ENISA Result:

Risk Management / Risk Assessment in European regulation, international guidelines and codes of practice

(also available under www.enisa.europa.eu/rmra)

Conducted by the

Technical Department of ENISA

Section Risk Management

in cooperation with:

Prof. J. Dumortier and
Hans Graux

lawfort

www.lawfort.be

June 2007

Executive Summary

This ENISA result encompasses international normative texts that directly or indirectly refer to aspects of Risk Management / Risk Assessment (RM / RA). The necessity of such a collection of regulations, directives, codes of practices and other document with normative character has been communicated to ENISA by different players in the area of Risk Management. To our knowledge, such a compilation of normative texts in the context of Risk Management / Risk Assessment is unique at the European level.

Due to the amount of available resources, only texts with European/international applicability have been considered within this document, while individual national normative texts have been left out of the scope of this document.

The identification of relevance of the considered texts to Risk Management / Risk Assessment has been performed on the basis of overview material delivered by ENISA in 2006 (see ENISA report on "*Risk Management: Implementation principles and Inventories for Risk Management / Risk Assessment methods and tools*"). The degree of relevance varies from direct relevance to indirect relevance according to the specificity of references found in the normative texts.

Except from the relevant provisions of the normative text, we present a short comprehensive description of what are the consequences of the text for Risk Management / Risk Assessment. This description will help experts without legal background to understand the essence of the normative text with regard to Risk Management.

The presented material can be used as a source of reference to existing legal frameworks. This is an inherent counterpart of initial phases of Risk Management / Risk Assessment where the applicable legal framework has to be identified (usually within the activity "*Definition of External Environment*"). It comprises one of the main parameters for the evaluation of impact of the assessed risks.

Furthermore, the presented material can be used by Member States to track national implementation status vis-à-vis existing international frameworks, as well as to reflect the status of transpositions of European directives and regulations. Upon the feedback we are going to receive in the future from interested parties (e.g. Member States, European stakeholders, European experts, organizations etc.), we are going to introduce a maintenance life-cycle for the presented material (e.g. expand it with additional normative texts, augment it with important national texts etc.). We expect that the flexible structure used for the compiled texts can be easily adapted to upcoming needs.

The presented material has been grouped in categories according to the horizontal applicability of normative areas, e.g. Data Protection/Privacy, National Security, Civil and Penal Law, Corporate Governance, etc. The vertical applicability according to application areas (e.g. Telecommunications, Financial Services, Health and Commerce Services) has not been considered. This was due to the fact the relevance of legal requirements to application areas may vary according to the security context of information being processed within the application. Thus, vertical aspects seemed not to be "stable" enough to be use as basis for the classification.

The content of this report is inline with a study performed by the ENISA ad hoc Working Group RANIS in 2006 (see also http://www.enisa.europa.eu/pages/ENISA_Working_group_RANIS.htm). The RANIS study presents EU legal instruments related to Network Information Security (NIS). This study is an inventory of European legislation on NIS, whereas the present report focuses on Risk Management and covers also international normative texts.

Contact details: ENISA Technical Department, Section Risk Management, Dr. L. Marinos, Senior Expert Risk Management, e-mail: RiskMngt@enisa.europa.eu

Contents

1. Introduction

The main objective of this study is to chart the primary components of the normative framework regarding risk management/risk assessment (RM/RA) practices within the European Union[1] and to assess their impact on European undertakings, both in the private and public sector. This knowledge is instrumental to determine to which extent these guidelines apply to management considerations, and thus to which extent they may impact network and information security practices.

While basic RM/RA obligations are clearly present in a number of European initiatives (including e.g. in the Privacy Directive[2]'s obligation to take the necessary technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access), it is also clear that such obligations do not cover the whole spectrum of RM/RA, nor are they specific to any given sector or field of endeavour.

