Auditing Global Compliance of Data Protection Mechanisms

In today’s society, the concern about the protection of personal data is steadily increasing.\(^1\) As a result of new technologies and social media, an ever-increasing amount of personal data is processed by more parties in more locations. Countries are responding by implementing updated or new data protection laws and by increasing enforcement activities.

However, both content and enforcement activities of these regulations are quite different; therefore, ensuring compliance with all local regulations is challenging for a global organization acting in several countries.

The need to audit global compliance is rising for the following reasons:
- Increased attention of regulators worldwide
- Reoccurring high-profile cases in international organizations
- The need to avoid financial and reputational risks arising from compliance cases

**COMPLIANCE GOALS DETERMINE AUDIT APPROACH**

Globally acting companies can choose from different approaches to satisfy data protection laws,\(^2\) irrespective of the type of data:
- One approach is based on ensuring data protection compliance on a per-country basis and is, in that sense, global—although not quite centrally driven. This could lead to, in this case, acceptable situations in which incidents in one country reoccur in another due to a similar root cause. The emphasis of this approach is to check whether the requirements or procedures are designed and implemented as required by the respective local law. This approach will mainly give assurance on the compliance level per country during the period that was audited.
- Another approach is to have an organizationwide data protection program to prevent, detect and respond to systematic errors across all countries. Examples of systematic errors are repeat failures to include the data protection organization in IT projects,\(^3\) continuous use of personal data beyond the purpose for which the data were collected and the outsourcing of data processing to service providers without checking the providers’ data protection level. This approach will give assurance of the effectiveness of the program in preventing data protection incidents.

Regardless of the approach that is chosen, it is important to understand that no organization can completely prevent data protection incidents from occurring since individuals can always make mistakes, such as accidentally sending an e-mail containing personal data to the wrong person or losing a data carrier (such as a Universal Serial Bus [USB] stick or backup tape). The key is to assess whether an organization is effective in reducing systematic vulnerabilities to an acceptable level. The level of what is acceptable for an organization is directly related to its risk appetite, which, in turn, is set by management and determined as part of a risk assessment.

The risk level, risk appetite and risk profile of an organization will influence the risk response.\(^4\) Specifically for data protection, the risk level, the risk appetite and risk profile are influenced by four factors:

1. **Operations in a regulated market**—All business operations need to comply with regulations relevant to their market; these range from, for example, registering the business with local authorities to obeying financial statement calculation rules. In addition, some markets (e.g., financial, health care) are more highly regulated and are under closer watch by authorities than others. Organizations that operate in such highly regulated markets are generally more concerned with reducing compliance risks.

2. **Strictness of laws in certain countries**—Some data protection laws are stricter or are enforced more rigorously than others. In Germany, for example, there is a strong enforcement structure,\(^5\) while the risk of

---

F. van Vonderen, CISA, CGEIT, MSIT, is managing consultant at Dutch consulting company Verdonck, Klooster & Associates and has more than 13 years of experience in IT advisory and auditing for several multinationals. Previously, he worked at Siemens AG as manager of IT audit, and he has published several articles on IT sourcing, operations and security in various Dutch magazines. He can be reached at
frank.vanvonderen@vka.nl.

---

Do you have something to say about this article?
Visit the Journal pages of the ISACA web site (www.isaca.org/journal), find the article, and choose the Comments tab to share your thoughts.

Go directly to the article:
financial damages in the US as a result of civil lawsuits is relatively high. Knowing the potential consequences of data protection breaches is necessary to assess the risk.

3. **Personal data as core business**—If the storing of personal data is an enterprise’s core business (e.g., the hosting of a human resources [HR] application), a data protection incident may influence customer attitudes and confidence more than if an organization stores personal data as a general asset to support business processes (e.g., maintenance of a customer database).

