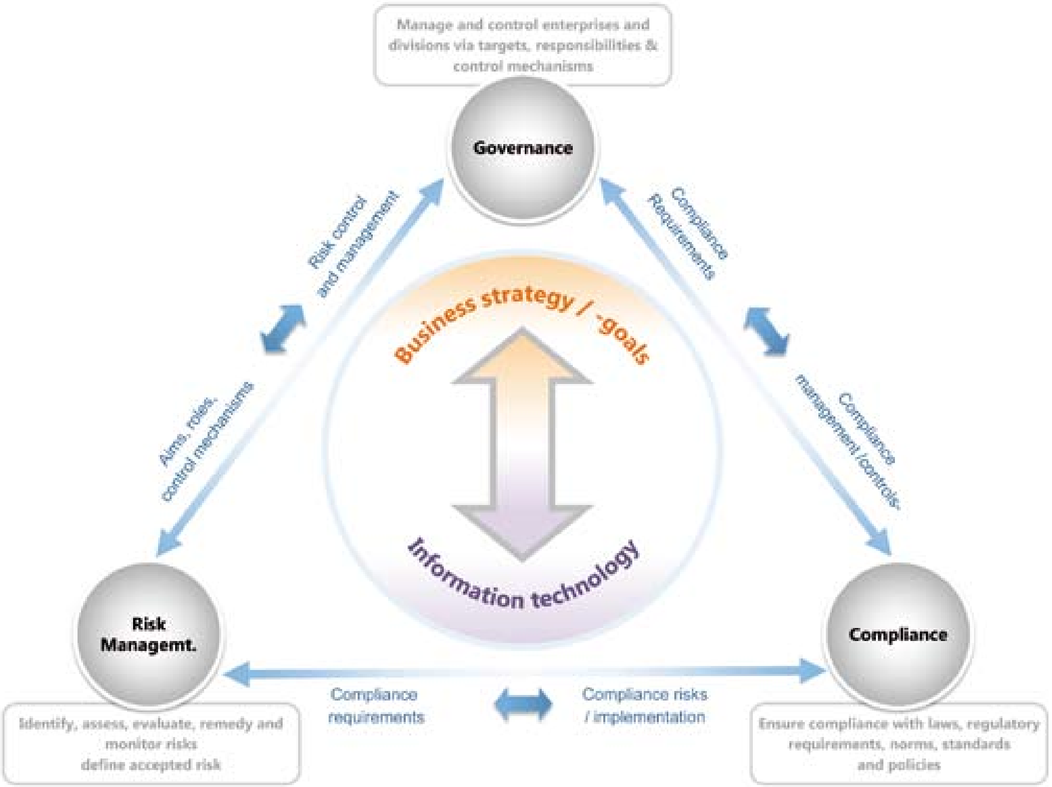

Manage and control enterprises and divisions via targets, responsibilities & control mechanisms
Governance
Risk control and management
Compliance Requirements
Business strategy / -goals
Aims, roles, control mechanisms
Compliance management /controls
Information technology
Risk Managemt.
Compliance
Compliance requirements
Compliance risks / implementation
Identify, assess, evaluate, remedy and monitor risks define accepted risk
Ensure compliance with laws, regulatory requirements, norms, standards and policies

Figure 3: Overview: Governance, Risk Management & Compliance

Governance is a generic term that refers to the responsible management of division within an enterprise, or the enterprise as a whole. This includes specifying targets and responsibilities, defining activities and controls, planning the use of resources and embedding this in a risk management process. Within the scope of controls at all levels, alignment of objectives with the enterprise strategy plays an important role – for example, in the area of IT governance.

Risk Management is a systematic approach and process for identifying, analyzing, evaluating, remedying and monitoring risks. One important objective of risk management is therefore understanding threats, vulnerabilities and risks for the enterprise and of mitigating risk, or deploying measures to help anticipating residual risks with as great a degree of accuracy as possible. The list of potential risk areas is long, starting with the safety of employees, buildings, production equipment and details of technology and project risks, through to risks in the field of compliance and criminality, ethics and culture, geopolitics and climate – just to name a few.

Compliance generally refers to activities to ensure that behavior complies with rules and thus to the provision of adequate tools to visualize the company‘s status. It is not just a question of complying with laws but also of adherence to the enterprise‘s own policies, which in turn can be based on best practices. This not only creates a code of behavior in the relation between business partners – serving to establish trust in business relationships – but also in customer relations.

"An enterprise that is well positioned with respect to GRC…

- *…improves the efficiency and effectiveness of organizational and technical processes*
- *…protects the company's image and assets*
- *…ensures transparency vis-à-vis external third parties such as investors, analysts, law makers, regulatory authorities, customers and employees*
- *…demonstrates responsibility for its staff and towards society*
- *…is better prepared for crises and disaster recovery*
- *…is better equipped to guarantee the security of enterprise and customer-related data*
- *…mitigates the risk of fraud."*

"How are compliance and business requirements related? Chapter 3 investigates the common denominators. This is followed by tangible implementation from the viewpoint of the business decision maker (Chapter 3) or IT stakeholders (Chapter 4)."

CHAPTER 3

PLAYING BY THE RULES?
MAKE THE MOST OF IT!

3. PLAYING BY THE RULES? MAKE THE MOST OF IT!

Synergies between business requirements and regulatory targets

Regulatory and business targets can be traced back to mutual intentions.

Regulatory and business requirements are not contradictory. On the contrary: Regulatory and business targets can be traced back to mutual intentions. If you look closely at the legal situation, you will come to the conclusion that certain topics keep on reoccurring. And from this coherent objectives can be identified. For example, when legislators refer to data protection, a company understands it to mean protection against fraud and industrial espionage, or maintaining a good image.

If one compares the intention of regulatory requirements with the motivations of business requirements the following objectives emerge: **protection, availability, traceability, transparency and due diligence,** relating to the handling of information in this context.

LEVERAGING BETWEEN SYNERGIES BUSINESS AND REGULARTORY OBJECTIVES

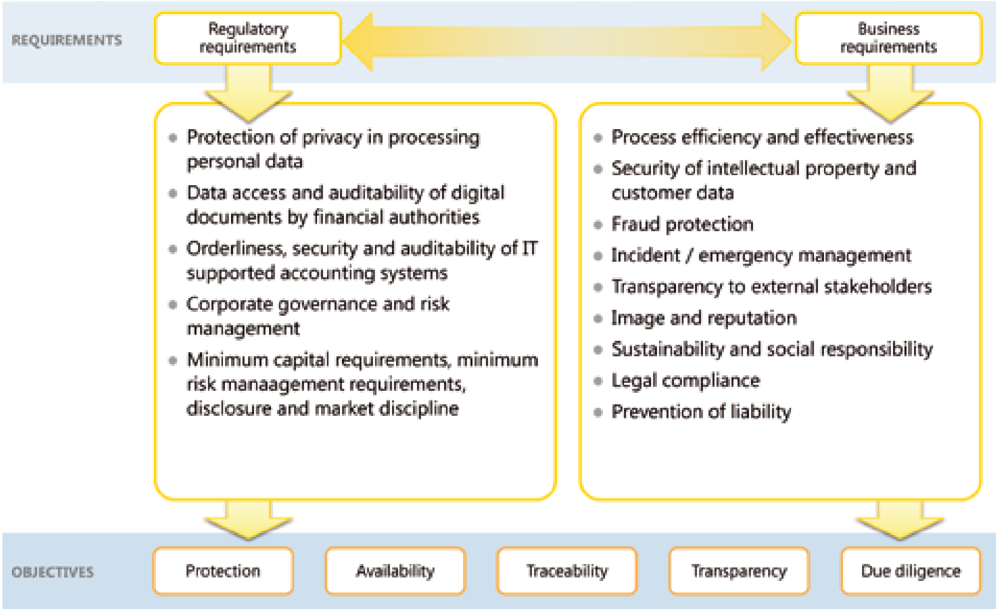

REQUIREMENTS
Regulatory requirements
Business requirements
Protection of privacy in processing personal data
Data access and auditability of digital documents by financial authorities
Orderliness, security and auditability of IT supported accounting systems
Corporate governance and risk management
Minimum capital requirements, minimum risk manaagement requirements, disclosure and market discipline
Process efficiency and effectiveness
Security of intellectual property and customer data
Fraud protection
Incident / emergency management
Transparency to external stakeholders
Image and reputation
Sustainability and social responsibility
Legal compliance
Prevention of liability
OBJECTIVES
Protection
Availability
Traceability
Transparency
Due diligence

Figure 4: Governance, Risk Management & Compliance: Synergies between business and regulatory targets

Protection in information processing

Case study [1] : Protection in information processing at Contoso Automotive

Contoso Automotive is a large automobile manufacturer in Europe. The company has completely reworked a range of models and plans the official launch for September 15. This deadline is strictly confidential. One week before the official announcement, the press publishes reports about the imminent event. Orders for the discontinued generation collapse, costing the automobile manufac-

[1] All case studies are fictitious – as well as the company Contoso and its suppliers. However, some elements of the cases are based on incidents that did take place in Germany and Europe.

turer millions of euros. Investigations reveal that a supplier is responsible for the leak. One of the supplier's employees had lost an unencrypted USB stick with technical specifications on the way home.

For companies, specific knowledge and the innovative potential based on it are valuable assets that need protection. **Protecting** intellectual property, personal data, financial and sales information is an essential requirement for the continuity and competitiveness of a business. **Confidentiality** and **data integrity** are two of the three key elements of basic information security requirements. Moreover, protection for information processing is an important basic requirement for an enterprise culture that is based on sustainability.

Aspects of protection are also found in various regulatory requirements, where they relate to health and safety at work, but especially relating to the data and information protection.
The German **Bundesdatenschutzgesetz (Federal Data Protection Act - BDSG)** stipulates rules for the handling of personal data of staff and customers. This data must not be accessible to third parties (aspect of confidentiality) or be modifiable without proper authorization (data integrity).

Protection of data with respect to accountability is another example of data protection. **Generally Accepted Accounting Principles (GAAP)** require both orderly accounting and the protection of data against manipulation at a later date, or unauthorized viewing by third parties.
Protection of personal data is also covered by the German **Telekommunikationsgesetz (Telecommunications Act - TKG)**. It typically dictates a general prohibition of checks on Internet and email use by employees to ensure privacy of telecommunications.

The overhead that compliance with data protection regulations involves can be reflected as added business value in the form of a data protection auditing seal of approval. To a third party, this seal of approval is proof of an enterprise's compliance with data protection regulations; and taking recent events into consideration, it can be a business advantage reflected in the establishment of trust.
The **Federal Data Protection Audit Act (Bundesdatenschutzauditgesetz - BDSAuditG)** planned for 2009 promises exactly this opportunity for suppliers of data processing equipment and providers of data processing services.
A voluntary, regulated data protection audit verifies the compatibility of a data protection model, or a technical system, with the data protection rules; and a data protection audit seal is issued as proof of compatibility.

experton GROUP

"Irrespective of legal requirements, the protection of data and information is also in an enterprise's business interests.
In an ideal case, it will prevent any kind of legal dispute, fraud and industrial espionage, and maintain the enterprise's good reputation."

Availability of information

Case study 2 : Failure of a mission-critical application leads to a temporary production standstill

Over the years, Contoso Automotive has outsourced a major proportion of its value added chain to suppliers. Following a software update at a specialist supplier's premises, a problem with a server system occurs. An overworked system administrator attempts to reconfigure the system. In the process, they inadvertently delete a database; this is due to the failure to adhere to the "Segregation of duties" principle for this critical action.
The ensuing failure of a mission-critical application based on this database is remedied within just two hours as the company has an actionable backup and recovery concept. This helps to avoid production downtime to a great extent. As this partner supplies "just-in-time" components which flow directly into the manufacturing process, it might delays in Contoso Automotive's own production.

The **availability** of information is just as important as protecting information against disclosure and manipulation. Today, manufacturing and service companies typically process most information electronically. If certain information fails to materialize within good time, processes in research and development, production, logistics and distribution, and in central areas such as sales, marketing, finance and human resources start to freeze.
Mid- to long-term archiving of information also protects a company against loss of data in case of system failure. Additionally, this ensures traceability for historic activities even though they may not directly impact daily business. As a rule, internal policies define a company's information availability requirements.

In certain cases, legislators require access to pertinent data within a prescribed period – as specified in the **Principles of Data Access and Verifiability of Digital Documents (Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen - GDPdU)**, which mandate audit compliant data storage and archiving.

Generally Accepted Accounting Principles (GAAP) also dictate long-term archiving, in this case to protect the legislator's interests under fiscal legislation.

Similar requirements, but with different aims, exist in ordinances such as the **Medical History Ordinance (Krankengeschichtenverordnung - KgVO).** This ordinance mainly serves, a patient´s health by ensuring that his medical history can be traced back for up to 30 years.

experton
GROUP

"Availability of information is very much in the best interest of a business. This applies in particular to fairly recent data required for ongoing operations. In turn, long-term archiving helps the enterprise to clarify legal issues with other companies, persons or the state."

Traceability of processes and methods

Case study 3: A dissatisfied employee tries to steal data

Contoso Financial Services (CFS), a Contoso Automotive group company, provides financial services to private and corporate customers. In the past, a demotivated employee was induced by drastic savings measures to pass on critical corporate data to a competitor. In the light of this incident, management and the shop council approved the security officer's proposal to install a security solution that ensures traceability of staff access and activities, including a corresponding written policy. When a dissatisfied account manager at Contoso Financial Services, who had already given notice, attempted to copy sensitive customer data onto a DVD in order to sell the data to a competitor, this activity was immediately identified as an anomaly. The CFS monitoring systems identified this unusually invasive access to a security-critical database and immediately revoked the employee's access privileges via the identity management system. This not only prevents losses caused by the data leak but also a loss of image.

Traceability in this case primarily refers to the enterprise's internal monitoring of workflows and structures – in contrast to transparency, which relates to the monitoring of an enterprise from the outside and will be discussed later on.

Documentation and the ability to monitor and audit business processes and systems are essential in that a company can establish who had access to what information, or possibly modified this information, at any time. The ability to map activities to persons, functions and roles serves to provide evidence of orderly processing of defined business workflows by authorized persons. On top of this, the enterprise can identify and evaluate the optimization potential of individual process steps and implement improvements. Finally, the ability to reproduce successful workflows offers the potential for rationalization and ongoing improvement. This puts a company in a position to work more flexibly and efficiently.

Traceability also structures knowledge management within the enterprise, thus guaranteeing precision and consistency in information handling.

Several regulations address the topic of traceability. For example, the **Federal Data Protection Act (Bundesdatenschutzgesetz - BDSG)** mandates traceability in the form of access logs and the ability to map entries relating to persons, data modifications and deletions, as well as forwarding of data to third parties.

Among other things, the European Union's **8th EU directive (EuroSOX)** stipulates complete, consistent and traceable documentation of IT privilege assignments.

Generally Accepted Accounting Principles (GAAP) in turn stipulate process documentation and retention periods for business relevant documents.

experton GROUP

"From a business point of view, the benefit of traceability requirements is – above all - that of implementation of more efficient and accurate processes. At the same time, businesses are better prepared for crises or legal issues."

Transparency for external stakeholders and advocacy groups

Case study 4: Transparency in case of a data protection infringement in retailing business

Contoso Retail is a new Contoso Automotive subsidiary that sells automobile parts. It does all of its business via an Internet portal. After receiving notification of an unauthorized disclosure of customer data, the management orders an internal audit. The audit reveals that a developer from the software department had modified the webshop platform from home on the weekend and then published the changes. The developer's negligence led to customer data such as names, credit card numbers, and dates of birth being publicly visible for several hours. The retailing company accordingly notified the customers in question and the credit card companies. Thanks to the swift response, the damage was minimal. As this incident sharpened the management's awareness of the subject of information security, the company has now optimized its security processes and had the shopping platform security certified by external auditors. The short-term damage to the company's public image has now been reversed.

