International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Role-Based IT-Access: Who Sets the Standards in German Internal Audit Departments?

C. T. Wildensee

Ph.D.(UChalco), DBA, CISM& CRISC (ISACA), Senior IT-Risk-Auditor, Stadtwerke Hannover AG, Hannover, Germany.

Abstract: ***Access management is essential for ensuring, that accounting-related ERP systems run according to the rules. Basics of legitimation and application requirements are established by laws and court judgements. The standards are characterized in detail by accountants and the product manufacturers, especially access restrictions. The german and EU administration are not able to set enough detailed regulation and unambiguity to force companies to do more than necessary against unauthorized data access, to implement effective authorization roles in accounting-related IT systems and finally to protect commercially sensitive data. Specifications exist, unambiguity and a graded threat of punishment is missing. The question is: What are the major influences on the work of german internal audit departments?***

Keywords: Corporate Governance, Internal Audit Function, accounting-related IT-Systems

1. Introduction

In order to offer authorised persons the necessary rights of access to the available IT infrastructure according to the "**Need-to-Know**" principle – as little as possible, as much as necessary (BSI, 2012: 28) – diverse process are to be developed by the IT service providers (the company's own IT department or a specialised IT service provider on the market in the course of an outsourcing contract for IT services to be provided; hereinafter also referred to as IT trustees in order to make it clear that the responsibility for the underlying data and its processing in conformance with the law lies in the company's specialist area). The legal principles of the state regulatory framework affect this organisation function, as well as the invoicing / accounting actually produced. Invoicing / accounting means that the IT systems deliver the base for commercial profit and loss accounts, for stock-taking, for accounts and for taxation.

2. Specific Legal Aspects

Companies can fundamentally use any legally, correctly introduced hardware and software in a preferred scenario for use in order to control their processes. Legislation cannot and should not provide detailed regulations, since otherwise the business-person's freedom to organise processes and organisation is cut.Within the framework of the statutory primary obligations as a businessman obligated to keep accounts (Führich, 2012, p. 45 et. seq.; e.g. keeping trading books, balance sheet and schedule of profits and loss within the framework of the annual accounts, safe-keeping and publication obligations) in the sense of e.g. the"Handelsgesetzbuch" (German Commercial Code, HGB) and the"Abgabenordnung" (German Fiscal Code, AO) there are design-related **secondary duties** also for the use of software products (hardware will be ignored in the following, since this to a large extend defines the technical framework for the use of software and the current processes), if they serve to develop accounting and invoicing. So largely generically formulated demands are made on commercial software solutions through the HGB and AO in order to guarantee proper accounting and consequently the observation of the "GrundsätzeordnungsmäßigerBuchführung" (German Generally Accepted Accounting Principles, GoB)– in particular in §§239 (management of trade books), 257 HGB (Safekeeping of documents), §146 AO (Procedural rules and guidelines for accounting and records) reference is made to the "GoB". Not only the main system to illustrate accounting in the widest sense is considered by this, but rather also all secondary systems if with their data as pre-processor or supporting systems deliver the bases of invoicing / accounting and determining taxes.

Compliance must remain in the establishment and company-specific adaptation of the IT system or respectively the IT-supported procedure in the specific company surroundings and for the duration of the safekeeping period. (GOBD, 2014: 8) Through the increasing integration of software products with inter-faces to upstream systems of accounting software, the function of accounting can hardly be clearly encap-sulated from a technical point of view. Compliance and security of the individual software modules outside the main system is therefore also of significance, but they run the risk that they are not considered in an overall consideration. Moreover, to satisfy the statutory safekeeping obligations, archiving systems based on the database will be used, on which the identical commercial and tax law requirements take effect. Fundamentally therefore, identical assessment criteria will be attached to the process-supporting systems which are also attached to the main accounting system. Some important features from this include:

