

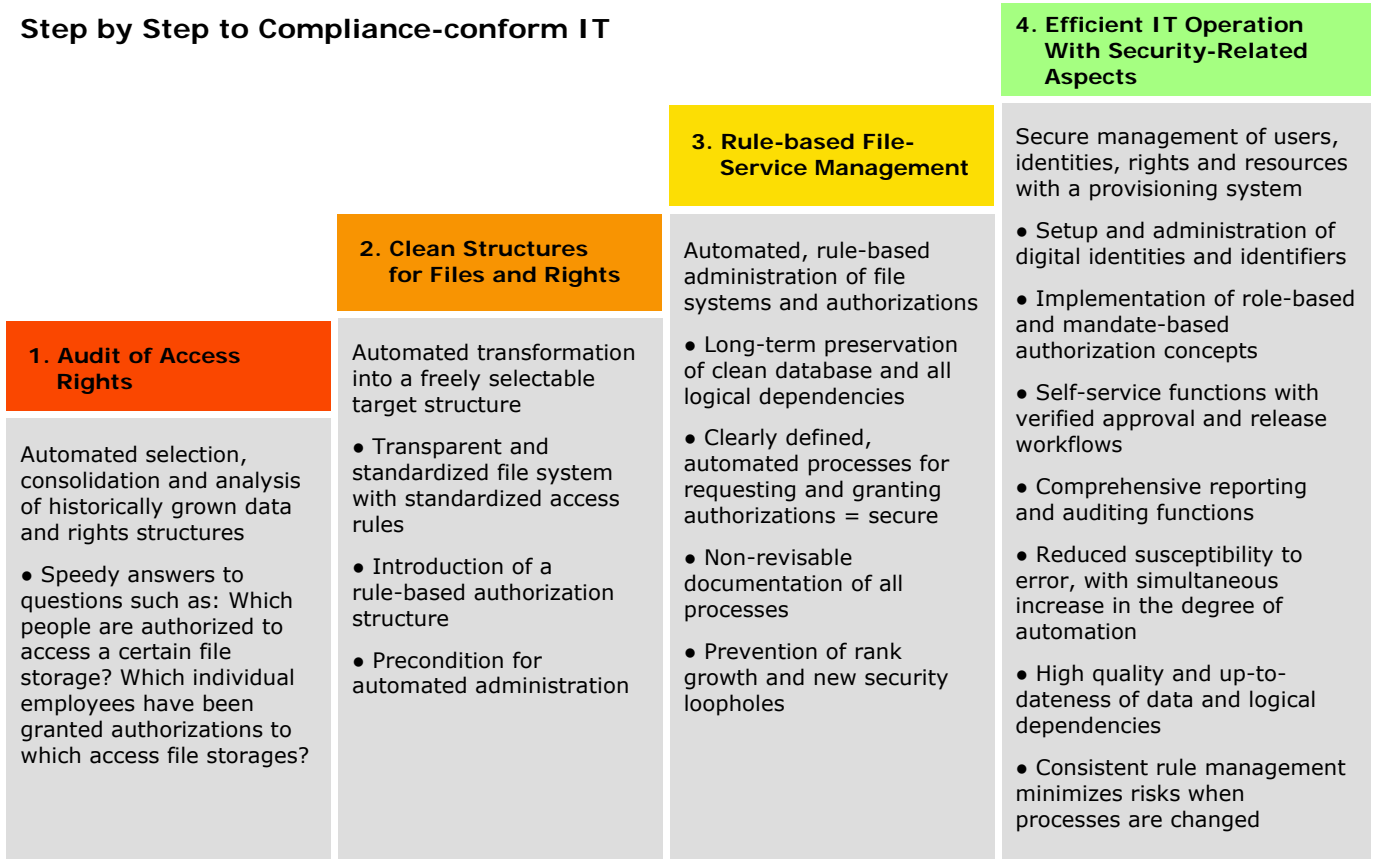
## Step by Step to Compliance-conform IT

### A methodical approach toward efficient IT operation under consideration of security-related aspects

Risk management, corporate governance, and compliance are challenges which must now also be faced by individuals tasked with IT responsibility. The increasing complexity and the accordingly confused view of systems, users and resources raise questions about previous and current practices for the administration and control of access rights.