External **transparency requirements** force the company to seriously investigate the documentation of business workflows, best-practice orientation and the introduction of a monitoring system. If these items are carefully implemented, the obligation of transparency can be turned into something positive. With respect to business flexibility, the company has made progress and can leverage optimized information management as the basis for internal decision making processes. Externally, transparency builds trust with customers and partners thus promoting positive business development.

The **Law on Control and Transparency (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich - KonTraG)** forces companies to install enterprise-wide early warning systems for potential risks and to publish statements on risk and risk management within the enterprise in the management report with their annual financial statements.

The **German Commercial Code (Handelsgesetzbuch - HGB)** encourages auditors to verify compliance with legal requirements in annual audits – especially with respect to the risk management system and corresponding measures.

Another example is the obligation to transparency in the **Telecommunications Act (Telekommunikationsgesetz - TKG)** which forces public telecommunications network carriers to disclose accounting information and technical specifications for companies authorized to access the networks.

experton GROUP

"Although individual companies may not always be in favor of external information and communication, there are some positive side effects. Used proactively, transparency can improve the perception of or boost a company's image. It is an important part of incident management while at the same time allowing for more intensive coordination with other companies, possibly from the same sector."

Case study 5 : Due diligence in system update handling at Contoso Flight

Contoso Flight is an air freight specialist and uses a fully-automated, computerized system for freight handling. Due to a system outage, it was impossible to handle some freight deliveries in good time. Investigations revealed that the outage was caused by a software update.
An operator had installed the update without sufficient testing in the integration environment. The management had insisted on the update being installed immediately as it accelerated freight handling by 30 percent. The operator had pointed out to the management that installing the update could constitute a major risk for the availability of the handling systems. However, the operator's objections were ignored. By ordering immediate installation of the update, the management negligently caused an interruption to services.

From the viewpoint of company management, **diligence** is a decisive factor in ensuring the economic viability and effectiveness of a company's business activities. The principles of due diligence must be firmly anchored in a company's culture. Sufficient procurement of information, adequate analysis of the situation, and responsible risk assessment are considered to be essential elements here.

Thus, due diligence is a central theme of objectives such as protection, availability, traceability and transparency.

Individual due diligence obligations are not codified for the main part. However, they can be derived from the organizational role of management within the company.

The **Companies Act (Aktiengesetz - AktG)** and **Limited Liability Company Law (Gesetz betreffend die Gesellschaften mit beschränkter Haftung - GmbH)** include imperatives on the due diligence of an orderly business person.

The obligations include orderly management of the company, arising from compliance with laws, articles, contracts of employment, and are binding for the executive board in particular. The executive board is obligated to engage in all business activities in the best interests of the company and to refrain from activities that could damage the company.

Additionally, the management is required to "exercise due diligence" as stipulated in the **German Civil Code (Bürgerliches Gesetzbuch - BGB).**

The requirements of **Basel II** or the **German Banking Act (Kreditwesengesetz - KWG)** are industry-specific examples of due diligence for the financial sector. They state that financial institutions are required to comply with principles of due diligence, have effective internal strategies, systems and controls in place in order to identify, evaluate, monitor and mitigate credit and thus avoid endangering their business, or prevent cases of liability.

experton GROUP

"Due diligence is also important against a background of business requirements. Due diligence on the part of company management is useful and contributes significantly to the success of a business."

General due diligence from the viewpoint of IT compliance includes developing, publishing and establishing corresponding **IT policies.** This means upholding industry standards, complying with legal requirements, establishing controls and ensuring compliance. Training and external certification are useful here.

History shows us that it is not typically necessary to reinvent the wheel. In most cases, existing processes and IT infrastructures can be used.

Protection, availability, traceability, transparency and due diligence are targets that are effected both by a number of regulations and by business policies. For an individual enterprise, an implementation model that gives the enterprise the ability to adapt to the most important common denominators of the regulations with which it needs to comply is optimal. It gives the company the ability to leverage synergy effects with imminent tasks and acceleration implementation.

If a company is proactive with respect to the intentions of business and legal requirements, it will find it easy to implement future compliance requirements. **In this way, a "must" becomes a "plus."**

At the end of the day, a model of this kind promotes **awareness** of the interdependencies between business processes and information technology.

History shows us that it is not typically necessary to reinvent the wheel. In most cases, existing processes and IT infrastructures can be used.

"It is now a question of identifying the common denominator for key areas in the implementation of regulations. After doing so, we can put together the pieces of the mosaic to create a holistic image. Chapters 4 and 5 help companies to focus on what matters."

CHAPTER 4

WHAT DO I NEED TO FOCUS ON? KEY ISSUES!

4. WHAT DO I NEED TO FOCUS ON? KEY ISSUES!

Five key areas of business and regulatory requirements

As we saw in Chapter 3, many regulatory and business requirements have common targets: protection and availability of information, traceability of processes and information processing, transparency towards third parties and due diligence in daily business. Based on these targets, we can derive five key areas on which an enterprise should focus to successfully implement compliance requirements.

Legislation gives rise to key areas which legislators regulate in the context of IT. These key areas are: **information protection, risk management, information management, internal control system and the duty to cooperate and disclose.**
Typically, any company will have departments or employees who work in these key areas. The target now is to coordinate, and thus promote, these activities throughout the enterprise.

MOTIVATION FROM THE VIEWPOINT OF BUSINESS DECISION MAKERS

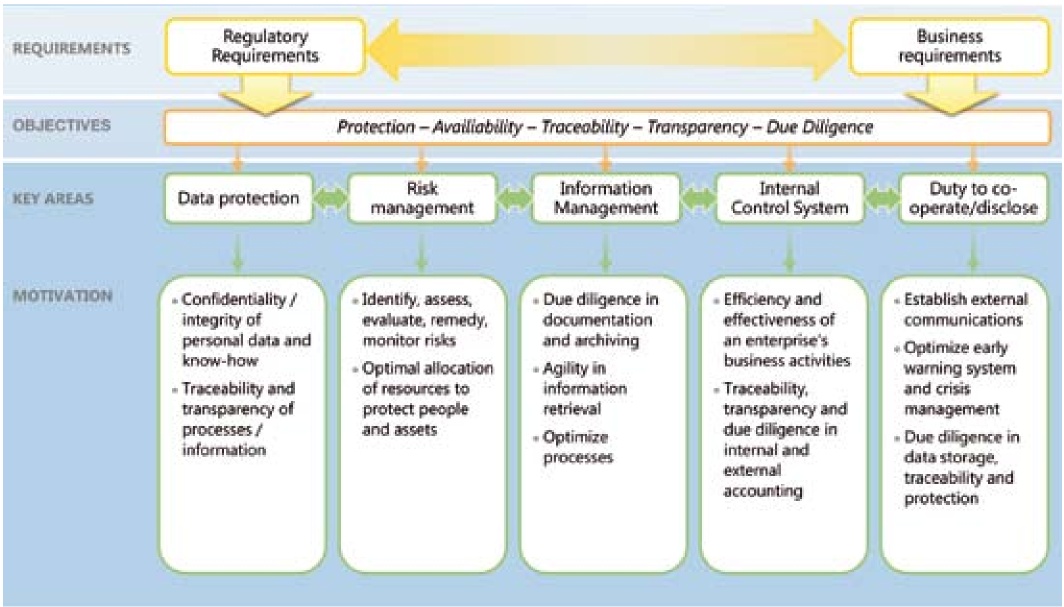

REQUIREMENTS
Regulatory Requirements
Business requirements
OBJECTIVES
Protection – Availiability – Traceability – Transparency – Due Diligence
KEY AREAS
Data protection
Risk management
Information Management
Internal Control System
Duty to co-operate/disclose
MOTIVATION
Confidentiality / integrity of personal data and know-how
Traceability and transparency of processes / information
Identify, assess, evaluate, remedy, monitor risks
Optimal allocation of resources to protect people and assets
Due diligence in documentation and archiving
Agility in information retrieval
Optimize processes
Efficiency and effectiveness of an enterprise's business activities
Traceability, transparency and due diligence in internal and external accounting
Establish external communications
Optimize early warning system and crisis management
Due diligence in data storage, traceability and protection

Figure 5: Governance, Risk Management & Compliance: Motivation

In the following section we will be looking at how enterprises can achieve set targets via these five key areas. Addressing these areas with due care will put a company in an excellent position to comply with many regulations – both present and future. The key areas serve as a common denominator for communications across various decision making and implementation levels. Based on this, a mutual understanding of their necessity, reasons and implementation arises from the viewpoint of management, technical decision makers and IT experts.

Information protection

From a company's viewpoint, information protection is critical for two reasons. In both cases it relates to the aspects of confidentiality and integrity – on the one hand for mission-critical information and the protection of intellectual property, and on the other for data and information subject to regulatory protection.

Besides the legal requirements discussed previously, information protection is also necessary to ensure the traceability and transparency of business processes, for example, in the sense of ensuring the immutability of logs.

Data leaks due to insufficient protection can also have a negative impact on the company's image.

Information protection measures are also defined in standards such as COBIT (Control Objectives for Information and related Technology), ITIL (IT Infrastructure- Library), BSI IT Basic Protection and IDW PS 330 published by the Institute of Auditors in Germany (Institut der Wirtschaftsprüfer in Deutschland e.V. (auditing standard)).

Risk management

Risk management refers to a systematic approach and process for identifying, analyzing, evaluating, remedying, and monitoring risk. It helps enterprises to identify threats, vulnerabilities, and risks. Risks, or residual risk, are calculated as accurately as possible, the extent of risk acceptance is defined, and priorities are set for security measures. This warrants investments in security measures while at the same time improving security awareness in the company – and especially at executive level.

The generic objectives of risk management are those of information protection and availability, traceability of processes and compliance with due diligence. One critical motivation for risk management is also optimal allocation of resources to protect humans and assets. Although risk management is in place at various levels within an enterprise, it is always oriented on the enterprise's objectives.

Risk management is the subject of many regulations and standards. They include KonTraG and Basel II, COSO Enterprise Risk Management (Committee of Sponsoring Organizations of the Treadway Commission), COBIT, and the international ISO/IEC 27005:2008 standard.

Information management

Information management gives enterprises the ability to achieve strategic objectives by means of methodical information control and communications measures. To apply these measures in an effective way, it is vital to exercise due care in documentation and archiving. The intersection between business and regulatory requirements in this case is that of achieving availability, traceability, and finally of due diligence in the information lifecycle.

Despite permanent data volume growth, enterprises need to be able to locate and retrieve specific information quickly when needed. GAAP, GDPdU and more recently EuroSOX require this. Additional regulations relating to data retention are found in the fields of product liability and legal code of procedure. The standardized ITIL process can help implement these requirements.

Internal control system

The internal control system (ICS) monitors efficiency and effectiveness in the implementation of key elements and serves to safeguard the efficiency and effectiveness of the enterprise's business activities.
ICS is also necessary to ensure traceability, transparency and due diligence in internal and external billing, and to guarantee compliance with legal requirements. This is typically effected by means of an internal control and monitoring system, supplemented by risk management.

Compliance with legal requirements is effected by state-specific standards such as IDW PS 330 for the annual and intermediate financial statements.

Duty to cooperate and disclose

Finally, an enterprise is obligated to cooperate and disclose. This is closely related to information protection, information and risk management, and internal control systems. The preconditions include the availability, traceability and transparency of data acquired and maintained with due diligence.

Although many companies consider their duty to cooperate and disclose an unpleasant one, it also allows for synergies with business objectives. They include external communications, optimized processes, maintaining and improving the company's image, responsible data handing, and above all the introduction of control mechanisms to identify critical incidents in good time.

The duty to cooperate and disclose can be incident driven, or a continuous process. The former is the case with the Federal Data Protection Act (Bundesdatenschutzgesetz), for example, and stakeholder's rights in the case of data protection infringements. The 2004/39/EC Markets in Financial Instruments Directive (MiFID), which defines business processes for changing suppliers in the gas sector (GeLi Gas) and the German Data Access and Digital Signature Authentication Law (GDPdU) are also examples of the duty to cooperate and disclose.

"It is important to address these five key areas enterprise-wide and across divisions. Information technology plays an important role in implementing this. Chapter 5 discusses matching solutions. And the discussion in Chapter 6 helps enterprises to gradually start aligning themselves with regulatory targets."

CHAPTER 5

AND NOW THE SOLUTION

5. AND NOW THE SOLUTION

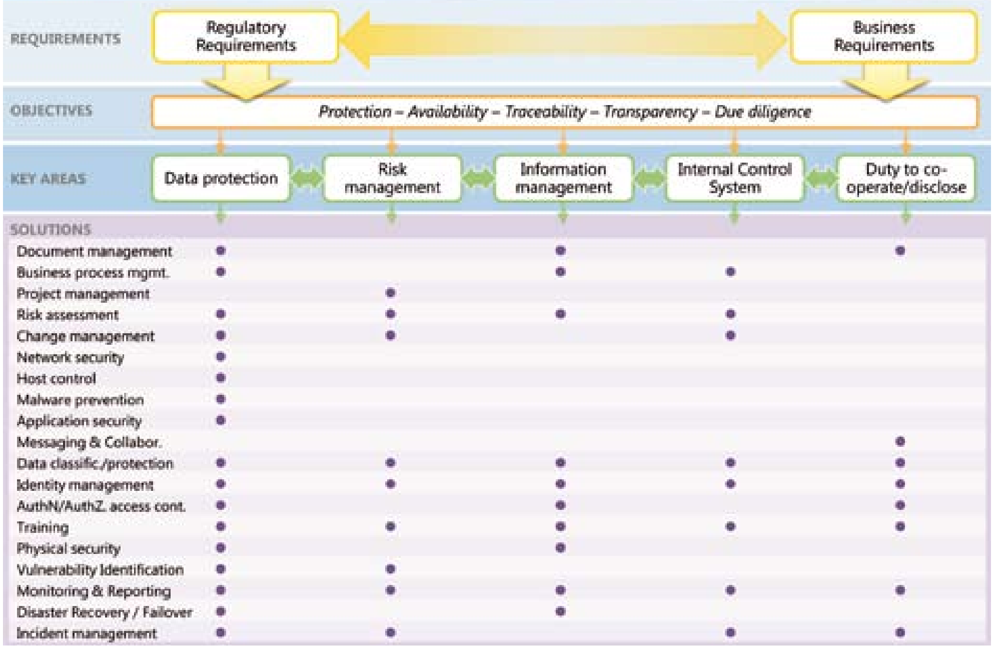
How information technology can contribute to implementation

Information technology plays an important role in ensuring and automating compliance. At the same time, it is a critical element in achieving business objectives. In the following section, we will be investigating how information technology can contribute towards achieving the business and regulatory objectives in the five key areas referred to in Chapter 4.

Microsoft has identified **19 solution categories** with relevance for compliance management [2]. Various forms of these technological solutions are necessary to implement common standards and regulations such as ISO 27002, EUDPD, Cobit, and others. Each of the five key areas poses its own requirements with respect to the use of these solutions.

IMPLEMENTATION THROUGH INFORMATION TECHNOLOGY

For easier readability and handling, mapping of the solutions to key areas focuses on critical items.



	Data protection	Risk management	Information management	Internal Control System	Duty to co-operate/disclose
Document management	●		●		●
Business process mgmt.	●		●	●	
Project management		●			
Risk assessment	●	●	●	●	
Change management	●	●		●	
Network security	●				
Host control	●				
Malware prevention	●				
Application security	●				
Messaging & Collabor.					●
Data classific./protection	●	●	●	●	●
Identity management	●	●	●	●	●
AuthN/AuthZ. access cont.	●		●		●
Training	●	●	●	●	●
Physical security	●		●		
Vulnerability Identification	●	●			
Monitoring & Reporting	●	●	●	●	●
Disaster Recovery / Failover	●		●		
Incident management	●	●		●	●

Figure 6: Governance, Risk Management & Compliance: Implementation by means of Information Technology

Information protection

Information protection relates to ensuring the **confidentiality** and **integrity** of personal data. Besides this mainly legal aspect, however, information protection also includes any and all measures designed to prevent the disclosure of intellectual property and the trading of secrets to unauthorized third parties. At the same time, it requires transparent and traceable handling of the data to be protected.

