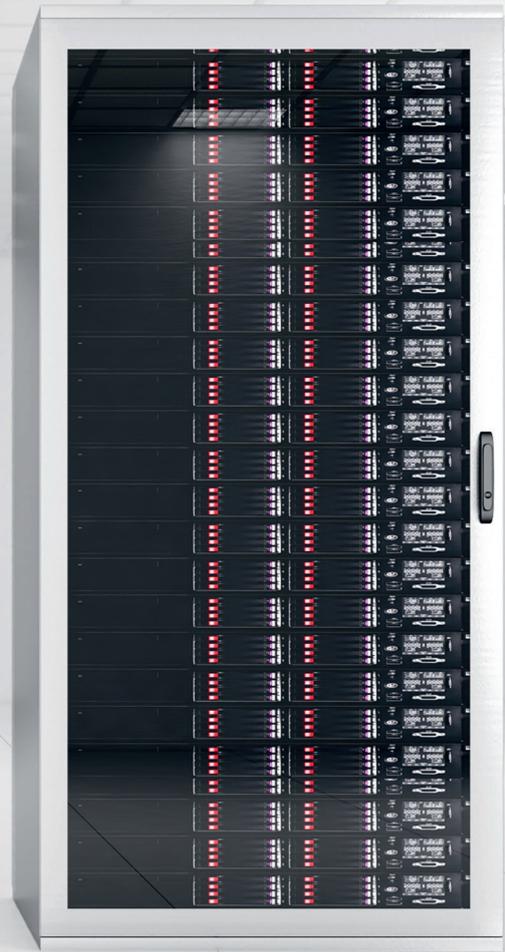




Data archiving

Certified according to BS 10008

Electronic Records
Management System (ERMS)



kpmg.ch/consulting



What is British Standard 10008?

BS 10008 contains a basic standard and three codes of practice with additional requirements for information storage and transfer, and the linking of information and electronic identities.

BS 10008, Evidential weight and legal admissibility of electronic information

British Standard BS 10008 defines the requirements for the implementation and operation of an electronic information management system. This includes data processing, sharing of information between computers and electronic storage. The standard addresses the authenticity and integrity of data to satisfy legal requirements.

Codes of practice for the implementation of BS 10008:

BIP 0008-1, Evidential weight and legal admissibility of information stored electronically

BIP 0008-1 serves as the supporting guideline for the implementation of BS 10008 and covers information management planning, risk evaluation, information security directives, documentation, data collection and processing, version control, storage systems, audit and continuous improvement.

BIP 0008-2, Evidential weight and legal admissibility of information transferred electronically

BIP 0008-2 targets in particular the authenticity, integrity and availability of information during electronic transmission (e.g. email, mobile messaging (SMS), instant messaging, web services, web forms, XML and electronic data interchange – EDI).

BIP 0008-3, Evidential weight and legal admissibility of linking electronic identity to documents

BIP 0008-3 deals with the authenticity, integrity and availability of electronic identities linked with documents (e.g. use of certificates and trusted third parties).

What are the risks of non-compliance?

The willful or negligent non-compliance with the obligation to retain records carries legal and material and immaterial risks. Various sanctions can apply if, for example, accounts are not properly maintained or stored in accordance with regulations. These sanctions range from the loss of pre-tax and after-tax (in the case of VAT-relevant services and products) to heavy fines and prison sentences. There are also immaterial risks, such as damage to reputation if, for example, data protection infringements are revealed and made public. Therefore, the structure of an ERMS should always include an adequate risk analysis. The diagram below shows some of the legal risk areas relevant to data archival.

The Criminal Code

In the scope of Art. 325, the Criminal Code stipulates fines for the infringement of obligations such as the proper management and storage of accounts and business correspondence.

Value Added Tax Act

VAT is a self-assessed tax. Proper bookkeeping and diligent storage are the basic prerequisites for tax assessment, tax levying and pre-tax collection. The following Swiss regulations define the basis for legally compliant archiving: Art. 958f OR (Swiss Code of Obligations), GeBüV and EIDI-V. Failure to comply with these regulations may result in a fine (Art. 98 MWSTG (Value Added Tax Act)).

The Data Privacy Act

The Data Privacy Act stipulates, inter alia, fines for the transfer of data collections abroad contrary to the statutory requirement to provide information (Art. 34). This also includes archiving abroad in particular.