4. **Amount of personal data that is being stored**—The more personal data that are stored, the more data can be unwillingly disclosed (e.g., after a hack or the loss of a data carrier). A direct correlation between the fine imposed by an enforcement scheme and the number of personal records that are exposed has been noted.6

**AUDITING COMPLIANCE WITH THE LAW**
When a company has chosen to ensure data protection compliance on a per-country basis, the focus of the audit is to check whether the organization has implemented the requirements of data protection laws as prescribed in the countries in which it is operating in. Data protection laws generally address the following topics:7
- Data quality principles, such as purpose limitation, proportionality and data retention
- Transparency to data subjects on the collection and storage of personal data
- Subject rights to be informed and to ask what and where personal data are being stored by an organization
- Accountability for third parties that process personal data on behalf of an organization
- Notification procedures on data protection breaches

The audit activities and questions can be specifically designed to check compliance with these requirements to determine whether an organization is following them. Some laws have specific requirements on controls that need to be in place,8 such as existence of data classification and data protection policies. For compliance with European privacy laws and regulations, there are comprehensive materials available that help auditors to prepare an audit.9

**AUDITING THE EFFECTIVENESS OF A DATA PROTECTION PROGRAM**
The objective of an audit on the effectiveness of the data protection program is to understand how effective an organization is in handling systematic errors relating to data protection. But, what is a data protection program? The Institute of Internal Auditors has noted the following aspects of a data protection program:10
- **Standards and procedures**—The organization should establish compliance standards and procedures that can be followed by its employees and other agents to reduce the prospect of criminal conduct.
- **Assignment of responsibility to senior personnel**—The organization should assign overall responsibility to oversee compliance with standards and procedures to specific individual(s) within the senior personnel of the organization.
- **Reliable background of staff**—The organization should, as a hiring requirement, use due care not to delegate excessive discretionary authority to individuals who the organization knows, or should know through the exercise of due diligence, have a propensity to engage in illegal activities.
- **Communication of procedures**—The organization should communicate effectively its standards and procedures to all employees and other agents (e.g., training and practical documentation).
- **Compliance monitoring and auditing**—The organization should take reasonable steps to achieve compliance with its standards (e.g., monitoring and reporting).
- **Consistent enforcement**—The organization should enforce standards consistently by means of a disciplinary system under which those who violate the organization’s code of conduct, e.g., the data protection guidelines, are reprimanded appropriately in relation to the offense.

---

**Enjoying this article?**
- Attend North America CACS 2012, where sessions will include topics such as “Practical Use of Encryption Technology for Data Protection” and “Understanding Your Data Flow: Using Tokenization to Secure Data.”
  
  [www.isaca.org/nacacs](http://www.isaca.org/nacacs)

- Learn more about and collaborate on privacy/data protection.
  
• **Appropriate response to an offense and prevention of similar offenses**—After an offense has been detected, the organization should take all reasonable steps to respond appropriately to the offense and to prevent similar offenses, including any necessary modifications to its program to prevent and detect violations of law.

Evaluating the effectiveness of these elements is the basis for an audit on a data protection program. Apart from these elements, the following should also be considered:

• **Risk assessment**—The organization should do a comprehensive analysis of the legal requirements vs. the business risks. The risk analysis results should be used to prioritize efforts, derive action plans and allocate resources.

• **Single definition**—The organization should use a generally accepted and enterprisewide definition of “personal data.” This is particularly challenging and crucial in a global organization. Between countries, there are cultural differences in what data are considered as personal. For example, salary information, gender, academic degree, religion and mother’s maiden name have different sensitivities throughout the world.

• **Organization and responsibilities**—The organization should define who is responsible for governance, implementation and effectiveness, and who the relevant stakeholders are within the organization.

• **Short- and medium-term targets and tasks**—The organization should ensure that people in the data protection organization understand, perform and achieve their tasks and targets (e.g., data protection controls implementation, assurance of the degree of awareness of relevant stakeholders, prevention of potential data protection incidents).

• **Basic set of controls**—The organization should ensure the effectiveness of the data protection controls as they are implemented (either the minimum set of technical and organizational controls as mentioned in laws or adequate controls as determined by the organization in its own baseline).