Information protection relates to organizational and technical tasks.

[2] Microsoft Technology Solutions for Compliance Management: See Microsoft IT Compliance Management Guide (http://www.microsoft.com/technet/SolutionAccelerators)

It is important to classify data by their need for protection. The question as to the owner of some records and information automatically arises. One critical precondition for compliance with information protection requirements is therefore that of clarifying responsibility. Each piece of information in a company must be assigned to an employee – typically the person responsible for the business process in question. The owner defines protection requirements for this information and decides who is given access. The security office defines tangible measures to implement this protection.

Best practices dictate a constellation in which a **Chief Information Security Officer (CISO)** defines the framework for data security and is supported by the management, divisions, and IT department. Another successful approach is that of establishing a **Security Steering Committee** as a forum for executives from various enterprise divisions, all of whom are information security stakeholders. This starts with the board and the CIO and includes the data protection officer, various divisional heads, the heads of human resources and finance and the compliance officer.

The CISO's responsibilities also include promoting awareness for the need to protect information in the enterprise. The board defines a general **direction and culture.** At the same time, all processes and incidents relevant to data protection must be documented.

Information technology offers support, particularly in the following areas:

- Document management solutions help to control, manage and trace access to sensitive data.
- Business process management (BPM) helps to handle complex information requests or transactions in a transparent and orderly manner, taking various applications and access privileges into consideration.
- Risk assessment identifies the risks to which certain data are exposed. Tools identify vulnerabilities and threats, especially in operations.
- Change management provides tools to support data change processes. After all, business processes and IT systems will change over time, and this can influence information protection.
- Network security restricts access to the enterprise's internal network resources to authorized persons.
- Host controls protect server and workplace infrastructures against unauthorized access or changes.
- Malicious software prevention – that is prevention of viruses, spyware or other threats such as rootkits – is essential to ensure confidentiality, availability and integrity of data.
- Application security removes vulnerabilities in applications which could otherwise leave doors open for attacks and fail to prevent data theft or manipulation.
- Data classification and protection facilitate manual classification processes by introducing automation tools. Data encryption on storing or transferring data is driven by protection requirements.
- Identity management governs the orderly assignment and withdrawal of access privileges for data and systems. At the same time it ensures transparency and traceability in access to resources with a view to identifying information protection infringements.

- Authorization, authentication and access controls prevent access to data and systems without the required privileges and credentials.

- Training promotes staff awareness of information protection requirements.

- Physical security is another building block of information protection, both in electronic and written form.

- Identification of vulnerabilities is an important information protection tool.

- Monitoring and Reporting help to verify the success of technical and organizational security measures, while at the same time forming a basis for identifying information protection infringements.

- Incident management and trouble tickets can help address and remedy data compromises and also provide a starting point for IT forensics.

Risk management

Every company faces risks: completely eliminating them is neither possible nor economically viable. Risk management therefore tends to focus on finding the perfect balance between anticipated damage and the costs of risk mitigation and/or adjusting to a level of "acceptable residual risk".

There are four basic approaches. One typical approach is that of reducing risk by means of suitable technical and organizational measures and control mechanisms. A second approach is that of transferring some risks to third parties, e.g. to insurance companies and (with some restrictions) to service providers. Avoidance of risk by discontinuing activities that lead to risk, e.g. by redesigning business processes, or avoiding new, insecure IT systems is another option. Finally, there is the option of accepting risk, if the countermeasures are disproportionate to the value of the commodity in question. Implementation of a risk management system always starts by defining the **objectives and motivation** of risk management. In particular, these are operative and strategic objectives and targets in internal and external reporting – at the same time the question as to which regulations, laws, and standards need to be implemented locally or globally also arises. Another important factor is that of defining roles in risk management, both at superordinate levels and in IT risk management. Enterprise-wide coordination processes between the stakeholders have to be established in order to achieve alignment with a mutual, enterprise-wide risk management framework.

The next step is for the enterprise to identify and evaluate information, systems, production equipment and other assets. After this, **risk assessment** (assessment) can take place.

To allow this to happen, **classification** of assets with respect to their protection requirements is essential, and this specifically includes classifying data. Following this, threats and vulnerabilities must be identified. Next, it is important to anticipate the potential impact of an incident and – based on the anticipated frequency – to calculate the risk it involves. Finally – and this is an important result of risk assessment – the enterprise must prioritize the relevance of individual risks.

Based on this information, a decision must be made as to which **measures designed for addressing risks** make business sense.
The four approaches referred to previously are available as options here. Risk acceptance or "risk appetite" is something the management has to decide.

Often ignored, but still very important, are tools for monitoring and validating processes and measures, and finally documenting and communicating the results of risk assessments.

Information technology offers support, particularly in the following areas:

- Project management: Project risks can be addressed by means of integrated risk management, including suitable methods and tools.
- Risk assessment is the key to risk management. Solutions for, e.g. vulnerability management and incident management help to implement these analyses.
- Change management: Risk profiles change in line with changes in business, information technology or threat scenarios. Tools can help in operative areas in particular.
- Data classification and protection: Data classification is essential to define protection requirements and standards for corresponding protection measures.
- Identity management not only improves protection, it can also be used to monitor measures and systems. The information this generates flows back into the risk management process.
- Training: Awareness must be trained in line with user functions and residual risk situations. This also promotes security awareness.
- Vulnerability identification provides critical input for risk evaluation.
- Monitoring and eporting reveal the effectiveness of the risk management program. They also provide input for vulnerability and threat assessment.
- Incident management and trouble tracking are important sources for performing threat assessment.

Information management

In the scope of information management the enterprise fulfills its archiving and documentation obligations while at the same time optimizing internal processes with the aim of more efficient information processing. Just like in information protection and risk management, any solution will need to classify data to differentiate data management in line with legal and business requirements.

From a technology point of view, information management mainly relates to the application level within the enterprise and the storage and archiving infrastructure. The key words at infrastructure level are information lifecycle management, which actually means data processing in line with legal and business requirements from data input through to archiving and deletion. Enterprise content management (ECM) and business process management (BPM) are also critical interdisciplinary aspects at application level. Enterprise resource planning (ERP) and business intelligence (BI) are further applications that relate to information management. Orderly accounting and the prevention of corruption and fraud are important targets at the application level.

Information technology offers support, particularly in the following areas:

- Document management solutions help to organize unstructured information, no matter what electronic format it takes.

- Business process management (BPM) helps to handle complex information requests or transactions in an orderly manner and to ensure transparency throughout.

- Risk assessments are also necessary in the context of information management to ensure a well-founded basis to justify investments in underlying security models and solutions.

- Messaging & Collaboration serve the exchange of information in the enterprise and beyond the company's borders. At the same time, they are part of information management, e.g. in the context of email archiving.

- Data classification and protection: Data classification is one of the first steps in information lifecycle management as it allows data to be stored, protected and archived in an optimal way that reflects its properties. Manual classification processes can be facilitated by automation tools. Encryption solutions protect archived data.

- Identity management ensures that access to, e.g. archived data is restricted to authorized persons, in line with their functions and access privileges.

- Authorization, authentication and access control guarantee data confidentiality and integrity.

- Training promotes policy-compliant handling of information in the enterprise.

- Physical security also protects information, for example in the form of physical access controls in datacenters.

- Monitoring and Reporting solutions reveal unauthorized access to information.

- Disaster recovery and failover define peri - ods in case of IT system failure, or to keep operations highly available thanks to redundant systems.

Internal control system

The internal control system (ICS) is represented as a control and monitoring system in various components. The alignment of the enterprise and its processes with a common standard such as COSO plays a particularly important role.

Four principles typically apply. The two-pairs-of-eyes principle introduces mutual controls by ensuring that at least two employees are responsible for a process. The principle of segregation of duties demarcates fulfillment and controlling of tasks and is important to maintain. The principle of transparency refers to the fact that enterprise process models must be traceable and understandable. Control targets make it possible for third parties to objectively ascertain whether employees are complying with set targets. Finally, the need-to-know principle ensures that staff do not receive more information than they need for their daily work.

All told, it is thus a question of defining control targets and mechanisms, monitoring for compliance with targets, efficiency and effectiveness tests, and finally maintaining consistent documentation.

These principles are not only reflected in processes, but also in the basic IT infrastructure and applications such as ERP. The counterpart to ICS at a business level is known as COBIT (Control Objectives for Information and related Technology) in IT.

Information technology offers support, particularly in the following areas:

- Business process management (BPM) ensures transparency and allows the enterprise to define processes that comply with ICS requirements.

- Risk assessments are a critical aspect of the internal control system. They also relate to aspects of information technology and can be automated by IT at the same time.

- Change management ensures that staff-related, business and technological changes do not conflict with policies such as segregation of duties or mutual controls.

- Data classification and protection help identify the owners and support risk assessments. This also forms a basis for defining which staff are allowed to access and modify what data. The two-pairs-of-eyes and need-to-know principles are in effect here.

- Identity management builds on the results of data classification and implements a process that defines which employees have access to what scope of information. It also supports the principle of "segregation of duties".

- Training is necessary to ensure that employees understand their roles and tasks with respect to ICS and are empowered to fulfill them.

- Monitoring and Reporting solutions add transparency to the implementation of control targets in IT.

- Incident management and trouble tracking also contribute to ensuring transparency with respect to identifying problems in supporting IT processes, or infringements of internal policies.

Duty to cooperate and disclose

Today's information and communications processes mainly use electronic means. Information technology therefore plays a critical role in an enterprise's duty to cooperate and disclose, and must comply with a variety of requirements with respect to the format of the content to be disclosed, the data transfer method, and security mechanisms.

Compliance with duties to cooperate and disclose includes various aspects. From an internal point of view, this duty imposes strict requirements on processes and on cross-divisional cooperation within the enterprise. In case of an incident that fulfills duty-to-disclose requirements, actionable crisis management and solid contingency planning are essential to successful crisis management and the accompanying presentation to third parties.

Information technology offers support, particularly in the following areas:

- Document and enterprise content management help to store, format and manage information for compliance with regulatory requirements.

- Messaging & Collaboration often serve the exchange of information between the enterprise and external advocacy groups or authorities. Under ideal circumstances archiving solutions will allow an enterprise to produce evidence of all communications in a business transaction when required to do so by a court of law.

- Data classification and protection: The duty to cooperate and disclose also requires the enterprise to know which data may and must be published. If needed, data are encrypted before transfer or electronically signed.

- Authorization, authentication and access controls that guarantee data confidentiality and integrity – extremely important in accounting and legal issues, but also in an enterprise‘s duty to disclose to authorities.

- Training promotes awareness and builds knowledge in the context of an enterprise‘s duty to cooperate and disclose.

- Monitoring and Reporting solutions help to identify compliance breaches and to start an escalation process if needed.

- Incident management and trouble tracking build on monitoring and reporting measures. This helps to comply with duties to cooperate in forensic cases.

”Each company has different basic requirements with respect to the implementation of compliance requirements in the five key areas. An IT infrastructure compliance maturity model that takes individual starting points into consideration and reveals the course of ongoing improvement is extremely useful in this context. For more details, see Chapter 6.“

CHAPTER 6

QUO ESQUE QUO VADIS?
COMPLIANCE, IMPLEMENTATION

6. QUO ESQUE QUO VADIS? COMPLIANCE, IMPLEMENTATION

IT infrastructure compliance maturity model for step-by-step alignment with regulatory targets

As described previously, information technology plays a critical role in fulfilling business and regulatory requirements in the five key areas information protection, risk management, information management, the internal control system, and the enterprise's duty to cooperate and disclose. An enterprise that is well positioned in these key areas will be capable of fulfilling many compliance requirements with just a **little more effort**. At the same time it can leverage the synergies between business and compliance.

Chief Information Officers (CIOs) often ask themselves how they can use IT infrastructure optimization (IO) measures to help fulfill legal or internal requirements. It is useful to identify the status quo on the one hand, and the future tasks to be fulfilled on the other.

The IT infrastructure compliance maturity model is a major help in this. Enterprises can assess their own maturity in four levels and, based on this assessment, ascertain the usefulness of achieving a higher maturity level; at the same time actionable steps for doing so are recommended.

A higher maturity level improves the cost efficiency of the IT infrastructure and adds value to the enterprise's business while at the same time preparing the enterprise more effectively with respect to compliance with regulatory requirements.

IT-INFRASTRUCTURE COMPLIANCE MATURITY MODEL

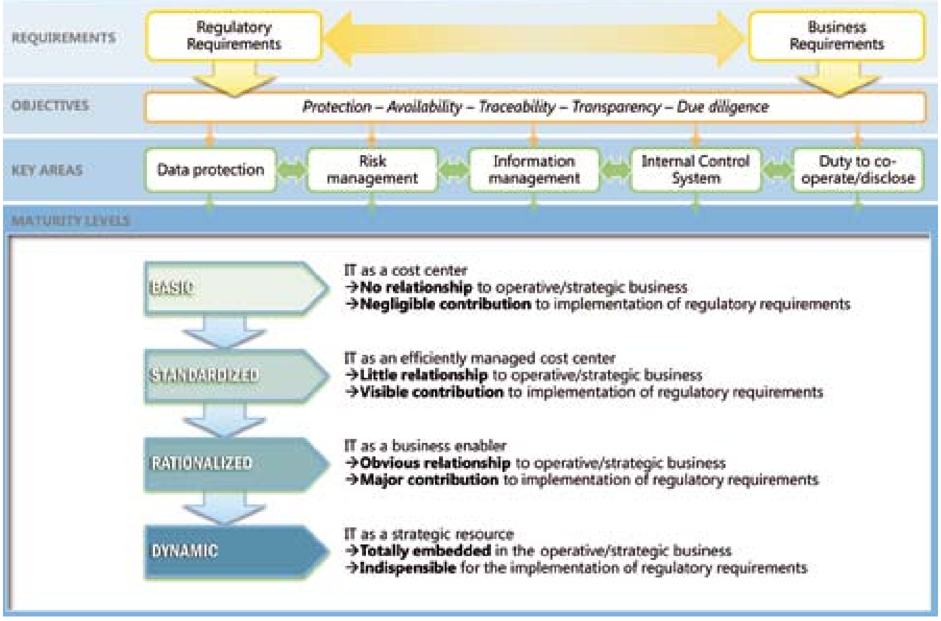

REQUIREMENTS
Regulatory Requirements
Business Requirements
OBJECTIVES
Protection – Availability – Traceability – Transparency – Due diligence
KEY AREAS
Data protection
Risk management
Information management
Internal Control System
Duty to co-operate/disclose
MATURITY LEVELS
BASIC
IT as a cost center
→No relationship to operative/strategic business
→Negligible contribution to implementation of regulatory requirements
STANDARDIZED
IT as an efficiently managed cost center
→Little relationship to operative/strategic business
→Visible contribution to implementation of regulatory requirements
RATIONALIZED
IT as a business enabler
→Obvious relationship to operative/strategic business
→Major contribution to implementation of regulatory requirements
DYNAMIC
IT as a strategic resource
→Totally embedded in the operative/strategic business
→Indispensible for the implementation of regulatory requirements

Figure 7: Governance, Risk Management & Compliance: IT Infrastructure Compliance Maturity Model

The model is mainly designed for IT decision makers, but also for stakeholders in information security, compliance, divisions, and management who are interested in acquiring more in-depth understanding of the relevance of information technology in compliance with regulatory and business requirements. It will help IT experts to demonstrate how technology can help achieve targets in the individual solution areas.

Maturity model

The IT infrastructure compliance maturity model defines four levels of maturity, all of which describe a specific enterprise status. To take the step from one maturity level to another, an enterprise must complete tangible activities which are defined for the key areas.

The individual maturity levels are characterized by the following states:

- **Basics:**
  Information technology is a cost center only and is not related to operative or strategic business. It makes a very small contribution to the implementation of regulatory requirements. The systems are complex and incompatible. Most IT resources simply react to problems and help to keep systems running as far as possible. As there are very few standards and automated tools, support is labor intensive and expensive.