Businesses are under pressure to cope with growing compliance requirements. They are obliged to comply quickly and they want to achieve compliance without the need for unreasonably large investments. The econet AG offers a methodical approach to gradual implement suitable measures which fulfill these requirements.

Only a small amount of effort is needed to create a quick-win situation that takes risk aspects into account. The final result is a highly automated system which forms the basis for regulatory conformity measures in the field of enterprise-wide access rights.



## **Background: Courts Demand Stricter Compliance with Rules**

The European Union (EU) has now adopted a guideline which is intended to fulfill the same purpose in Europe as its counterpart, the Sarbanes-Oxley Act (SOX), fulfills in the USA. The EU's members are required to implement "EuroSOX," the 8<sup>th</sup> EU guideline, in their national laws by June 29, 2008. Among its other stipulations, this new guideline prescribes that enterprises whose shares are traded on stock markets, as well as other enterprises of public interest, must create and assure the effectiveness of internal control systems and, if applicable, internal review and risk-management systems.

IT currently forms the basis for the majority of business processes in enterprises, so IT is strongly affected by the 8<sup>th</sup> EU guideline and by other already existent guidelines and laws such as the Bundesdatenschutzgesetz (German Federal Data-Protection Law), GdPDU, KontraG, etc. Providers of solutions in the fields of risk management and compliance have already repeatedly communicated the fact that management and supervisory boards can potentially be held personally liable. Many people, however, may not yet be aware that verdicts have already been handed down on the basis of these legal foundations.

A central issue in assuring compliance is to know who has access to which information in a business's network. Nearly every guideline ultimately requires proof and gapless documentation of access rights and the processes for the granting of such rights.

Many people tasked with IT responsibilities are aware that their businesses are not adequately equipped to comply with existing requirements. They're under pressure to comply, so they're grateful for a provider who can offer a methodical approach to the gradual buildup of a management solution for users, identity data, rights and resources which consistently implements compliance requirements. They're also grateful for a provider who can offer corresponding tools for rapid compliance and for the minimization of risks posed by these urgent problems.

## **From Audits of Access Rights to File and Rights Structures in Conformity with Compliance Guidelines**

The econet AG recommends a multistage approach of this kind. In an initial step, this Munich-based enterprise provides the capability, with the help of a special tool, to automatically identify and select rights from historically grown file structures. Businesses thus get immediate answers to particularly delicate questions such as which people have which rights to access a certain file storage within the enterprise? To answer this question, employee identifiers are resolved into actual names. Another sensitive question is: Which rights to which file storages has a particular employee accumulated over the years? To answer this question, the tool reads the rights allocations from the affected file storages, consolidates the acquired data and delivers the results in the form of a readable report.

In a second step, the software makes it possible to automatically transfer the structures of the files and rights into a freely selectable target structure. Comprehensible reports about the potential consequences of future target scenarios are generated based on analyses of the status quo and of particulars such as how the architecture of a new file structure ought to be. If necessary, warnings are issued: for example, if the software discovers invalid authorizations or unduly long pathways. After the report has been

checked and cleared by specialized departments and administrators, the transformation solution automatically restructures the file systems according to predefined specifications, reorganizes the file structure (if necessary), and updates the authorizations. Here too, the new status is presented in the form of reports.

The result is a standardized file system with standardized access rules. For many businesses, this is a first important step toward conformity with compliance regulations. To further minimize the IT risk for business-relevant processes, it's essential to maintain this transparency for users, access rights and data – despite daily changes. Furthermore, it's crucial to assure that these change processes themselves are governable, assessable and always open to scrutiny.

### **From Harmonized Rights Structures to File-Service Management in Conformity with Rules**

The next logical step toward fulfillment of regulatory requirements applicable to IT is to introduce standardized and automated file-service management, i.e. rule-based administration of file structures and authorizations. When deploying a corresponding solution, the selfsame rules and policies that had previously been used to restructure the file system can continue to be used to administrate it. The clean database and all logical dependencies are preserved.