- Compliance must remain in theestablishment and company-specific adaptation of the IT system or respectively the IT-supported procedure in the specific company surroundings and for the duration of the safe-keeping period. (§ 239 Para. 2 HGB)
- Corrections made which are not be made as a direct change to the data, but must rather be made by cancelling and re-entering, or by writing change documents.
- A posting, entry or record may not be changed in a way in which the original content can no longer be determined. Also such changes, the properties of which make

it uncertain whether they are original or were not made until later, may not be made. (§ 146 Para. 4 AO)
- Records relevant to invoicing / accounting must be visible within the framework of sufficiently defined safekeeping periods and / or be reproducible (§ 146 Para. 5 AO)
- Records must be able to be presented through referencing the activities which were the cause of the process and the persons activating them – also over the system limits.
- With regard to the audit track, why, when and through whom a data change is made in the IT systemsrelevant here, in 6.2.4 of the "Generally Accepted Accounting Principles in storage oriented IT-Systems (GoBS) is described as follows: All provisions through which data and programs cannot be changed byunauthorised persons are to be described as measures to maintain the integrity of the data. Alongside the description of the access authorisation procedure, this includes **evidence of proper allocation of access authorisations.**
- Furthermore, for example the reports of the Information Technology Committee of the German Institute of Public Accountants (FAIT) in FAIT1.3.1(23) stresses the importance of the personal information in user information: Authorisation means that **only persons determined in advance**can access data (authorised persons) and that only they can exercise the rights defined for the system.These rights concern reading, compiling, changing and deleting data or the administration of an IT system. Through this only the **authorised image of business events are guaranteed in the system**. Suitable procedures for this are physical and logical access limitation measures (e.g. password protection). Organisational provisions and **technical systems for access protection** are required to implement the **division of functions required**. [...] There is authenticity if **a business event is clearly allocated to a cause**.
- FAIT1.4.2(84) stresses the importance of authenticity and graded authorisations for the tasks to be carried out. **Through logical access controls, e.g. using user ID and passwords, the identity of the users of IT systems is clearly determined, and therefore unauthorised access is prevented. Employees are only to be granted authorisations which are necessary to fulfil their tasks.**
- The IDW audit standard (PS) 330 with its references, primarily PH9.330.1, Checklist for annual accounting audits using information technology, likewise shows analogous points. Under PS330.2(12) the complexity of the system to be examined is mentioned as one of the authoritative criteria. […] In complex IT systems, a comprehensive IT system check is always required because an evaluation of the compliance and security of the IT-supported invoicing / accounting without considering the programmed processes relevant to invoicing / accounting is not possible.Under 3.4.2(57) and (58) there is a specific demand for logical access controls. (57) […] The audit procedures within the framework of the preliminary audit of logical access controls is based on the implementation of an organisational procedure for application, authorisation and opening by those authorised for use in IT systems. This concerns both the authorisations on operating system levels (registrations in computers in a network) as well as the rights to carry out transactions in an IT application. Access controls are to be evaluated as appropriate if they are suitable to determine that the administration of authorisation and the established system rights comply with the determination in the security concept, and therefore unauthorised accesses to data and information as well as program processes to change data are excluded. In addition, access controls must be organised in such a way that they clearly determine the identity of the user and unauthorised attempts at access will be turned away. (58) Checking the effectiveness of the logical access controls extends to the agreement of defined processes with the actual processes of the user administration and maintenance. Furthermore, user authorisations are to check in random samples whether the established authorisations correspond with the rights applied for and the actual area of responsibility of the employee.

3. IT-Security GAP

In the past, in spite of increasing regulation from the point of view of commercial and data protection law, the legislator has made hardly any specific provisions regarding IT risk considerations in companies with regard to control and transparency in the sector,or even formulated minimum requirements for risk management – either for IT as an area of risk, or for IT as a risk manager (Kapffer et. al., 2013: 12).All statutory provisions have at their core the following four central requirements: the material risks of the company are to be identified systematically; the identified risks must be quantified and reported in a comprehensible form to the company management; there are suitable measures to limit and control the risks; an internal control system must be set up in order to avoid risks. (Kapffer et. al., 2013: 12 et. seq)

In which granularity, so with which depth / which intensity or also aggregation this is done is not determined and lies in the company's room for manoeuvre, to only satisfy formalities, or to integrate meaningful control mechanisms. In this regard activities in the field of IT security, authorisation management and also data protection, where required,may be lowered to an argumentative tenable minimum. This might not appear clever at first sight, but it is a fallacy to assume that decisions made by management are always rational and without trade-offs. In times of increasing pressure on the provision of financial and human resources, the room for manoeuvre in commercial activity is falling. There is a lack of legal framework conditions to force on a company or respectively responsible acting person more than the minimum in the field of IT security and IT auditing, authorisation management and also data protection and, where necessary, to impose effective sanctions. The legislator – both national and European – was previously hardly interested, or in the position with regard to consensus in the EU, to demand more than the previously often imprecisely formulated contents, and apply obligations to companies with causally clear lines of cause and effect (i.e. "penalties follow breaches"). Few, legally unambiguous requirements must of course be considered, in particular from commercial and data protection law. The defined minimum with lower verification runs the risk that it will not suffice in the case of damages orrespectively checks and become a sanctionable set of circumstances.