- **Standardized:**
  Information technology acts as an efficiently managed cost center, but still has little to do with the enterprise‘s operative and strategic business. However, it makes a visible contribution towards the implementation of regulatory requirements. At this level of maturity, the IT department is centralized and more effective; however, the systems remain complex, incompatible and expensive to maintain. Stand-alone solutions still exist in some divisions and departments.

- **Rationalized:**
  Information technology is already acting as a business enabler and is clearly related to the enterprise‘s operative and strategic business. It makes a major contribution towards the implementation of regulatory requirements. Combined IT and business teams develop strategies and define IT policies which are implemented as technological solutions. Thanks to standards and careful technical planning, application compatibility improves and the complexity of integrated systems drops.

- **Dynamic:**
  At this level, information technology acts as a strategic resource, totally embedded in the enterprise‘s operative and strategic business. It is indispensable in the implementation of regulatory requirements. Business agility has higher priority than short-term cost cutting. The IT systems are highly automated and flexible. They adapt quickly to changes in business framework conditions.

Information protection

Entry Level - Basic

The enterprise does not have a data classification schema, and has not assigned owners and responsibilities for processing of specific data. There is a lack of ongoing coordination between management, human resources, finance and operative divisions on the one hand, and the IT division on the other. The data protection officer virtually never communicates with IT stakeholders and rarely with management – the officer's function in the enterprise is more or less insignificant. Awareness of information protection in the enterprise is very low. Legal and regulatory requirements are virtually unknown in IT.

If at all, risk assessments are isolated, informal and irregular, typically within the scope of projects. Data protection is only in place for HR applications.

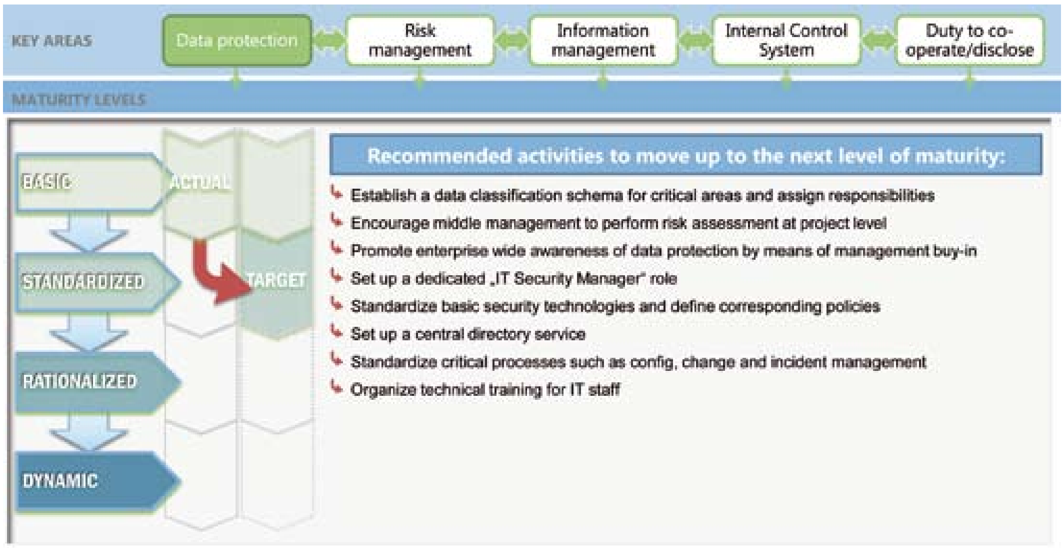
The enterprise handles problem and change management ad hoc by "fire fighting". System monitoring is restricted to servers and not automated. Security issues are identified by chance or after system failure. It is highly likely that nobody would notice the loss of confidential data.

Basic security functions such as a firewall and virus protection are in place, but there are no standards or policies. Protection is reactive only. Generic host controls and, more specifically, patching are weak points, as is application security. Awareness of physical security is very low; this is a consequence of the lack of staff training. It is also unclear which mobile devices are used where, how and to what end. Encryption solutions are rarely used. Various directory services may be in use, however, there is no centralized directory service and no identity management.

Document management is in place – if at all – as an isolated stand-alone solution in various areas. Business process management solutions are not in place.

All told, IT is a cost center and is not related to the enterprise's operative and strategic business. It makes virtually no (visible) contribution to the implementation of regulatory requirements.

The following figure shows which activities are necessary to move up to the next highest maturity level.



Recommended activities to move up to the next level of maturity:

- Establish a data classification schema for critical areas and assign responsibilities
- Encourage middle management to perform risk assessment at project level
- Promote enterprise wide awareness of data protection by means of management buy-in
- Set up a dedicated „IT Security Manager" role
- Standardize basic security technologies and define corresponding policies
- Set up a central directory service
- Standardize critical processes such as config, change and incident management
- Organize technical training for IT staff

Figure 8: IT Infrastructure Compliance Maturity Model - Information protection: Activity plan BASIC - STANDARDIZED

Standardized

A basic data classification schema is in place, but it is built on intuition and not deployed throughout the enterprise. This also applies to data owners and responsibilities. Coordination between IT organization and management is ad hoc and not institutionalized.

Awareness of information protection is growing. The data protection officer communicates with the management and individual operative divisions but has little contact with the IT department. An "IT security officer" may exist. Risk assessments are performed in the scope of projects only. Standardization is slowly spreading, however, it has not been implemented and documented enterprise-wide. Legal and regulatory requirements are partially known in IT.

Problem and change management are only partly standardized and automated. There is a policy for handling security issues and critical servers are subject to constant monitoring. Despite this, security problems are not always identified, and monitoring involves considerable personnel overhead.

Basic security functions such as firewalls, virus protection and some network security elements are in place and standardized, and security policies exist for these subjects, although ongoing monitoring to ensure compliance has not been introduced.

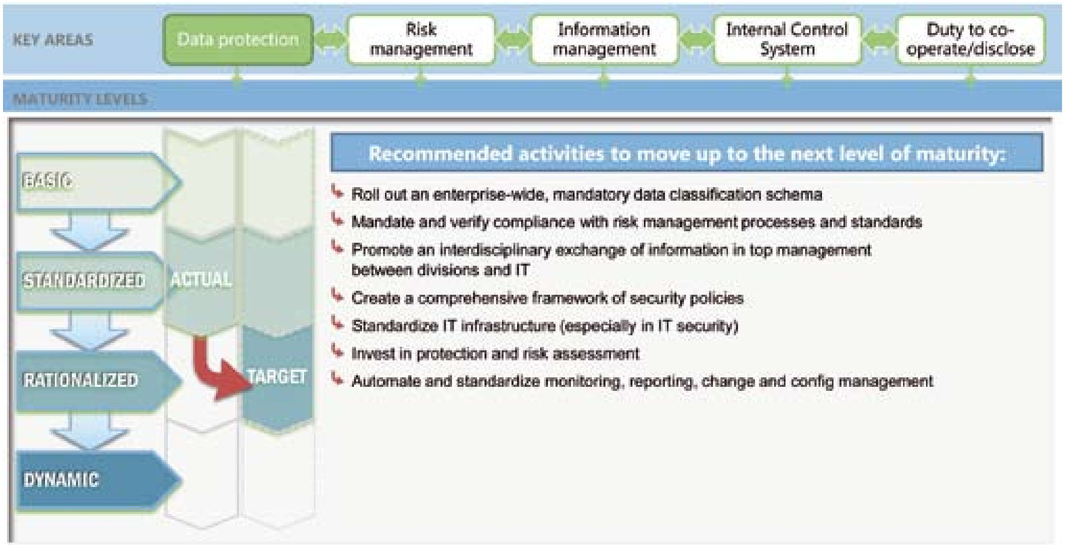
Encryption solutions are used occasionally, but not systematically on the basis of data classification and risk assessment. Client infrastructure management is standardized for the main part; however, it does not fully cover mobile devices. There is a centralized directory service, but it does not include comprehensive identity management.

Application security and physical security are still problematic. Compliance relevant training is held for individual IT staff, but is primarily technical and vendor-specific.

Document management is in place but not fully consolidated. Business process management solutions are used in various areas.

All told, information technology acts as an efficiently managed cost center, but still has little to do with the enterprise‘s operative and strategic business. However, it makes a contribution towards the implementation of regulatory requirements.

The following figure shows which activities are necessary to move up to the next maturity level.



Recommended activities to move up to the next level of maturity:

- Roll out an enterprise-wide, mandatory data classification schema
- Mandate and verify compliance with risk management processes and standards
- Promote an interdisciplinary exchange of information in top management between divisions and IT
- Create a comprehensive framework of security policies
- Standardize IT infrastructure (especially in IT security)
- Invest in protection and risk assessment
- Automate and standardize monitoring, reporting, change and config management

Figure 9: IT Infrastructure Compliance Maturity Model - Information protection: Activity plan STANDARDIZED - RATIONALIZED

Rationalized

An enterprise-wide and consistent data classification schema exist for the most part.
This also applies to data ownership and critical responsibilities. Coordination meetings occur regularly between IT and other divisions, and include upper management. The data protection officer communicates with management and individual operative divisions, and with the IT department. Additionally, an ”IT security officer“ exists.

Awareness of information protection is high and is promoted by training for new staff.

The enterprise understands risk management in its operative and IT divisions as a management responsibility and has installed standardized processes to assess and handle risks. The IT division is aware of most legal requirements and regulations.

Security technologies are implemented end-to-end based on risk assessment and all security issues concerning wireless networks, branches and home offices are clarified.

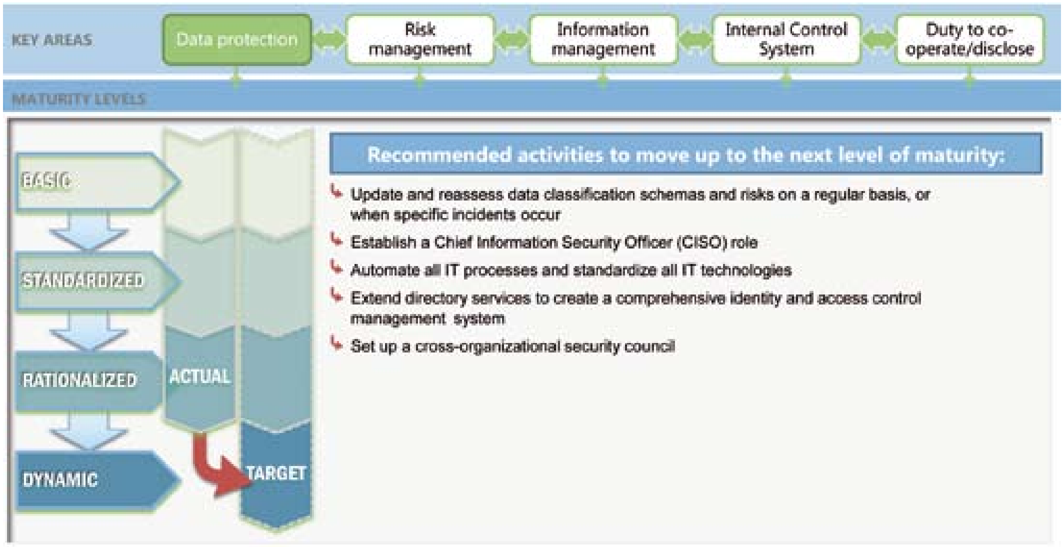
The enterprise often identifies security issues in good time and then triggers incident management activities. A comprehensive set of security policies exists and automated auditing tools are in place. Problem, configuration and change management are automated, as are monitoring and reporting.

The enterprise is addressing details of application and physical security. A consolidated document management solution is in place and the enterprise makes intensive use of business process management software.

Individual areas such as firewall and wide area networks (WAN) are managed by external service providers on the base of centrally defined service level agreements. Management of the client infrastructure including mobile devices is standardized. There is a centralized directory service and some initial identity management, including differentiated authentication methods.

All told, information technology is already acting as a business enabler and is clearly related to the enterprise's operative and strategic business. It makes a major contribution towards the implementation of regulatory requirements.

The following figure shows which activities are necessary to move up to the next maturity level.



Recommended activities to move up to the next level of maturity:

- Update and reassess data classification schemas and risks on a regular basis, or when specific incidents occur
- Establish a Chief Information Security Officer (CISO) role
- Automate all IT processes and standardize all IT technologies
- Extend directory services to create a comprehensive identity and access control management system
- Set up a cross-organizational security council

Figure 10: IT Infrastructure Compliance Maturity Model - Information protection: Activity plan RATIONALIZED - DYNAMIC

Dynamic

A data classification schema exists and has been implemented consistently throughout the enterprise. It is updated regularly, whenever changes occur (at least once a year). Data ownership and responsibilities are completely clarified and allocated. Awareness of information protection in the enterprise is very high. Training for new staff, but also for existing staff, promotes more awareness. IT stakeholders are aware of legal and regulatory requirements.

Coordination between IT, the divisions and the data protection officer takes place regularly and is institutionalized in the form of a security steering committee. The value of IT is accepted and rewarded at all levels.

The Chief Information Security Officer (CISO) works outside of IT and reports to the Chief Risk Management Officer or directly to the executive committee.

Risk management is implemented and managed consistently as a structured, enterprise-wide process. Acquisition, evaluation and documentation of risk management information are highly automated. Responses to business incidents that IT and information security need to consider are rapid.

Security technologies are implemented end-to-end based on risk assessment. A comprehensive set of security policies is in place and automated auditing tools are used.

Problem, configuration and change management are fully automated, as are monitoring and reporting. The security systems are continually monitored, as are defined service level agreements[3] by operative divisions and management. PCs and other devices infected by malware, or non-policy-compliant PCs and devices are automatically quarantined. Management and security are standardized on mobile devices and of the same standard as for PCs.

Comprehensive identity management is in place, including automatic provisioning (and blocking) of user accounts. Customers and partners are given orderly and secure access to selected systems and data on the enterprise network as needed.

All told, IT acts as a strategic resource and is fully embedded in the enterprise's operative and strategic business. IT is indispensable in the implementation of regulatory requirements.

Risk management

Entry Level - Basic

If at all, risk assessments are isolated, informal and irregular, typically within the scope of projects. Risk assessments are performed independently in various areas of the enterprise. They are largely ignored by management and there is a lack of training to promote staff awareness. Neither formal nor informal processes exist to identify and evaluate business risks, not to mention change management. The catalog of risk mitigation measures in the enterprise is inconsistent and not standardized. Security problems are typically addressed in a reactive manner.

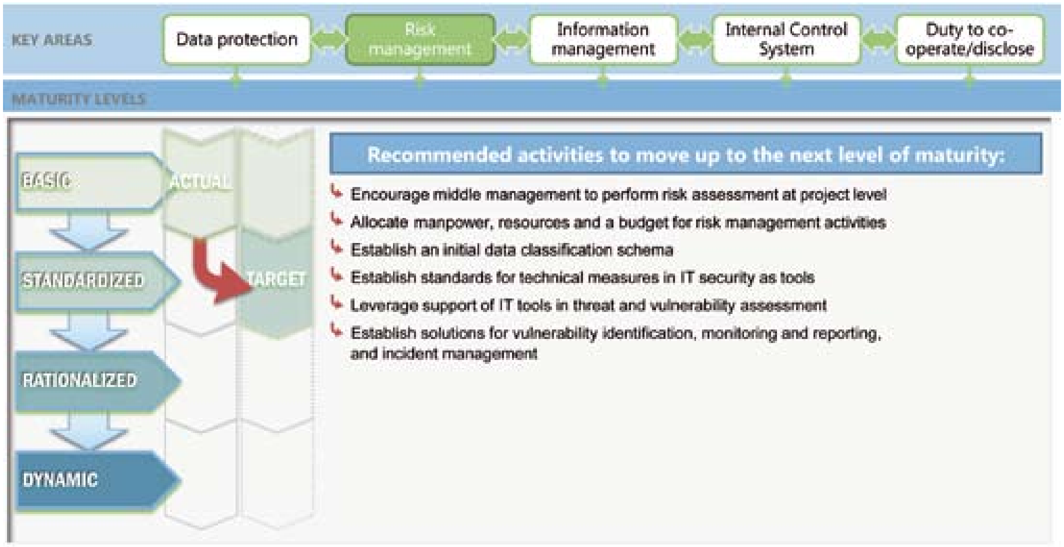
Existing IT infrastructures and tools are not used to automate risk assessment.