Clearly defined, automated processes for provisioning project or file storages to departments, project groups or individual employees prevent new rank growth from causing the same old security loopholes. Automated approval workflows for issuance of rights prevent the accumulation of unnecessary or even unallowable authorizations; such workflows also guarantee that each coworker receives only those specific authorizations which are permissible in accord with his tasks and his position in the business.

With the assistance of these workflows, which require only minimal input, even technically untrained personnel can request access rights and/or the new creation of file storages via a service portal. Rights can be granted only by specially authorized persons, who, as a rule, are high-ranking individuals in the specialized department. The correctness of the authorization process is guaranteed by the fact that these decision-makers are firmly integrated into automatically running process chains. After a request has been authorized, the corresponding rights are automatically granted on the appropriate systems in accord with the specifications of the business's guidelines and IT policies.

An important factor here is that processes and process steps must be auditable. Historical data are recorded so that they cannot be subsequently altered or revised. This assures that an auditor can find out, reliably and whenever desired, exactly who possesses which rights to access which materials, why an authorization was granted, and who approved the authorization. For example, this capability guarantees the constant availability and testability of the full history of all authorizations which have been granted to participants in the financial-reporting process.

## **A Firm Grasp on Identities, Rights and Resources**

In addition to the inadequate ability to audit the granting of access rights, other factors which likewise jeopardize the secure execution of IT-supported business processes include:

- Non-erased user accounts which belonged to former employees
- Inconsistent access conditions
- Numerous user accounts requiring labor-intensive administration
- Manual administration with high susceptibility to human error
- Lack of user management

A suitable IT solution which supports the comprehensive management of users, identities, rights and resources is essential to neutralize these risks and satisfy the corresponding verification requirements. Many of the functions are by no means solely needed for specific regulating requirements, but are already also preconditions for efficient IT operations. Such functions include the automated provision of tools, resources and information to employees, as well as the granting and revocation of authorizations. Functions of this sort are subsumed under the category of "provisioning."

The implementation of the correct provisioning system increases the security of business processes and accelerates their execution.

- Setup and administration of digital identities and identifiers
- Implementation of role-based and mandate-based authorization concepts
- Self-service functions with verified approval and release workflows
- Comprehensive reporting and auditing functions
- Reduced susceptibility to error with the increase in the degree of automation
- High quality and up-to-dateness of data and logical dependencies
- Consistent rule management minimizes risks when processes are changed

But what if administrators circumvent the provisioning system when they grant authorizations? To prevent such risky practices, the provisioning system automatically compares its rights-related information with the corresponding data in the connected target systems. The provisioning system recognizes and reports illegitimate changes and, if desired, it can automatically countermand them.

To prevent the unauthorized utilization of rights, it is essential to assure that accesses can be blocked and authorizations can be revoked, deactivated or erased at any desired time and from a central location: for example, when an employee leaves the company or switches to a new department within it. This so-called "de-provisioning" is a central component in all rules. Measures to secure the IT infrastructure via audits, as well as obligatory verifications of authorization structures, can be derived from this component.

## **About econet**

The Munich-based econet AG is a provider of business software in the fields of identity and service management with core strength in the field of authorization and provisioning, reporting and auditing. Founded in 1994, econet helps globally active businesses and large public administrative bodies set up, operate, administrate and bill their IT services. The econet AG also assists them in the task of optimizing their IT business processes.

The econet AG offers businesses and large public administrative bodies a methodical approach to gradually set up suitable measures so that they can:

- Quickly satisfy progressively more rigorous compliance requirements with a reasonable amount of effort
- Automate processes to achieve securer and more efficient IT operation
- Make the ordering of IT services (e.g. applications, e-mail or data storages) as simple and transparent as ordering a book from an online shop.

This leads to a higher level of security and long-lasting reductions in the cost of operating, administrating and setting up IT services. econet's solutions combine ITIL Best Practices and a service-oriented architecture (SOA) as infrastructure. Based on Microsoft's .NET development platform, they've been awarded numerous prizes in the industry.

## **econet AG**

Kaiser-Ludwig-Platz 5  
80336 München · Germany  
fon +49 (89) 514 51-0  
fax +49 (89) 514 51-199  
[info@econet.de](mailto:info@econet.de)  
[www.econet.de](http://www.econet.de)