A data protection program should also help an organization sustain compliance. One way to audit future compliance is to check whether there should be mandatory or voluntary consultations with data protection specialists in the case of:

• Changes in business models (e.g., a move into consumer business, different marketing strategies)
• Changes in IT developments (e.g., moving data to a public cloud, consolidation of global HR processing in one country)
• Changes in law under which the data protection specialist would initiate the impact assessment for the company

This combined set of elements will allow auditors to provide reasonable assurance regarding the effectiveness of the data protection program and the ability of the organization to prevent systematic errors.

**GENERAL CHALLENGES**

When auditing a data protection program at a multinational organization, there are some general challenges that are helpful to consider:

• More and more physical products are storing personal data about their owners (e.g., cars, medical equipment). The protection of personal data in physical products may not be on the agenda of the data protection organization. Adding this to the scope of the audit is recommended.

• When using third-party processing, the oversight on the third-party assurance of data protection requirements can be limited. Either there is no adequate overview of third parties that process personal data on behalf of an organization, or the review activities on the quality of work performed by third parties are insufficient. The audit program needs to consider the contractual relationship between an organization and a third party. Since an organization is accountable for the third party’s performance, it needs to have the proper means in place to monitor the third party’s performance, including the third party’s efforts toward protecting personal data.

• Enterprise resource planning (ERP) systems (such as Oracle and SAP) regularly hold personal data of different types (e.g., staff data, customer data). Data protection laws require limitations to the possibilities for users to access personal data outside their area of responsibility, e.g., a sales person should be able to see customer data, but not staff data. Having specific subject matter expertise on the ERP systems available in the audit team will allow proper evaluation of these potential issues.
The audit process can be obstructed by discussions on the legal interpretation of requirements and obligations. Legal expertise in the audit team will help facilitate discussions and enhance delivery of results. Adding local privacy officers to the audit team is a useful option, as long as they are not put into a position in which they have to audit their own work. For example, a privacy officer from one country can support the audit team from a different country.

Auditing the effectiveness of a data protection program is very complicated if a structured program does not exist within the organization. While this may sound trivial, it is crucial that the auditee and the auditor have the same understanding of what an effective program is. Having a structured program for data protection would, therefore, be a prerequisite for any audit that is set up to result in an audit opinion.

**CONCLUSION**

Auditing the effectiveness of data protection at a multinational organization is influenced by the organization’s efforts to be compliant. An audit on compliance with legal procedures will show whether an organization has been compliant over the last period, while an audit on the data protection program will lead to assurance on how effective an organization is at preventing data protection incidents from happening.

**ENDNOTES**

1. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data defines personal data as “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.” All organizations collect personal data on employees. In addition, depending on the nature of the business, personal data are often collected on customers, suppliers and shareholders. Other examples include patient data and the personal data that companies process on behalf of their customers.

2. During their audit work, the authors observed only the two general approaches described; there may be other approaches.

3. Note that “data protection organization” is a general term. It can also be referred to as “privacy organization” or even “information security organization.”


5. A recent example of the strong enforcement structure in Germany: “The Data Protection Commissioner’s Office (Independent Centre for Privacy Protection [ULD]) calls on all institutions in the federal state of Schleswig-Holstein, Germany to shut down their fan pages on Facebook and remove social plug-ins such as the ‘like’ button from their web sites.” See www.datenschutzcenter.de/presse/20110819-facebook-en.htm.

6. In the UK, the maximum fine under the Data Protection Act is a per-record fine; see www.dotmailer.co.uk/email_marketing_resources/law/penalties_for_noncompliance.aspx. Under US Massachusetts 201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth, penalty schemes are based on a formula that multiplies the fine with the number of data subjects affected (people); see www.malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93i/Section2.

7. There are more than 50 individual data protection laws in the world. The most leading laws are related to Europe’s Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications) and US Massachusetts 201 CMR 17.00. The German Federal Data Protection Act is generally considered to be one of the strictest laws.

8. See US Massachusetts 201 CMR 17.00 and the German Federal Data Protection Act.


10. The Institute of Internal Auditors, 2100-5 *Legal Considerations in Evaluating Regulatory Compliance Programs*, USA, 28 March 2001