[3] In the broader sense of service level agreements (SLA)

With Respect to monitoring, vulnerability management, incident management and identity ma-nagement solutions, as well as data classification and protection, the enterprise is at the "Basic" information protection level, i.e. no risk management solutions are in place.

The IT department is simply regarded as a cost center. Compliance requirements are known only to the stakeholders in the individual functional areas, and they are addressed in isolated cases if at all.

The following figure shows which activities are necessary to move up to the next maturity level.



Recommended activities to move up to the next level of maturity:

- Encourage middle management to perform risk assessment at project level
- Allocate manpower, resources and a budget for risk management activities
- Establish an initial data classification schema
- Establish standards for technical measures in IT security as tools
- Leverage support of IT tools in threat and vulnerability assessment
- Establish solutions for vulnerability identification, monitoring and reporting, and incident management

Figure 11: IT Infrastructure Compliance Maturity Model - Risk Management: Activity plan BASIC - STANDARDIZED

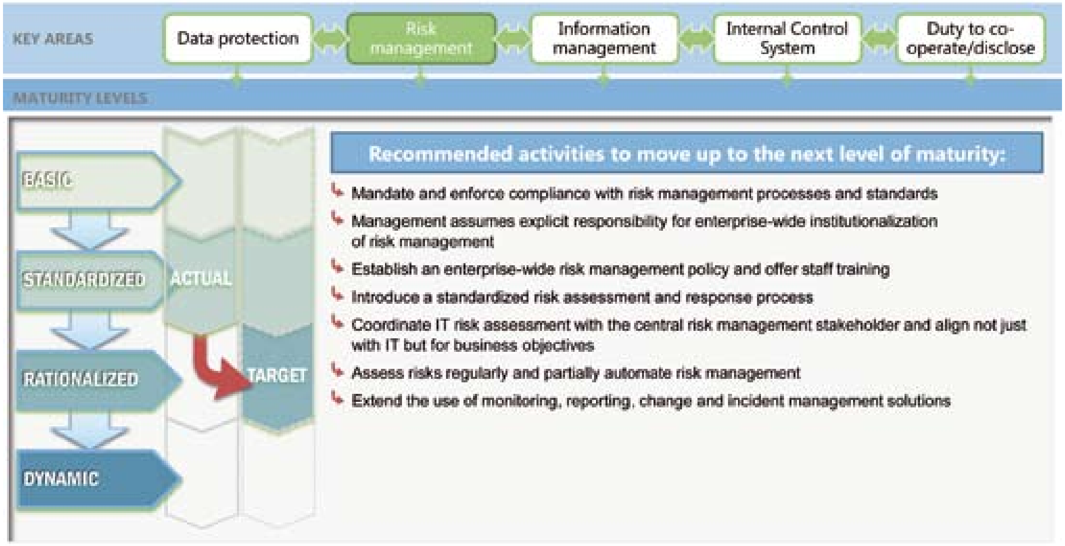
Standardized

At this stage, a basic, unified, bottom-up approach to the deployment of risk assessment is identifiable. Risk assessment occurs at project level – typically in the scope of large projects, or when problems have already occurred. Risk management as a process is used only superficially by the enterprise, and not as part of an enterprise-wide framework. There is no regular and structured training on the subject of risk management. When risks are identified, the enterprise uses isolated processes and standardized measures to mitigate them.

The enterprise is in the initial phase of data classification.

Existing IT infrastructures are only rarely used to automate risk assessment, and various departments in the enterprise work with a variety of risk management tools. Isolated vulnerability identification, monitoring and reporting, and incident management systems are deployed.

The following figure shows which activities are necessary to move up to the next maturity level.



Recommended activities to move up to the next level of maturity:

- Mandate and enforce compliance with risk management processes and standards
- Management assumes explicit responsibility for enterprise-wide institutionalization of risk management
- Establish an enterprise-wide risk management policy and offer staff training
- Introduce a standardized risk assessment and response process
- Coordinate IT risk assessment with the central risk management stakeholder and align not just with IT but for business objectives
- Assess risks regularly and partially automate risk management
- Extend the use of monitoring, reporting, change and incident management solutions

Figure 12: IT Infrastructure Compliance Maturity Model - Risk Management: Activity plan STANDARDIZED - RATIONALIZED

Rationalized

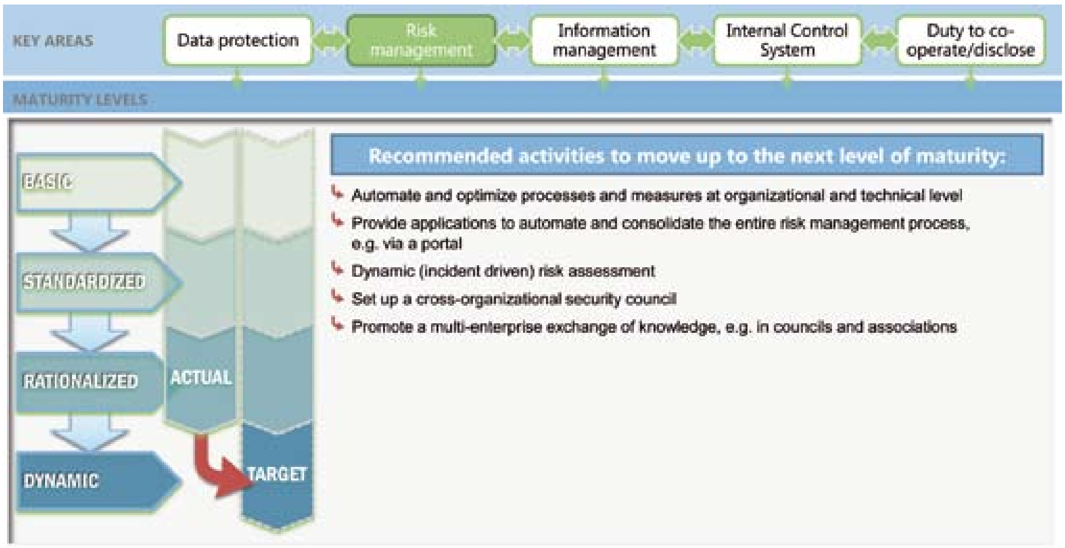
Risk management is an executive responsibility both in business operations and IT. Risks are evaluated and managed by standardized methods. An enterprise-wide risk management policy defines when and how risk assessment is performed. Executives are informed in case of deviations from the risk management process and appropriate measures are taken. At the same time, the management team is advised when changes in the business and IT environments occur that could have a significant impact on existing risk scenarios. Risks are addressed both at project level and regularly throughout IT.

IT risk management is tightly knit with business risk management and the exchange of information between the stakeholders is institutionalized. Additionally, a detailed data classification schema has been established. Management can evaluate the enterprise's total exposure and knows what level of residual risk it is prepared to accept. Identified risks are assigned to a single employee and both the board and the CIO define the risk levels they are prepared to tolerate.

In IT in particular, stakeholders develop standard methods to evaluate risks and perform cost/effectiveness analyses for countermeasures to be taken. Company management allocates budgets and resources to an operative risk management project to ensure that risks are investigated on a regular basis and to allow for reassessment if needed. Training promotes good awareness and is useful preparation for risk assessment.

A risk management database exists and parts of the risk management process are gradually being automated. In IT, risk mitigation strategies are establishing themselves. Information from existing identity, vulnerability and incident management solutions, and from monitoring and reporting is evaluated in a structured manner to support risk management.

The following figure shows which activities are necessary to move up to the next maturity level.



Recommended activities to move up to the next level of maturity:

- Automate and optimize processes and measures at organizational and technical level
- Provide applications to automate and consolidate the entire risk management process, e.g. via a portal
- Dynamic (incident driven) risk assessment
- Set up a cross-organizational security council
- Promote a multi-enterprise exchange of knowledge, e.g. in councils and associations

Figure 13: IT Infrastructure Compliance Maturity Model - Risk Management: Activity plan RATIONALIZED - DYNAMIC

Dynamic

At this level of maturity, risk management means a structured, enterprise-wide process that is deployed consistently. The enterprise continually optimizes the existing methods. Acquisition, evaluation and documentation of risk management information are highly automated. Risk management stakeholders act in a future-oriented manner and exchange views with experts outside the enterprise. Risk management is completely integrated with business and IT operations. It is highly accepted and covers IT users. Management reacts if larger operative decisions and investments in IT are made without taking the risk management plan into account. At the same time, it assesses risk mitigation strategies as part of an ongoing process. IT is optimized to reflect business interests and can adapt quickly to change. IT is a strategic resource in the enterprise.

Information management

Entry Level - Basic

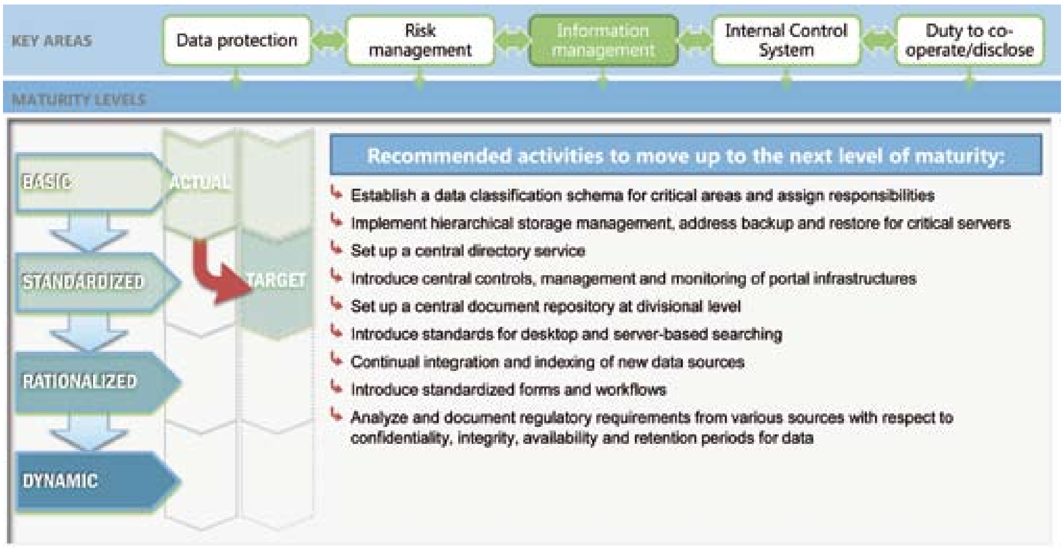
The enterprise does not have a data classification schema, and has not assigned owners and responsibilities for processing of specific data. The IT department lacks knowledge of confidentiality, integrity, availability, retention periods for data, and other legal requirements. Information handling is not guided by a risk management process. Authentication, authorization and access control for specific applications and information is insufficient. The enterprise lacks identity management, monitoring and reporting, and data encryption. Awareness of physical security requirements is low.

Information lifecycle management (ILM) and hierarchical storage management have not been implemented. Data backups are rudimentary and there are no tests of the ability to restore data and systems. This results in a very expensive IT infrastructure that barely supports business requirements. Cooperation is mainly based on email and personal meetings, and on shared access to file servers and public folders. Collaborative workspaces, static intranets and isolated portals are used in an ad hoc manner. These are typically legacy, isolate platforms. Static user lists exist, but the enterprise lacks a central directory service. Business process management solutions are not in place.

With respect to content handling, the enterprise uses local disks and shared file servers. Files are archived manually. Many processes are paper-based and data input is redundant.

Due to a lack of standard search technologies, information is difficult to retrieve. Searches are typically performed in silo structures which are used only by isolated members of staff. The focus is on email, desktop or server based documents and webpages. Very little in the line of business intelligence functionality exists; reporting and automation are very restricted, and data analysis is based mainly on Excel sheets.

The following figure shows which activities are necessary to move up to the next maturity level.



Recommended activities to move up to the next level of maturity:

- Establish a data classification schema for critical areas and assign responsibilities
- Implement hierarchical storage management, address backup and restore for critical servers
- Set up a central directory service
- Introduce central controls, management and monitoring of portal infrastructures
- Set up a central document repository at divisional level
- Introduce standards for desktop and server-based searching
- Continual integration and indexing of new data sources
- Introduce standardized forms and workflows
- Analyze and document regulatory requirements from various sources with respect to confidentiality, integrity, availability and retention periods for data

Figure 14: IT Infrastructure Compliance Maturity Model - Information Management: Activity plan BASIC - STANDARDIZED

Standardized

A basic data classification schema is in place, but it is built on intuition and not consistent throughout the enterprise. Data ownership and responsibility is typically assigned, but there are some loopholes.

Information protection measures are typically but not consistently based on risk assessments. Isolated training in information handling takes place in critical areas.

The IT department has incomplete knowledge of confidentiality, integrity, availability, retention periods for data, and other legal requirements. Authentication, authorization and access control mechanisms for specific applications and data exist but are not completely standardized. Monitoring, reporting and data encryption is isolated.

Some awareness of physical security requirements exists, however, there is room for improvement.

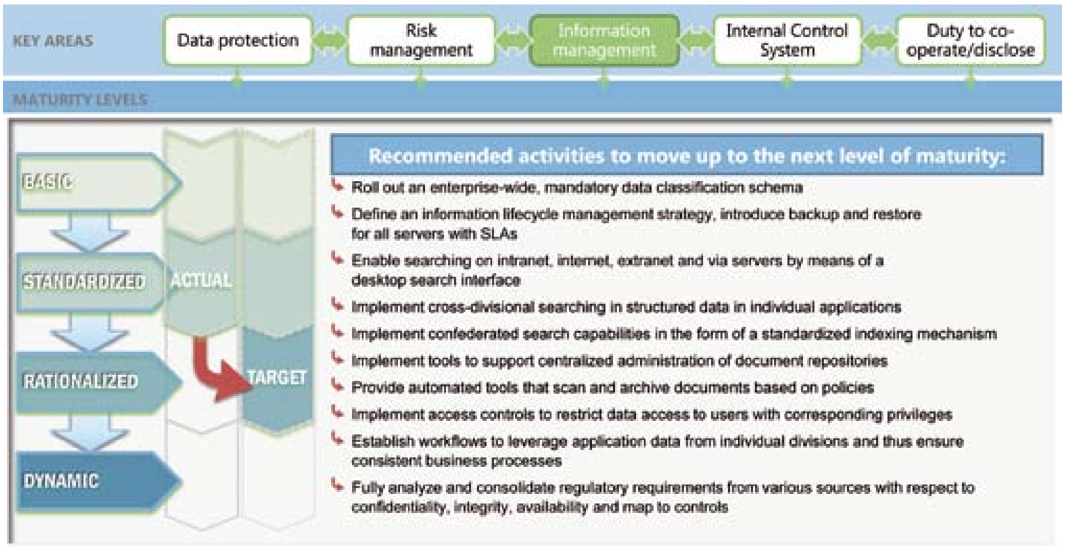
Hierarchical storage management is in place in some areas; however, the enterprise lacks a detailed strategy for information lifecycle management. System backup and restore mainly exist for critical servers. This results in a slightly more cost-effective IT infrastructure that provides limited support to business requirements.

There is an enterprise-wide infrastructure that supports shared workspaces with content versioning and various portals. However, superordinate controls are not fully in place.

The enterprise uses a centralized directory service that includes access to the portals. Business process management solutions are used in various areas.

With respect to content handling, the enterprise relies on isolated document repositories where content is consolidated and documents are archived. Transaction processes are mainly form-based.

Information retrieval is highly complex; however, there is at least some basic functionality for desktop and server searching. Granular searching is basic and text-based, based on document properties and divisions such as human resources. There is a shared search index for various data sources such as websites, content management systems, email, databases and employee directories. Individual divisions use business intelligence in a standardized way. Reporting and assessment are partly automated, although highly IT-related.



