**Send by fax to: +49 3375 217459-19 or by email to: kundendienst@deuzert.de**

DeuZert® Deutsche Zertifizierung in Bildung und Wirtschaft GmbH

Hochschulring 2, 15745 Wildau near Berlin / Germany

|  |  |  |  |
| --- | --- | --- | --- |
| **Type of application** | | | |
|  | Initial certification | | |
|  | Recertification | | |
|  | Modification of the scope of an existing certification | | |
|  | Transfer of an existing certification | | |
| **Headquarter of the organization** | | | |
| Company: |  | | |
| Street no: |  | | |
| Postal code, City |  | | |
| CEO: | Given and family name | | |
| Phone / Fax: | / | Website: |  |
| **Billing adress, if different** | | | |
| Company: |  | | |
| Street No: |  | | |
| Postal code, City |  | | |
| **Point of contact** | | | |
| Given and family name: |  | | |
| Position: |  | | |
| Street No: |  | | |
| Postal code, City |  | | |
| Phone / Fax: | / | Email: |  |
| **Information about the organization** | | | |
| Which products and/ or services are provided? | | | |
|  | | | |
| Which areas of business are represented by your clients? (e.g. data processing, automotive industry, etc.) | | | |
|  | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Was an external consultant involved during the development of the Information Security Management System (ISMS) according ISO/IEC 27001:2013? | | | | | |
| Yes | | | No | | |
| If so, please name the company and consultant. | | | | | |
|  | | | | | |
| Are there any non-applicable requirements claimed? | | | | | |
| Yes  Risk acceptance criteria: **,      ,** | | | No | | |
| Are there ISMS-relevant areas in your organization that cannot be made accessible to the audit team for reasons of confidentiality? | | | | | |
| Yes | | | No | | |
| If so, please name these areas. | | | | | |
|  | | | | | |
| **Basic data of the ISMS** | | | | | |
| Are the business processes of the organization computer-controlled? | | | | Yes | No |
| Is the organization subject to increased demands regarding data protection (secrecy, administration of personal data)? | | | | Yes | No |
| For reasons of data security does the organization operate "separate" (dedicated) systems? | | | | Yes | No |
| Does the company manage external data? | | | | Yes | No |
| Information Security Requirements (Confidentiality, Integrity, Availability) | many sensitive / confidential information; high level of requirements | a range of sensitive / confidential information; medium requirement level | | little sensitive / confidential information; low requirement level | |
| Number of critical assets in terms of confidentiality, integrity, availability | many critical assets | a range of critical assets | | few critical assets | |
| Number of processes and services | more than 2 complex business processes with many interfaces and integrated business units | up to 3 simple business processes with few interfaces and included business units | | a main business process with few interfaces and integrated business units | |

|  |  |  |  |
| --- | --- | --- | --- |
| Business risk within the scope of the ISMS | high business risk | medium business risk with higher regulatory requirements | low business risk without regulatory requirements |
| Scope and variety of IT technology and environment used | high diversity or complexity of the IT environment | standardized IT environment with a variety of IT platforms, servers, operating systems, databases and networks | highly standardized IT environment with little diversity |
| Extent of outsourcing to external service providers within the scope of the ISMS | high dependency on outsourcing or suppliers with a high impact on important business activities | partial outsourcing | no outsourcing and low dependency on suppliers OR well established or supervised outsourcing with certified ISMS at the outsourcer |
| Scope of system development | Extensive internal software development in various ongoing projects for key business applications | System development using standardized software platforms with complex configuration; customized software solutions | no in-house system development using standardized software platforms |
| Number of disaster recovery sites | high requirement (24/7) with various disaster recovery sites and data centers | medium requirement and max. 1 disaster recovery site | no request and max. 1 disaster recovery site |
| **Number of employees (full time equivalent) in the scope of the ISMS:** | | |  |
| Number of employees | ≥ 1.000 | ≥ 200 | < 200 |
| Number of employees who maintain / administer the IT systems | *≥* 100 | ≥ 20 | < 20 |
| Number of locations | ≥ 5 | ≥ 2 | = 1 |

|  |  |  |
| --- | --- | --- |
| **Locations** | | |
| How many **locations**[[1]](#footnote-1) should be certified in total? ***Please fill out the form "Request - Information for location WP04 I - F01ae" for each location.*** | | |
| A **group certification**[[2]](#footnote-2) is only possible if the following points apply: | | |
|  | The organization applies a single information security management system for all locations. | |
|  | The organization has a head office as part of the organization (not necessarily the headquarter of the organization, not necessarily a single location). | |
|  | The head office has the organizational authority to define, implement and maintain the information security management system. | |
|  | The information security management system is subject to a central review by the top management of the organization. | |
|  | All locations are subject to the organization's internal audit program. | |
|  | The head office ensures that data are collected and analyzed from all locations. It can demonstrate that it has the authority and ability to initiate organizational changes, i.a. to the following owns:   * Management system documentation and its changes, * Management review, * Handling of complaints, * Evaluation of corrective actions, * Planning of internal audits with evaluation of the results as well as * Consideration / compliance with legal / regulatory requirements regarding ISO/IEC 27001:2013. | |
| The members of the group are audited in a reference selection process.. When choosing a sample in a group certification, it should be noted that there are locations with similar / comparable processes / activities / products, but also locations with essentially different processes / activities / products. For this reason, DeuZert must be informed of the processes / activities available there for each location. ***Please fill out the form "Request - Information for location WP04 I - F01ae" for each location.*** | | |
| Should all locations be listed on a single certificate? | | |
| Yes | | No |
| Please give us your suggestion for the certificate text for your group after successful certification: | | |
|  | | |
| Desired audit date (Calendar week): | |  |
| Place and date: | |  |
| Given and family name: | |  |
| Signature for the validity of this statements: | |  |

1. At a fixed location, the organization continuously carries out work or services, including associated or affiliated activities. At a virtual site, the organization carries out work using an online environment or provides services based on physical site processes. A virtual site is considered a single location to determine the audit time. [↑](#footnote-ref-1)
2. Certification of an organization with an information security management system in multiple locations. [↑](#footnote-ref-2)