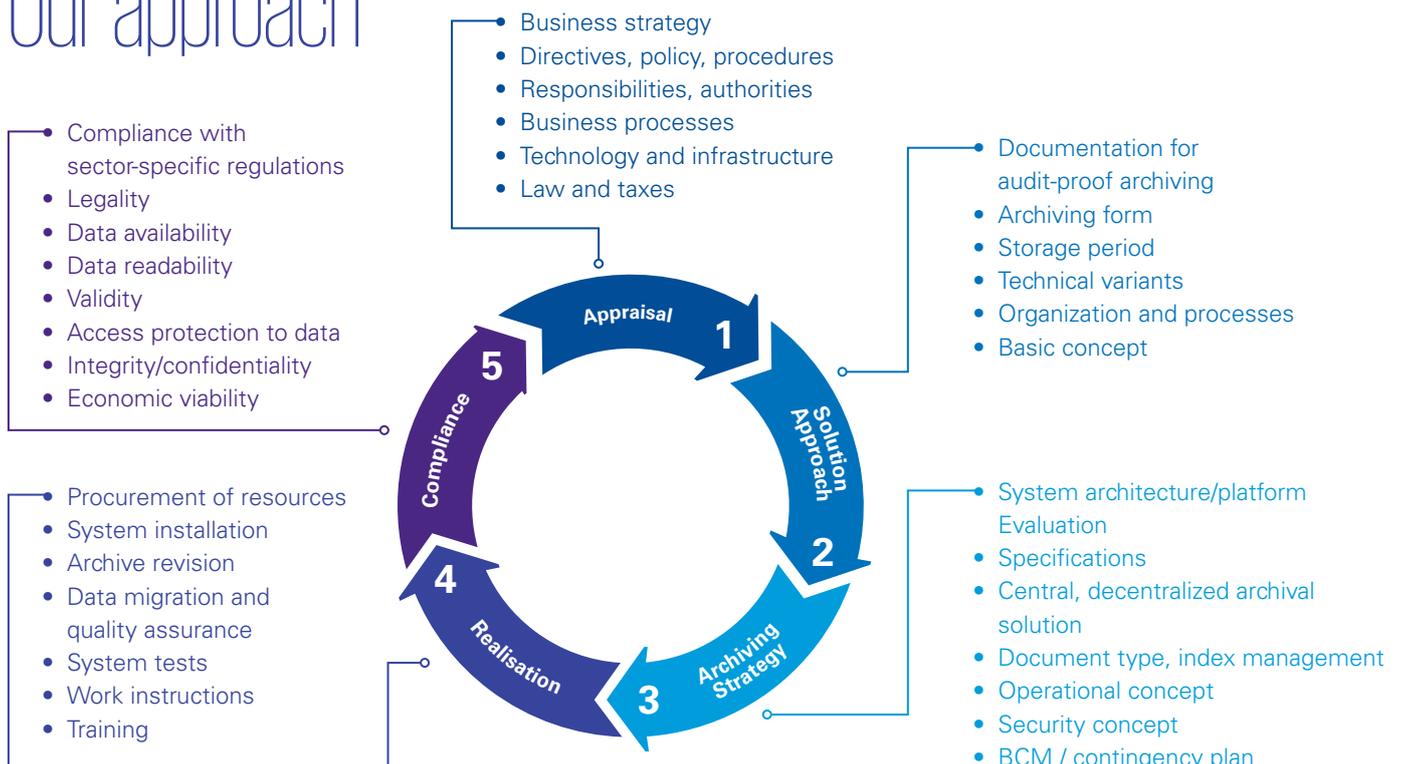
Regulations in the banking and financial market

Various provisions in the banking and financial market sector regulate the storage of relevant accounting records, supporting documents and the disclosure of such information and secrets. Over the last few years, penalties have become significantly stricter. Infringements can result in large fines and prison sentences and also carry regulatory risks.

The risk control system at a glance

Level	Standard	Chapter / control target areas of the ERMS	
Strategic level	BS 10008 <i>Evidential weight and legal admissibility of electronic information</i>	Planning of ERMS policies <ul style="list-style-type: none"> Information management Information security Electronic data archiving / transfer / identity evaluation 	<ul style="list-style-type: none"> Risk evaluation Audit processes Observation and monitoring Compliance and improvement
Tactical level	BS 10008 <i>Evidential weight and legal admissibility of electronic Information</i>	Planning <ul style="list-style-type: none"> Roles and responsibilities of employees Reports and communication 	<ul style="list-style-type: none"> Documentation and archival Information management tests
Operational level	BS 10008 BIP 0008-1 BIP 0008-2 BIP 0008-3	Implementation and operative <ul style="list-style-type: none"> Acquisition of information Self-adjustment of data Framework documents Version checking System maintenance 	<ul style="list-style-type: none"> Index and metadata Result Identity Use Back-up and regeneration
Principles, IT architecture	BS 10008 BIP 0008-1 BIP 0008-2 BIP 0008-3	Support <ul style="list-style-type: none"> Information storage Information transfer 	<ul style="list-style-type: none"> Information security / architecture External service provider
Basic security and IT architecture	ISO/IEC 27001	Basic security <ul style="list-style-type: none"> IT architecture Communication / transmission 	<ul style="list-style-type: none"> Identification / authorization Access / authorization concept