Recommended activities to move up to the next level of maturity:

- Roll out an enterprise-wide, mandatory data classification schema
- Define an information lifecycle management strategy, introduce backup and restore for all servers with SLAs
- Enable searching on intranet, internet, extranet and via servers by means of a desktop search interface
- Implement cross-divisional searching in structured data in individual applications
- Implement confederated search capabilities in the form of a standardized indexing mechanism
- Implement tools to support centralized administration of document repositories
- Provide automated tools that scan and archive documents based on policies
- Implement access controls to restrict data access to users with corresponding privileges
- Establish workflows to leverage application data from individual divisions and thus ensure consistent business processes
- Fully analyze and consolidate regulatory requirements from various sources with respect to confidentiality, integrity, availability and map to controls

Figure 15: IT Infrastructure Compliance Maturity Model - Information Management: Activity plan STANDARDIZED - RATIONALIZED

Rationalized

A data classification schema exists for the most part and has been implemented consistently throughout the enterprise. Data ownership and responsibilities are clarified and allocated to a great extent. The IT department is typically aware of confidentiality, integrity, availability, retention periods for data, and other legal requirements and they are taken into consideration in risk assessments.

Authentication, authorization and access controls for specific applications and information are standardized for the main part, as are monitoring and reporting, and data encryption. Physical security is an integral part of information management.
Hierarchical storage management is in place for the most part, and a detailed information lifecycle management strategy does exist, although it has not been implemented consistently.

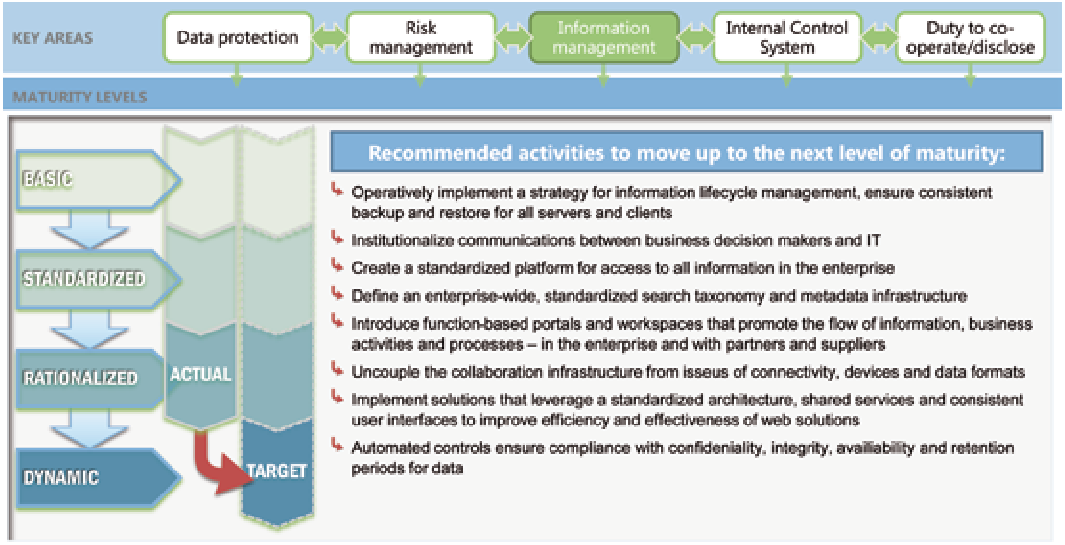
System backup and restore are performed for all servers on the basis of service level agreements. Additionally, centralized backups have been introduced for branch offices. This results in a rationalized IT infrastructure that provides full support to business requirements.

The enterprise has a standardized collaboration and portal infrastructure with central controls. This connects employees and external groups, processes and information throughout the enterprise in a secure manner. Collaboration methods are mature; if needed, documents can be taken offline, and content-based social computing functionality is integrated with the existing infrastructure.

Integrated document repositories exist to manage and archive documents and files. They support sophisticated searches for data relating to persons or departments. Data retention is automated and ensures structured archiving of relevant content, e.g. for HR data. The infrastructure allows editing and publishing of content on the intranet, extranet, or for Internet sites. Electronic, form-based solutions are in place and support enterprise-wide business processes. Business process management solutions are established and standardized.

The business optimization potential of being able to search for information is recognized at this level of maturity. Searches are possible across various platforms, such as desktops, servers, portals, databases and content management systems, specific departmental applications and employee information – also against the backdrop of social computing. Data management including assessment and reporting functions is centralized. It is standardized and consolidated throughout the enterprise.

The following figure shows which activities are necessary to move up to the next maturity level.



Recommended activities to move up to the next level of maturity:

- Operatively implement a strategy for information lifecycle management, ensure consistent backup and restore for all servers and clients
- Institutionalize communications between business decision makers and IT
- Create a standardized platform for access to all information in the enterprise
- Define an enterprise-wide, standardized search taxonomy and metadata infrastructure
- Introduce function-based portals and workspaces that promote the flow of information, business activities and processes – in the enterprise and with partners and suppliers
- Uncouple the collaboration infrastructure from isseus of connectivity, devices and data formats
- Implement solutions that leverage a standardized architecture, shared services and consistent user interfaces to improve efficiency and effectiveness of web solutions
- Automated controls ensure compliance with confideniality, integrity, availability and retention periods for data

Figure 16: IT Infrastructure Compliance Maturity Model - Risk Management: Activity plan RATIONALIZED - DYNAMIC

Dynamic

An enterprise-wide and consistent data classification schema exists. It is updated regularly, whenever changes occur, at least once a year. Data ownership and responsibilities are completely clarified and allocated. The IT department is aware of confidentiality, integrity, availability, retention periods for data, and other legal requirements and demonstrably implements them at the technical and organizational level.

A detailed information lifecycle management strategy exists and is in place in many areas of the enterprise. System backup and restore are now performed consistently and include clients. This leads to a dynamic IT infrastructure that fully supports business requirements and shapes business activities in part.

The enterprise has a standardized and integrated collaboration and portal infrastructure. The infrastructure links a variety of groups within and outside of the enterprise and gives them access to the required persons, processes and information.

The organization is capable of building modular applications within a role-based environment. Social computing abilities are highly represented and promote relationships beyond the confines of the enterprise.

Document management and retention have been optimized. Files are quickly found via a standardized search infrastructure.

Access to intranet, internet and extranets is customized thanks to comprehensive identity management. Processes are defined to be cross-departmental, multi-system and valid beyond the enterprise borders using standardized tools to support business process management.

The enterprise uses a common, standardized infrastructure to search for information. It covers both structured and unstructured information. The user interface is consistent and context sensitive. The data classification schema is also used for a standard taxonomy of critical business data.

Internal control system

Entry Level - Basic

At this level only a fragmentary internal control system exists, and it receives little support from IT. Neither the two-pairs-of-eyes nor the segregation-of-duties nor the need-to-know principle is adhered to. Control targets and mechanisms are rudimentary, as are documentation and transparency. The enterprise does not have a system of metrics to measure the efficiency of ICS. Business process management solutions are not in place.

Legal and regulatory requirements are unknown in IT for the most part, and communications between IT stakeholders on the one hand and the management, process owners, internal auditing, and external auditors on the other is a matter of chance or does not happen at all.

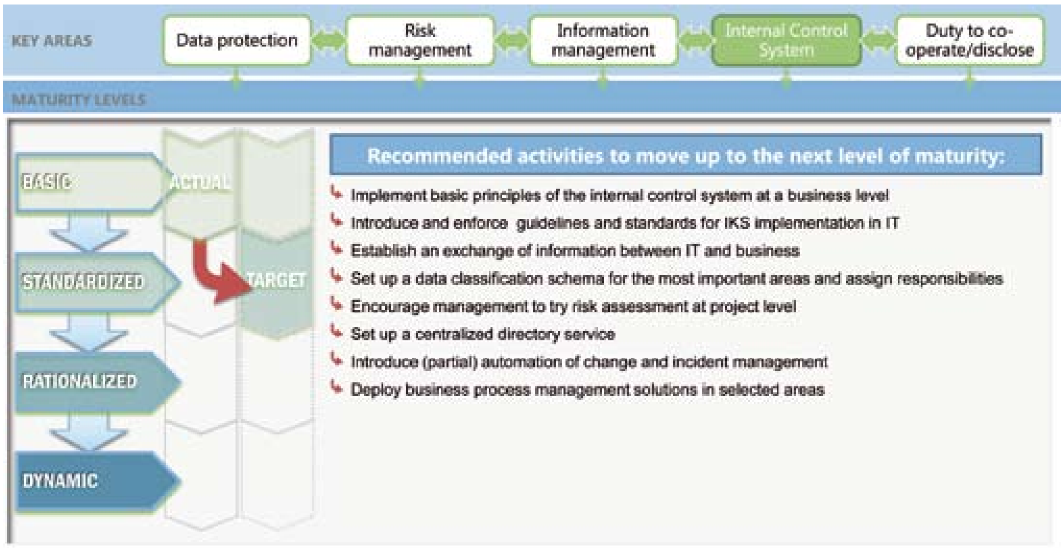
The enterprise does not have data classification schema, and has not assigned owners and responsibilities for processing of specific data.

Awareness of internal controls and security is very low in the enterprise. If at all, risk asessments are isolated, informal and irregular, typically within the scope of projects.

The enterprise handles problem and change management ad hoc by ”fire fighting“ and without information flowing between IT and the operative divisions. System monitoring is restricted to servers and not automated. Security issues are identified by chance or after system failure. It is highly likely that nobody would notice the loss of confidential data.

Various directory services may be in use; however, there is no centralized directory service and no identity management. This explains why IT finds it difficult to implement the segregation-of-duties principle.

The following figure shows which activities are necessary to move up to the next maturity level.



Recommended activities to move up to the next level of maturity:

- Implement basic principles of the internal control system at a business level
- Introduce and enforce guidelines and standards for IKS implementation in IT
- Establish an exchange of information between IT and business
- Set up a data classification schema for the most important areas and assign responsibilities
- Encourage management to try risk assessment at project level
- Set up a centralized directory service
- Introduce (partial) automation of change and incident management
- Deploy business process management solutions in selected areas

Figure 17: IT Infrastructure Compliance Maturity Model - Internal Control System: Activity plan BASIC - STANDARDIZED

Standardized

An internal control system is in place; however, it is not adequately supported by IT. Both internal controls for IT management and the implementation of the enterprise-wide, internal control system is typically ad hoc and isolated. Only a few metrics exist to measure the effectiveness of the ICS. But at least standards for internal controls are slowly establishing themselves. Business process management solutions are occasionally used.

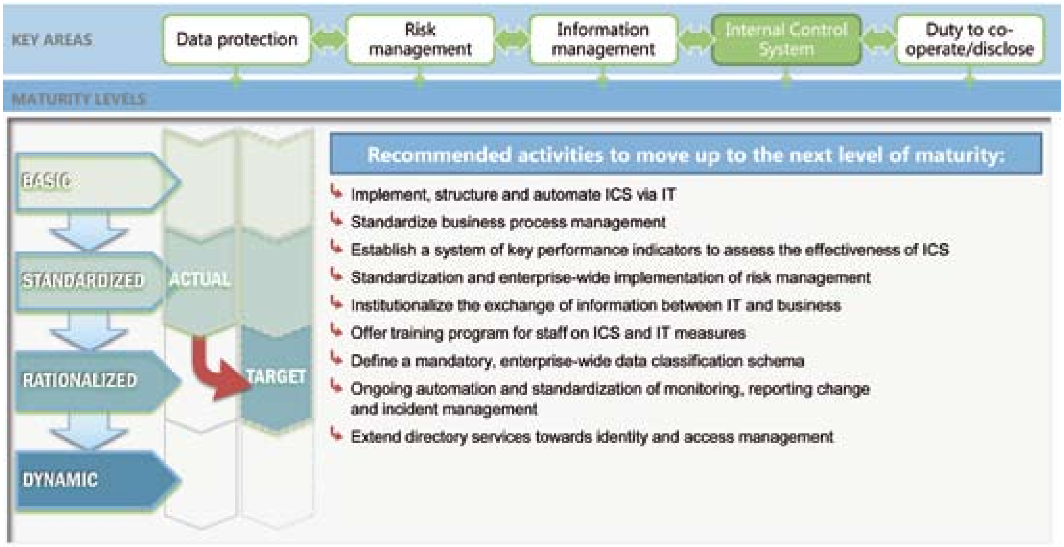
Legal and regulatory requirements are partly unknown to IT, and communications between IT stakeholders on the one hand and the management, process owners, internal auditing, and external auditors on the other are not institutionalized.

A basic data classification schema is in place, but it is built on intuition and not deployed throughout the enterprise. Risk assessments are performed in the scope of projects only.

Standardization is gradually gaining ground, however, documentation does not exist enterprise-wide.

Problem and change management are only partly standardized and automated. A strategy for handling security problems exists and critical servers are monitored 24x7. All told, security problems are not always identified, and monitoring involves considerable personnel overhead. There is a centralized directory service, but it does not include comprehensive identity management.

The following figure shows which activities are necessary to move up to the next maturity level.



Recommended activities to move up to the next level of maturity:

- Implement, structure and automate ICS via IT
- Standardize business process management
- Establish a system of key performance indicators to assess the effectiveness of ICS
- Standardization and enterprise-wide implementation of risk management
- Institutionalize the exchange of information between IT and business
- Offer training program for staff on ICS and IT measures
- Define a mandatory, enterprise-wide data classification schema
- Ongoing automation and standardization of monitoring, reporting change and incident management
- Extend directory services towards identity and access management

Figure 18: IT Infrastructure Compliance Maturity Model - Internal Control System: Activity plan STANDARDIZED - RATIONALIZED

Rationalized

An internal control system has been established; it is well-supported by IT and automated. The ICS and IT controls and/or IT governance collaborate closely. The effectiveness of the ICS is measured by a basic system of metrics. Standardized business process management solutions are in place throughout the enterprise.

Risk management is an executive responsibility both in business operations and IT. Standardized methods are used to assess and manage risks. The IT department is familiar with legal and regulatory requirements. Communications between IT stakeholders on the one hand and the management, process owners, internal auditing, and external auditors on the other are institutionalized for the most part. All told, awareness of the relevance of the ICS and necessary measures is high in IT, mainly thanks to a working training program for staff, including IT. The fact that a function has been created to handle internal controls in IT is a big help.

A data classification schema exists for the most part and has been implemented consistently throughout the enterprise. Data ownership and responsibilities are clarified and allocated to a great extent.

Security problems are often identified in good time and lead to incident management activities. A comprehensive set of security policies exists and automated auditing tools are in place. Problem, configuration and change management are widely automated, as are monitoring and reporting.

The enterprise has a central directory service and basic identity management, including a differentiated authentication method. All told, IT acts as an enabler for business operations and more specifically for ICS.

The following figure shows which activities are necessary to move up to the next maturity level.