The partial orientation to available standards and guides (e.g. BSI, COBIT, ISO 27K-family) is however often insufficient to be able to report activity. It is remarkable in cases of damage that abuse of access authorisations through system users with strong authori-sation with their own motivation, generally represent no challenge in determining fault legally and especially in the case of employment law if the evidence can be presented. The misuse of such access through authorised persons privileged with rights initiated by superiors is however especially perfidious, but means the exploitation of the authority to issue instructions related to tasks and roles of superiors placed higher in the hierarchy. Functional uses, recorded in the details of the IT systems and identified as misdemeanours are unproblematic to report as exclusively articulated instructions with evidence from higher in the hierarchy if there is a lack of knowledge of the law, or what is wrong, by the actor in a case of breaches against regulations.

A complete neglect of existing standards, so e.g. the references and guides of solution manufacturers (and for SAP the largely recognised German SAP user group[DSAG]), would be a fault in particular for responsible acting persons of IT and top management, since it is precisely these requirements which are considered "best practice" and can in this regard hardly be ignored. However, informed partial enforcements suffice for the goals of the company if the company documents the will to do this through security and data privacy policies (in this regard much is intended and little is realised). The departments responsible for IT will in this regard also alwaysensure partial implementations, since well-chosen points in the subject of IT security and data protection in the guides are already provided in the technical implementation guides of the products used.

4. Effectiveness

The list of those who can formulate demands in the subject described as claimant from outside, is small: The data protection authority and the external financial auditor (Public Accountants). Further authorities such as the accountant of the financial authorities or customs within the framework of tax field auditing, the trade supervisory office or other state institutions pursue express goals which place no focus on IT-specificcontents.

Audit authorities like the state data protection authorities will normally only be active upon instigation, i.e. if concerned parties (mostly anonymous) write appeals and the regulatory authority then follows this uppunctually. The focus here is the process complained about, in which **personal data or data where personal information can be obtained** are processed, and the documentation is according to extensive formal requirements of the"Bundesdatenschutzgesetz"(„German Federal Data Protection Act", BDSG).

The authorisation concept itself is hardly considered, since there must be auditor capacity and specific know-how for this – already on the basis of the extent of the documentation which is often significant – in order to be able to recognise errors or intentional deception and conflicts of goals. This is hardly to be guaranteed. Collisions in roles from the question of operation of the IT systemrelevant to invoicing / accounting in conformance with the law are likewise not considered. Express attention is given to the storage and processing of the personal data or data in which personal information can be obtained. And the function of the person in the companyauthorised with data protection as part of the company's control of itself runs the risk of breaching allegiances in the employment contract despite often adequate projection of know-how in the case ofdisagreements in interpretation with the employer, if he unilaterally draws on the responsible internal auditing authority for clarification and explicitly refers to a particular trouble. He can damage himself permanently.

Only the external financial auditors(Public Accountants) with their IT audit teams can ensure redress on the basis of his legitimate exercise of functions and also enforce unpopular measures to increase IT security, makingreference to the statutory bases and his (institutional) interpretation. Within the framework of the mandate issued and the annual accounting audit he refers mostly to both the capacity as well as knowledge in order to question critically and searchingly. Whether these contents are audit contents is based on the order and not always stated. In the agreement of the mandate, suggestions will often already be provided which alsoinclude consideration of the authorisation concept with specific focus on auditing. If the assessment should also carry out these contents, the know-how cap is mostly put at a high level, alongside the simple timedimension. The extent of available auditor capacities, the exchange of information amongst the auditing team and the punctual inclusion of specialist auditors in processing the order ensures this. These are based on the requirements of the standards of the IDW (German Institute of Public Accountants) and the recognised extensive literature on products / procedures (DSAG, guidelines from manufacturers, specialised literature, also audit literature). This certainly does not mean that requirements will be produced to the highest values. A certain degree of interpretability and necessary consideration of individual company interests lead to powers of discretion in detailed issues. But at least extensive part implementation is demanded.