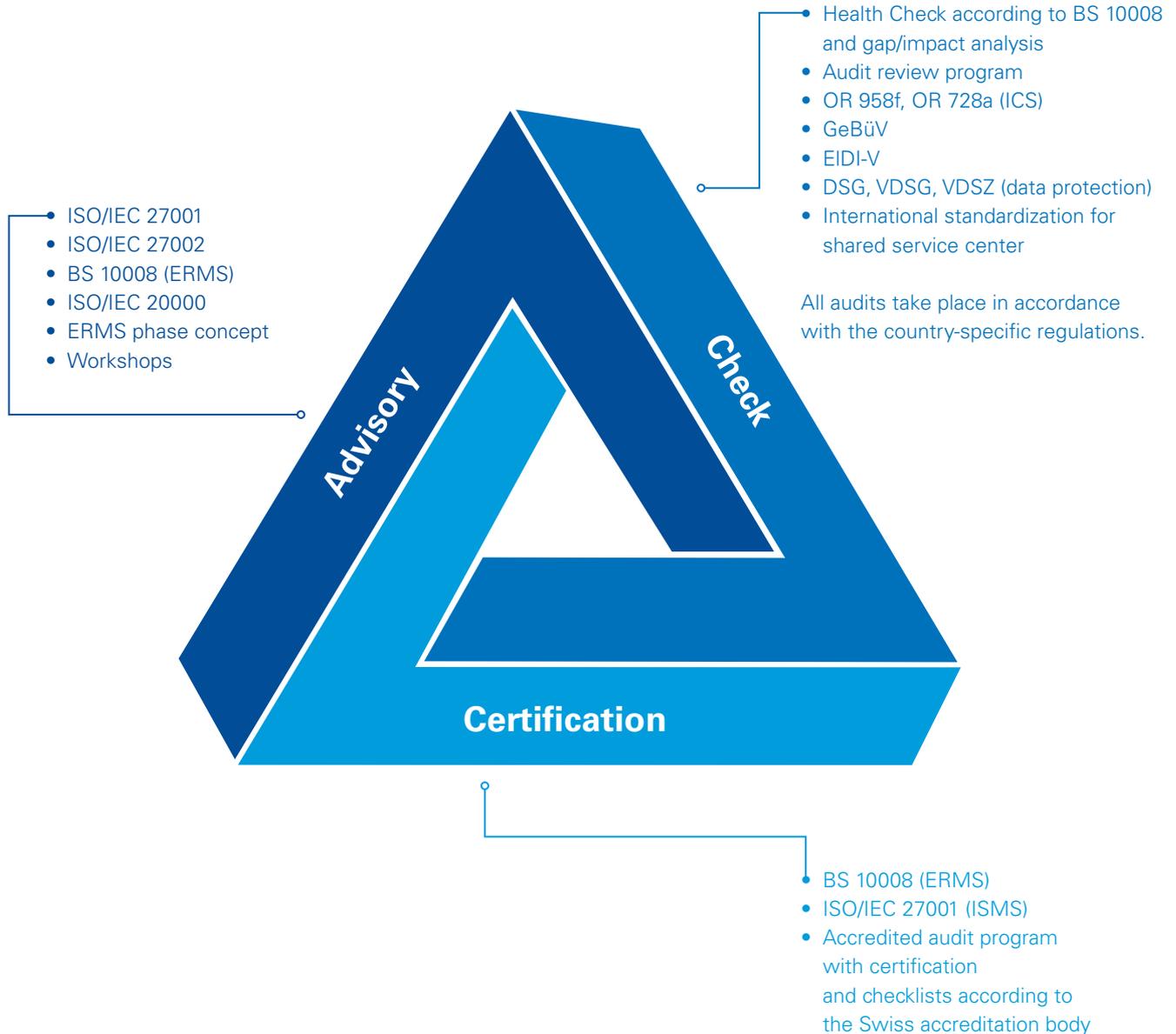
Our approach



Our service portfolio

As a multidisciplinary team with experts from information risk management, legal, tax and audit, we have more than 10 years of extensive experience in the consultation and inspection of archival and records management.

We offer the following certification services:



Contact

KPMG AG

Badenerstrasse 172
PO Box
CH-8036 Zurich

kpmg.ch/consulting

Matthias Bossardt

Partner
Head of Cyber Security

+41 58 249 36 98

mbossardt@kpmg.com

Reto Grubenmann

Director
Head of Certification Services

+41 58 249 42 46

retogrubenmann@kpmg.com

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received, or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. The scope of any potential collaboration with audit clients is defined by regulatory requirements governing auditor independence.

© 2016 KPMG AG is a subsidiary of KPMG Holding AG, which is a member of the KPMG network of independent firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss legal entity. All rights reserved.