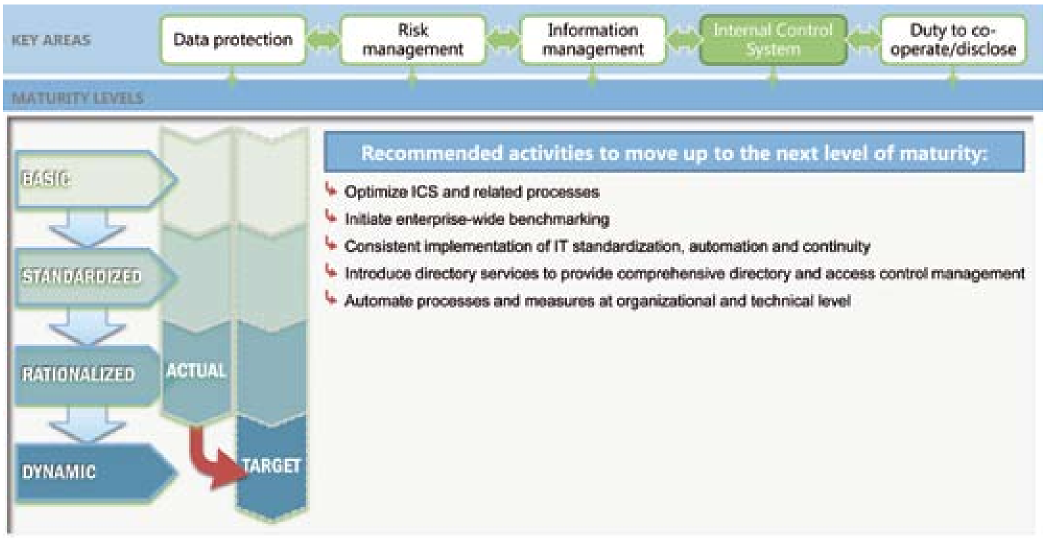

KEY AREAS
Data protection
Risk management
Information management
Internal Control System
Duty to co-operate/disclose
MATURITY LEVELS
BASIC
STANDARDIZED
RATIONALIZED
DYNAMIC
ACTUAL
TARGET
Recommended activities to move up to the next level of maturity:
Optimize ICS and related processes
Initiate enterprise-wide benchmarking
Consistent implementation of IT standardization, automation and continuity
Introduce directory services to provide comprehensive directory and access control management
Automate processes and measures at organizational and technical level

Figure 19: IT Infrastructure Compliance Maturity Model - Internal Control System: Activity plan RATIONALIZED - DYNAMIC

Dynamic

At this level, it is a question of optimizing the existing internal control system and related processes. To this end, management initiates an enterprise-wide continual improvement program that integrates knowledge management, best practices and assessment of relevant metrics. In this context the enterprise takes a farsighted step and institutionalizes benchmarking. The exchange of information within the enterprise and training are highly targeted.

Risk management is implemented and managed consistently as a structured, enterprise-wide process. Acquisition, evaluation and documentation of risk management information is highly automated. Response times to business incidents with relevance to IT and information security drop considerably.

A data classification schema exists and has been implemented consistently throughout the enterprise. It is updated regularly whenever changes occur, at least once a year.
Data ownership and responsibilities are completely clarified and allocated. Legal and regulatory requirements are known in IT.

Problem, configuration and change management are fully automated, as are monitoring and reporting. Security systems are monitored and evaluated 24x7, as are service level agreements in operations and management.

The enterprise uses a comprehensive identity management system including automated provisioning (and blocking) of user accounts. Customers and partners are given orderly and secure access to selected systems and data on the enterprise network as needed. The principles of segregation-of-duties and two-pairs-of-eyes are fully supported.

Duty to cooperate and disclose

Entry Level - Basic

At the entry level, the company is hardly capable of fulfilling its duties to cooperate and disclose in line with regulatory requirements. Compliance requirements are virtually unknown in IT. The enterprise does not have a process or contingency planning to trigger proactive fulfillment of its duties to cooperate and disclose. If at all, the company only reacts to these duties, for example, in the case of a major information protection incident, or – less commonly – as a response to an audit.

The reason for this is that communications between IT and business are haphazard. The finance division only fulfills basic obligations vis-à-vis the fiscal authorities, but without involvement of and controls by IT.

The enterprise does not have a data classification schema, and has not assigned owners and responsibilities for processing of specific data. It is unclear who is allowed to communicate what information externally in case of an incident.

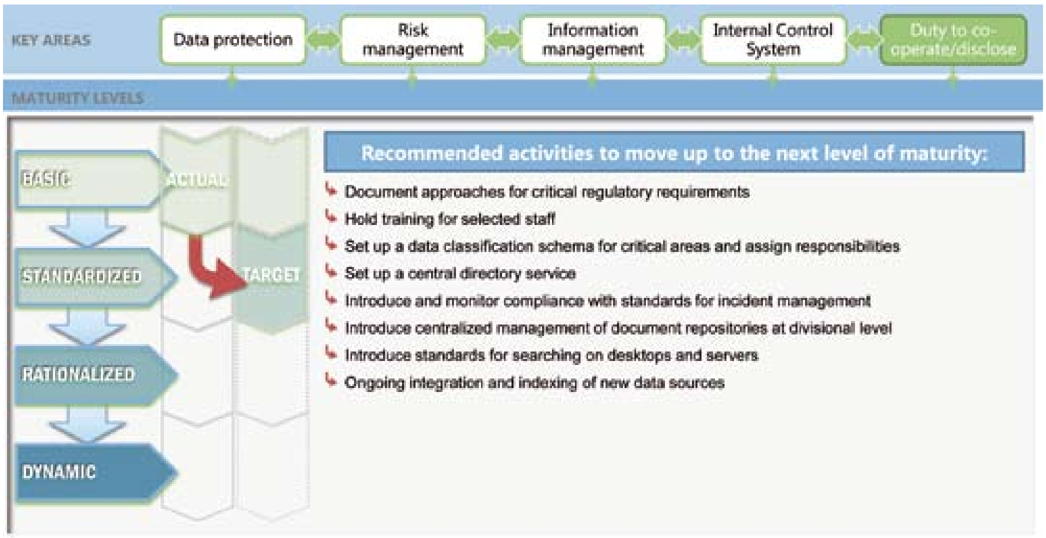
Incident management is handled in an ad hoc manner by "fire fighting." System monitoring is restricted to servers and not automated. Security issues are identified by chance or after system failure. It is highly likely that nobody would notice the loss of confidential data – it would thus be impossible to inform stakeholders.

Authentication, authorization and access control for specific applications and information are insufficient. The enterprise also lacks identity management, monitoring and reporting, and data encryption. If at all, the enterprise uses freely available encryption solutions provided by the external organizations to be notified (such as federal agencies or associations). Static user lists exists, but the enterprise lacks a central directory service. Thus, a secure and orderly information process is not ensured.

Content handling is restricted to storage on local disks and shared file servers. Files are archived manually.

Many processes are paper-based and data input is redundant. Due to a lack of standard search technologies, information is difficult to retrieve. Searches are typically performed in silo structures which are used only by isolated members of staff. This makes it extremely difficult for the enterprise to fulfill its duties to cooperate and disclose in good time.

The following figure shows which activities are necessary to move up to the next maturity level.



Recommended activities to move up to the next level of maturity:

- Document approaches for critical regulatory requirements
- Hold training for selected staff
- Set up a data classification schema for critical areas and assign responsibilities
- Set up a central directory service
- Introduce and monitor compliance with standards for incident management
- Introduce centralized management of document repositories at divisional level
- Introduce standards for searching on desktops and servers
- Ongoing integration and indexing of new data sources

Figure 20: IT Infrastructure Compliance Maturity Model - Duty to Cooperate and Disclose: Activity plan BASIC - STANDARDIZED

Standardized

At this level of maturity, the enterprise fulfills its obligation to cooperate for the main part, for example in finance. However, it lacks institutionalization of third party information in case of a ”crisis.“ Legal and regulatory requirements are not always known in IT. Processes for compliance with the company‘s duty to cooperate and disclose have not been standardized throughout, but there are some initial, documented approaches for regulatory requirements considered ”critical.” As handling of these obligations is still closely tied in to the knowledge of individual employees, implementation is error-prone and not consistently reproducible.

Communications between IT and business are typically ad hoc with respect to compliance. The enterprise organized isolated training for staff in key areas, especially in finance.

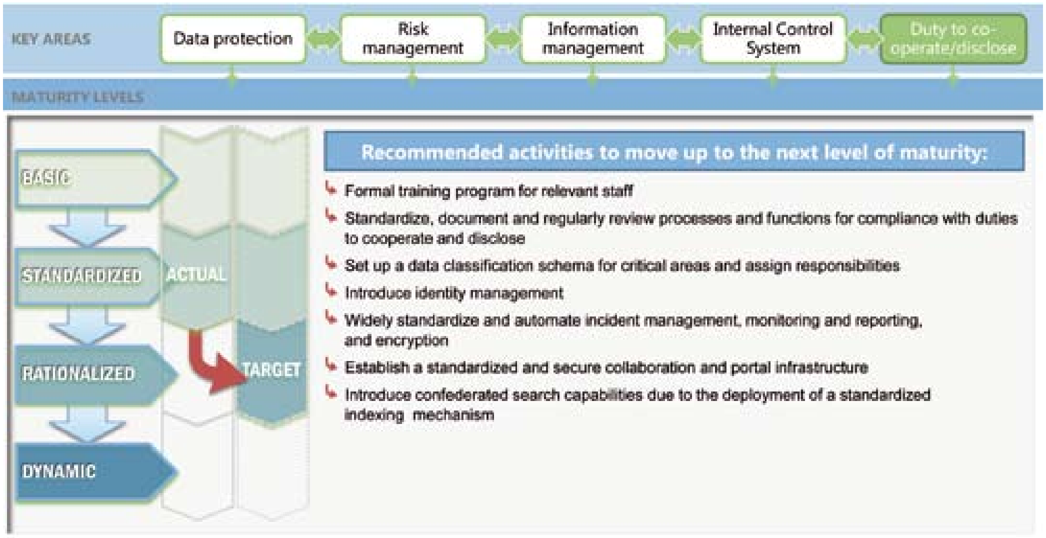
A basic data classification schema is in place, but it is built on intuition and not deployed throughout the enterprise. Encryption solutions are used in isolated cases. There is a centralized directory service, but it does not include comprehensive identity management. This means that it is still possible for unauthorized persons to misuse the company‘s obligation to disclose or to spy out information.

Problem and change management are only partly standardized and automated. A strategy for handling security problems exists and critical servers are monitored 24x7. Despite this, security problems are not always identified, and monitoring involves considerable personnel overhead. As a result, the enterprise has a limited ability to inform external stakeholders of problems that impact them – for example in the field of information protection.

Retrieving information – for example following a court order – involves considerable overhead, but some basic functionality for desktop and server based searching is available. Granular searching is basic and text-based, based on document properties and divisions such as human resources. There is a shared search index for various data sources such as websites, content management systems, email, databases and employee directories.

This helps the company's IT at least to react to queries by external stakeholders and to provide information with a manageable overhead.

The following figure shows which activities are necessary to move up to the next maturity level.



Recommended activities to move up to the next level of maturity:

- Formal training program for relevant staff
- Standardize, document and regularly review processes and functions for compliance with duties to cooperate and disclose
- Set up a data classification schema for critical areas and assign responsibilities
- Introduce identity management
- Widely standardize and automate incident management, monitoring and reporting, and encryption
- Establish a standardized and secure collaboration and portal infrastructure
- Introduce confederated search capabilities due to the deployment of a standardized indexing mechanism

Figure 21: IT Infrastructure Compliance Maturity Model - Duty to Cooperate and Disclose: Activity plan STANDARDIZED - RATIONALIZED

Rationalized

The enterprise is now in an excellent position to fulfill its duties to cooperate and disclose. Legal and regulatory requirements are widely known in IT.

This is supported by a formal and binding training program for all staff involved in these duties.
The enterprise has – for the main part – standardized and documented its processes for compliance with its duties to cooperate and disclose. Functions and responsibilities are clear and transparent. Regular audits take place to assess the effectiveness of the cooperation and disclosure processes.

A data classification schema exists for the most part and has been implemented consistently throughout the enterprise. This also applies to data owners and responsibilities. Authentication, authorization and access controls for specific applications and information are standardized for the main part, as are monitoring and reporting, and data encryption. This helps the enterprise to ensure that mandatory disclosures are made only by persons authorized to do so, and that information is kept confidential.

Security problems are often identified in good time and lead to incident management activities.

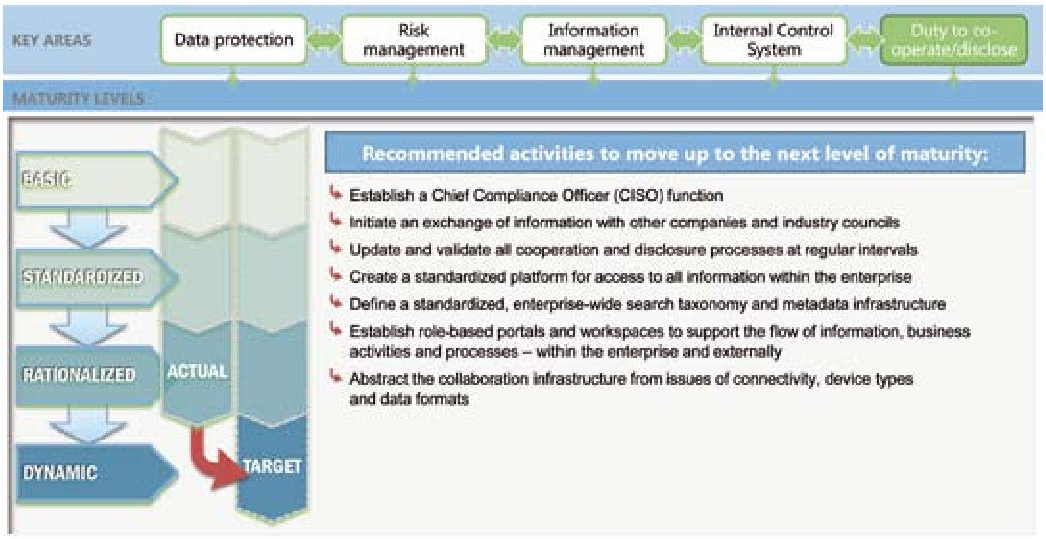
A comprehensive set of security policies exists and automated auditing tools are in place. Problem, configuration and change management are automated, as are monitoring and reporting. This puts the enterprise in a good position to inform external advocacy groups about problems that relate to them, for example, in information protection.

The enterprise has a standardized collaboration and portal infrastructure with centralized controls. This connects employees and external groups, processes and information throughout the enterprise in a secure manner. Collaboration processes are mature, and documents can be taken offline if needed. Confidential material is always encrypted before transmission. At the same time, this infrastructure can be used to report to associations, customers and authorities, wherever policies allow this to happen.

Integrated document repositories exist to manage and archive documents and files. They support sophisticated searches for persons or department-related data. Data retention is automated and ensures structured archiving of relevant content, e.g. for HR data.

The business optimization potential of being able to search for information is recognized at this level of maturity. It is supported across various platforms – such as clients, servers, portals, databases, document and content management systems, and specific applications in the enterprise's divisions for structured and unstructured formats.

The following figure shows which activities are necessary to move up to the next maturity level.



Recommended activities to move up to the next level of maturity:

- Establish a Chief Compliance Officer (CISO) function
- Initiate an exchange of information with other companies and industry councils
- Update and validate all cooperation and disclosure processes at regular intervals
- Create a standardized platform for access to all information within the enterprise
- Define a standardized, enterprise-wide search taxonomy and metadata infrastructure
- Establish role-based portals and workspaces to support the flow of information, business activities and processes – within the enterprise and externally
- Abstract the collaboration infrastructure from issues of connectivity, device types and data formats

Figure 22: IT Infrastructure Compliance Maturity Model - Duty to Cooperate and Disclose: Activity plan RATIONALIZED - DYNAMIC

Dynamic

At this level the enterprise optimizes its processes for compliance with its duties to cooperate and disclose. A function has been defined to exclusively handle the coordination of corresponding measures and compliance with regulatory requirements. Planning actively addresses the future to ensure continuity in compliance with external requirements. The processes are so well established that training mainly focuses on new staff.

At the same time, the enterprise leverages the exchange of information with other companies and committees in the industry to actively influence new regulations and/or address them in line with best practices.

The consistent data classification schema is updated regularly, whenever changes occur (at least once a year). Data ownership and responsibilities are completely clarified and allocated.

The enterprise has a standardized and integrated collaboration and portal infrastructure. The infrastructure links a variety of groups within and outside of the enterprise and gives them access to the required persons, processes and information. The organization is capable of building modular applications within a role-based environment. Access to intranet, internet and extranets is customized thanks to comprehensive identity management. This ensures maximum efficiency and security in the enterprise's duty to disclose to other enterprises.

Document management and retention have been optimized. Files are easily retrieved thanks to a standardized search infrastructure. The enterprise uses a common, standardized infrastructure to search for information. It covers both structured and unstructured information. The user interface is consistent and context sensitive. The data classification schema is also used for a standard taxonomy of critical business data. This accelerates information retrieval, which in turn adds efficiency and improves the quality both in the handling of regular cooperation duties and in incident-driven disclosure.