For companies the view of the externalfactors involved is very important, and allows them to make a grading assessment of the importance of regulatory requirements, also with economic considerations. In particular the non-statutory regulatory framework leads to a pressure to implement in the company which is not to be underestimated. It is moreover also sensible if the specialisations in the internalaudit department– to be seen as elements of a company's self-control in spite of differing legitimacy and content focus with regard to company data protection and IT security, at least in inquiries from Identity & Access Management, system basis security and to their specific processing aspects as allied together in spirit – to accept theyardsticks from the auditing standards of the IDW, to simulate their internalaudits as externalaudits and also to justify the advice and assessments based on this. This means that for internal audits in the field of IT systems relevant to invoicing / accounting, the following questions are always raised: How would an external auditor proceed? Where will he place the main emphasis in terms of content? The external auditor is re-

quired to inspect the audit reports of the internal audit department from the previous periods in order to satisfy himself on the one hand about the central points, the depth and the quality of the work (consideration for the effectiveness of the internal audit department), and on the other hand to derive whether main emphases are also deducible for him from this.

Through indication of a well mapped-out auditing procedure the internal audit department can take on a supporting role for the company and, at least influencing the objectives of the audits nearing conclusion, can make a determined contribution to the value – a protective mechanism from the risks which means a legally legitimate audit authority with the implied possibility to cause negative effects for the company with a high power of discretion.

5. Final View

From the point of view of business information technology the topological and configuration risks individual to the company are limitable and known by the responsible officers of the IT service providers. Although the predominant records are fundamentally insufficient and stand in the area of tension between a high demand for meaningfulness and a volume increasing and retracing time problematic, this leads to an overall rather low risk assessment. The risks which result from the installation and development of software / source codes are problematic, be it through development by the company itself or through installation of the code through the manufacturer or specialised third party service / implementation provider. Both regularly provide codes which are suitable for the official transport routes in the systems, but cannot be considered in its effect risk through the company using it from volume (number of transported objects and code lines).Security instructions throughthe system itselfand Security Researcherswill indeed be done away with through patches (provided that they are recognised as such through the software solution manufacturers), but between emerging relevant security loopholes which were found by external researchers and the particular appropriate patch (whether explicit patch, multi-patch for several loopholes or silent patch) between a month and several years could pass. There is evidence that two weak points per week are discovered through external security researchers. Whether they were established comprehensibly is not known. But the discrepancy between recognition and closing security loopholes opens possibilities to attackers to test attack scenarios and to place them extensively. An active patch management, so contemporaneous installation of patches without security gap in the company, is of priority in security. In spite of that there is a large time window for attacks, be it from inside or outside the company. Also in the case of source codes created by the company, the danger of attacks by internal employees is fundamentally high and hardly retraceable in cases of damage. In the code example presented, a dilemma is demonstrated. A source code need not be damaging from itself, but rather it opens the system for the import of any codes and in cases of use it leaves responsible actors in uncertainty, as described.Retracing is not possible. Besides a company's own program development, it can further be determined that the monitoring of interfaces and the rights of highly privileged users (internal / external) also continue to be problematic. An effective limitation and monitoring of consul-ting, administration, module support, system and interface accounts provided with extensive rights is hardly realisable, unless it happens in the future that the administration of the system and the communication between systems for access possibilities to business data are decoupled.

The defects determined by the internal audit department, if established as an effective security position in the company, and the external auditors are not to be valued as interpretable "nice-to-have" views, but rather as important contributors to value which protect the company from security compromises and data manipulation with legal legitimacy.

References

[1] **BSI(2012)**, Bundesamt für Sicherheit in der Informationstechnik, Leitfaden Informationssicherheit - IT-Grundschutz kompakt, Stand Februar 2012, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf?__blob=publicationFile.

[2] **FÜHRICH(2012)**, Wirtschaftsprivatrecht, 11. Auflage 2012.

[3] **GOBD(2014),** Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD), BMF, 14.11.2014, http://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/Datenzugriff_GDPdU/2014-11-14-GoBD.pdf?__blob=publicationFile&v=1.

[4] **KAPFFER/KAUFER(2013)**, IT: Risiko-Ursache und -Bewältigerin zugleich, in: Computerwoche, 42(2013) vom 14.10.2013,S. 12-14.

Author Profile

Christoph T. Wildensee, Ph.D. (Business Administration / UChalco), Dipl.-Betriebswirt, CISM&CRISC (ISACA), is a Senior IS-Risk-Auditor with main focus on SAP-Systems for Stadtwerke Hannover AG, Hannover, Germany (www.enercity.de). Additionally, he worked from 2001to 2002 as aSAP-Consultant for the IBS Group, Hamburg, Germany. With more than 20 years of IS auditing experience, he is responsible for security and processual audits in all accounting-related SAP-Systems.