Overall compliance maturity model – Case study

For more clarity, it is sensible to visualize overall maturity in the form of an overview. This clearly reveals the key areas in which the enterprise has scope for improvement. We will be using a fictive company named Contoso to illustrate this in the following.

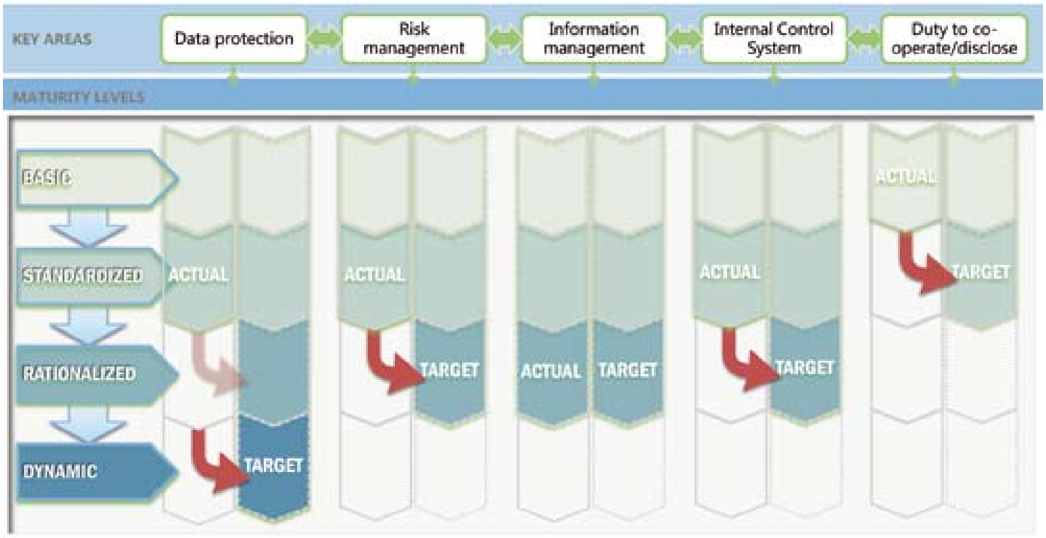


Figure 23: IT Infrastructure Compliance Maturity Model – Fictive Example Contoso

With respect to **information protection,** Contoso has achieved a ”standardized” level of maturity. In some areas, especially in research and development as well as finance, the enterprise demonstrates a solid technical approach to addressing information protection issues. However, the enterprise is gradually starting to appreciate the fact that it cannot protect information end-to-end in this way. For this reason, Contoso is looking to roll out its data classification schema enterprise-wide and leverage the schema with respect to information protection. A framework of security policies will support this project.

Contoso has also achieved a ”standardized“ maturity level with respect to **risk management.** However, discussions between the CIO and the Chief Risk Manager have revealed that the flow of information with regard to the risk situation between IT and business is still very incomplete. For this reason, the company will be looking to install binding risk management standards and processes at the next step. This will involve introducing a standard risk assessment method and process in risk management. On top of this, Contoso will be introducing a formal training program on the topic of risk management.

Contoso is looking to implement these measures along with its information protection planning and to leverage existing monitoring and reporting as well as change and incident management solutions more effectively in the context of risk management.

Contoso is in a good position with respect to **information management** and has reached the ”rationalized” level. The motivation originally came from technical decision makers in research and development, production, logistics and distribution. By now, enterprise-wide standards have been established for content management, collaboration and business assessment. The enterprise is now focusing on interruption-free operations as a multiple day production outage would cost the company a huge amount of money. Contoso views the current maturity level as sufficient for the next two years and plans to leverage its achievements in the area of information management more intensively for other areas such as information protection and risk management.

With respect to the **internal control system** Contoso has achieved the "standardized" level. The company has set up an internal control system; however, it is not sufficiently supported by IT. Both internal controls for IT management and the implementation of the enterprise-wide, internal control system is typically ad hoc and isolated. Contoso would therefore like to promote the exchange of information between IT stakeholders, the management, process owners, internal auditing and external auditors. The company sees itself making considerable progress thanks to the risk management measures it has planned. To test effectiveness of ICS, Contoso is currently establishing a key indicator system.

Contoso has so far widely ignored its duty to **cooperate and disclose** and currently finds itself at the "basic" maturity level. Contoso does not have process or contingency planning to trigger proactive fulfillment of its duties to cooperate and disclose. So far, the stakeholders at Contoso have been happy to say that "everything has worked out fine." Activities in the fields of information protection and risk management have now provoked an increasing awareness of these duties – and the risks of non-compliance. Contoso is now planning to at least identify the most important regulatory requirements and document approaches and best practices in this context. The company is intending to use standardized approaches to incident management in the course of this change.

7. AUTHORS

Wolfram Funk is a Senior Advisor with the Experton Group. Funk's focus is on advising ICT service providers, manufacturers and telecommunications service providers in topics of market research and go-to-market strategies. He specifically focuses on information security and ICT convergence. Funk also advices enterprise-level users on security and risk management and sourcing of security solutions and services. Before joining Experton Group AG in 2005, Funk was Senior Consultant, Vendor Consulting with META Group Deutschland GmbH. Between 1997 and 1999, he worked in Sales and Marketing for Xcc Software AG. In this position he was jointly responsible for strategic market research and envisioning and implementation of the mid-sized IT service provider's marketing strategy. Funk has a degree in industrial engineering from the University of Karlsruhe (TH) and is a Certified Information Security Manager (CISM, ISACA).

Kristina Javorková is specialist in the field of IT law and employed by Microsoft GmbH in Germany. She focuses on information protection and IT security, especially on compliance aspects. Javorková's expertise extends beyond legal questions to cover the practical and business requirement optimized implementation of regulatory compliance. In the past, she has gained experience in compliance issues with a number of major law firms of international repute and is currently working on a PhD on the subject of "The Impact of European Jurisdiction on IT Deployment in the Enterprise (IT Compliance) with Particular Reference to Data Protection" at the Karls University Prague. Javorková has also gained much experience by participating in various pan-European IT compliance legal advisory projects.

Michael Kranawetter possesses a well-founded background in economics after studying the subject at university, and owes his wide spectrum of knowledge in various information processing disciplines to 15 years of experience in the IT industry. As a project manager and consultant Kranawetter successfully implemented a number of major infrastructure projects before taking on various international positions with a global reinsurer as a project manager, architect, chief designer and strategist in the field of enterprise architecture, service management and IT governance, as well as directory services and portal strategies. In the last three years Kranawetter was responsible for the internal, globally active Security Audit Team and for information security risk management, compliance and governance as Program Manager Risk Assessment. He now works for Microsoft as Chief Information Security Advisor (CSA). In this function, Kranawetter works with Chief (Information) Security Officers on the subjects of governance, risk and compliance and Microsoft's information security strategy. His Kranawetter's experience in information technology is reflected by three international certifications (CISM, CISA, CIPP).

8. IT INFRASTRUCTURE SOLUTIONS RELEVANT TO COMPLIANCE

This section presents the technology solution categories that are relevant to GRC. This white paper has investigated the technology solution categories required to implement common standards and regulations. We can identify 19 solution categories. The following list was validated for relevance and compliance with common standards including ISO 27002, National Institute of Standards and Technology (NIST SP800) recommendations, and other frameworks.

Application Security
Application security solutions combine good development practices with specific software security.

Authentication, Authorization, and Access Control
Authentication usually involves a user name and a password, but it can include additional methods to demonstrate identity, such as a smart card, retina scan, voice recognition, or fingerprints. Authorization focuses on determining whether someone (after they are identified) is permitted to access requested resources. Access is granted or denied depending on a wide variety of criteria, such as the network address of the client, the time of day, or the browser that the person uses.

Change Management
Change management systems are process structures that cause IT managers to review proposed changes for technical and business readiness in a consistent manner. IT stakeholders can then restrict or extend changes to adjust to business needs.
For example, an organization could introduce a database to help staff make better decisions and changes based on historical data that indicate the success or failure of similar changes it has tried in the past. Change management is also a structured process that communicates the status and existence of changes to all stakeholding parties. This leads to an ”inventory system“ that indicates what actions were taken, when and by whom. This in turn affects the status of key resources required to identify problems and manage resources.

Data Classification and Protection
This category deals with the classification of data, for example by protection requirements, and the application of these classifications to data either stored on a computer or in transmission. This solution category also addresses the question of information protection in terms of providing confidentiality and integrity to data stored on hard disks or in transmission. Cryptographic solutions are the most common technology that organizations use to provide information protection.

Disaster Recovery and Failover
If a natural or man-made disaster occurs, information systems must be restored to an operational status as quickly as possible. This is precisely what disaster recovery and failover means. Failover refers to redundant systems that operate parallel to the operational systems at all times. It makes sense to operate these systems in different geographical regions.

Document Management
Document management solutions combine software and processes to help enterprises manage unstructured information. This information might exist in many digital forms. They include documents, engineering drawings, XML files, images, and audio and video files.

Business Process Management
Business process management (BPM) applications help provide end-to-end visibility and

control over all segments of complex, multistep transactions or information requests that involve a variety of applications and people in an organization or externally.

Host Control
Host control solutions control the operating systems in servers and desktops. Their functions also include implementing security best practices at all levels of the operating system in each host, installing the most current updates and patches, and using secure methods for daily operations.

Identity Management
In an information network, organizations use identity management software and processes to help manage users' digital identities and their digital entitlements.

Incident Management and Trouble Tracking
Incident management and trouble-tracking solutions are customized systems that manage specific business processes end-to-end. The actual system functionality is not dissimilar to that of Customer Relationship Management (CRM) systems.

Messaging & Collaboration
Messaging and collaboration applications have become indispensable tools. Collaboration applications can range from integrated document programs to portals, instant messaging, online presentation software, and peer-to-peer (P2P) programs.

Network Security
Network security solutions constitute a broad solution category designed to address the security of all aspects of the network for the organization. They include firewalls, clients, servers, routers, switches and access points.

Physical Security
Physical security solutions secure physical access and control of the information systems and desktops in an enterprise.

Project Management
Project management solutions apply knowledge, skills, tools, and techniques to a broad range of activities to help meet the requirements of a particular project. Project management knowledge and practices are best described in terms of modular processes. These processes divide into five process groups: envision, plan, develop, stabilize, and deploy.

Risk Assessment
The term risk assessment has various meanings. The information security community defines it as a systematic method to identify the assets of an information-processing system, the threats to those assets, and the vulnerability of the system to those threats. In the context of regulatory compliance, risk assessment is the process of assessing the level of compliance and compliance inadequacies within an organization.

Training
Training makes an enormous contribution to the overall success of an organization by familiarizing employees with requirements and processes specific to security and compliance. Training provides the critical link between people, processes, and technologies that make security programs work.

Malicious Software Prevention
This includes antivirus, antispyware, and antispam solutions as well as rootkit detectors.

Vulnerability Identification
Vulnerability identification solutions provide tools that can help test for vulnerabilities in the information systems of organizations IT staff must be aware of vulnerabilities in their IT environments before they can effectively address them.

Monitoring and Reporting
Monitoring and reporting solutions collect and audit logs that result from authentication and access to systems. These solutions are either designed to collect specific information based on compliance to certain regulations, or use existing logs built into operating systems or software packages.

A subcategory of monitoring and reporting is the collection, assessment, and correlation of all logged data across an organization. This task is sometimes accomplished through a dashboard-type solution which can better analyze the various types of information gathered throughout an organization. This type of solution allows IT management to better determine whether or not events are correlated to each other.

9. IT-GLOSSARY

Benchmarking
Benchmarking refers to the act of comparing a company's own key indicators and values with a reference value, e.g. the average for the industry.

Chief Information Security Officer (CISO)
The Chief Information Security Officer is responsible for information security in an enterprise. Ideally, the CISO reports to the executive committee, and/or the CEO, or to the enterprise's risk management officer. The CISO liaises between business and IT stakeholders. The "CISO" frequently reports to the CIO, thus primarily fulfilling technical roles (IT Security Manager). This said, the position of information security in IT is problematic as it tends to lead to a purely technology-related view that is additionally subjected to practical constraints such as the cost and performance of IT systems.

Compliance
Compliance generically refers to a status that is in line with laws and regulations, as well as the corresponding behavior. Requirements to be taken into consideration include cross-industry and industry-specific regulations, legal requirements such as laws, jurisdiction and regulations, non-legally-binding standards, reference models and policies (recommended or mandated by associations or committees), local regulations (for Germany) and internationally valid regulations, and – of course – a company's internal policies which may have some relevance to employment law.

Dynamic IT Infrastructure
A dynamic IT infrastructure provides an efficient and controlled IT environment in which IT supports an enterprise's business development as an active resource.
A dynamic IT infrastructure gives an enterprise the ability to implement new IT services easily and quickly, to automate processes, reduce costs, optimize service levels and flexibility, and thus generally reduce complexity. Users benefit from internal audits and continual improvement, and can retrieve information wherever they are in a more simple and secure way. Systems for automatic provisioning and quarantine management ensure policy compliance and high availability.

Extranet
An extranet is basically an intranet that is not only accessible to staff, but also to third parties. It gives an enterprise an efficient – and if needed secure – method of communicating with and supplying information to, or exchanging information with, freelancers, partners, customers and suppliers.

Information
There are many definitions of information. Generally speaking, information refers to a "datum" that can be assigned a specific meaning within a tangible context, or to transferable knowledge. Data is thus potential information.

Information security
Information security includes all organizational and technical measures for ensuring the confidentiality, integrity and availability of data, processes and systems. More specifically it concerns protection against threats, identification of vulnerabilities and security issues, incident management and response, restoring of systems and processes and retrospective forensics.

Intranet
An intranet is a private (internal enterprise) network that gives employees the ability to exchange information and collaborate, which generally improves communications.

IT Infrastructure Compliance
IT infrastructure compliance refers to specific legal requirements imposed on IT systems and infrastructure components.
It is a subset of general compliance.

IT Security Manager
The IT Security Manager reports to the CIO and is mainly responsible for planning and implementing technical security measures.
If the enterprise does not have a CISO, the IT Security Manager will typically be responsible for information security management and risk assessment, however, a technology bias is likely.

IT Security
IT security is a subcategory of information security that focuses on technical aspects only.
IT security more specifically describes the state of an IT infrastructure or an IT application where the risks due to threats to information technology are restricted to an acceptable level by suitable measures.

Pareto Principle
If a small number of high values in a set of values contributes more to the total than the large number of small values in the set, this is referred to as the Pareto principle or effect.
The term is named after Vilfredo Pareto who analyzed the distribution of wealth in Italy and discovered that some 20 percent of the families owned 80 percent of all assets. Based on this, Pareto concluded that banks should mainly concern themselves with this 20 percent to secure a large share of its business.

Security Experts
In the context of this document, security experts are professionals who focus on the field of information and IT security. The range extends from technology experts to experts at executive level who are more concerned with organizational and process-oriented issues.

Social Computing
Social computing is a generic term for IT systems that support social networking between private persons, employees and teams in an enterprise, or across a market. The main benefit is the ”social” component of the individual and the individual‘s behavior which is reflected in the individual composing, editing and publishing information. Thanks to networking and the tie-in to tangible persons, individual pieces of information gain value.

Confidentiality, Availability, Integrity
Data and/or information, systems and processes need to be accessible and usable, that is, available to an enterprise. Confidentiality means: Data and/or information is regarded as confidential if access is restricted to authorized persons. Integrity: Describes a status of data and/or information in which the data/information is protected against manipulation by unauthorized third parties. In the context of data and information confidentiality and integrity, a distinction is typically made between data at rest and data in transit.

Microsoft Deutschland GmbH
Konrad-Zuse-Straße 1
85716 Unterschleißheim

Telefon: +49 (0) 89 - 3176 - 0
Fax: +49 (0) 89 - 3176 - 1000

E-Mail: sicher@microsoft.com
Internet: www.microsoft.com/germany

Handelsregisternummer:
HRB 70438
Umsatzsteueridentifikationsnummer:
DE 129 415 943