No clear overview presently appears to exist of the predominant regulations in the field of RM/RA, nor to the norms being applied when attempting to conform to such regulations. This informational gap presents a double risk, both to private sector interests and from a policy perspective. On the one hand, private entities have no way of comprehensively determining whether or not they are in material compliance with any applicable regulations, nor can they verify which standards are available to them in attempting to ensure compliance, as no overview exists in either regard. On the other, public sector initiatives are equally impeded by the realisation that they potentially risk overlapping with an unknown number of pre-existing guidelines, and that they may not be fully aware of applicable norms in the field they are attempting to regulate.

Thus, an overview of RM/RA regulatory and normative initiatives, covering both organisational and infrastructural considerations, is a precondition for the proper development of good practices and possible new normative initiatives.

The classic regulatory areas well known in the field of RM/RA, such as data protection, have already been widely documented in the past, including as a part of ENISA research activities. On the other hand, some normative areas, in particular corporate governance, are less well documented and do not appear to have received the same level of scrutiny.

This is perhaps surprising, since corporate governance in the last decade has shown a distinct trend towards normative formalisation into guidelines, standards and generally accepted practices. Because this practice area is of general importance in daily business life, the creation of an overview document identifying and describing the main normative texts can be a useful resource in charting auditing requirements, applicable standards and corporate good practices.

Thus, this report will attempt to identify and analyse the main normative texts with regard to RM/RA applicable to European organisations, covering both international and European regulatory initiatives emanating from public sector bodies (including directives, regulations, resolutions, treaties, and conventions), as well as the most influential normative instruments originating from both generic and sector-specific private initiatives (including norms, (de facto) standards, guidelines, recommendations, and good practices).

Research therefore has been done on different levels, ranging from the EU and international institutions, through national regulations or standards, and sectoral or

[1] The study covers normative texts that apply in Europe while being of European and/or international origin.
[2] 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

normative body rules. However, this report only focuses on texts with a normative influence that extends beyond the national borders of any specific country. In the first section of the report below, we will define the basis on which texts will be included as relevant to this study.

The aspired final outcome of the report is the identification and summary description of the main normative texts with regard to RM/RA obligations, specifically in any legally binding references, that directly of indirectly impose or foresee the employment of RM/RA as a management activity within organisations and/or application systems, or provide guidance on how to comply with such obligations. The resulting report will provide ENISA with a general insight in the dominant norms in this respect, thus also providing a useful aid for any potential future field of activity.

2. RM / RA: Definitions and Scope

2.1 Defining RM/RA

In order to delineate the scope of the document, it is important to first define exactly what is meant by RM/RA. As a working basis for this document, the report relies on the definitions presented by ENISA itself in its report on '*Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools*'[3]. Annex I to this report contains a glossary, defining a number of key notions, including:

> *"G.30 Risk Assessment: A scientific and technologically based process (G.24) consisting of three steps, risk identification (G.38), risk analysis (G.29) and risk evaluation (G.36). (ENISA)*
>
> *[…]*
>
> *G.39 Risk Management: The process (G.24), distinct from risk assessment (G.30), of weighing policy alternatives in consultation with interested parties (G.18), considering risk assessment and other legitimate factors, and selecting appropriate prevention and control options. (ENISA)"*

Based on these definitions, it is clear that this report should focus on normative texts which contain:

- Explicit technical, organisational or legal requirements or recommendations with regard to RM/RA;
- A requirement or recommendation to conduct risk identification, analysis studies and risk evaluation studies on existing processes;
- A requirement or recommendation to prospectively conduct these same studies on planned processes (i.e. risk projections);

Normative texts which meet these criteria can be said to be directly relevant to RM/RA.

However, in addition to these criteria the report should also take into account any normative texts which contain requirements or recommendations to report risks or incidents to public/private sector bodies; or which regulate specific activities (e.g. e-commerce) or technologies (e.g. e-signatures) in which RM/RA is an implied consideration. These texts can be said to be indirectly relevant to RM/RA.

In order to provide a meaningful overview of the regulatory playing field, this report will describe both directly and indirectly relevant texts.

However, following these definitions, the scope of this report is still immensely broad, including detailed and sector specific regulations in such fields as biochemistry, aviation and transportation, agriculture and fishery, etc., all of which have their own standards which can be interpreted as directly or indirectly relevant to RM/RA. Most of these have only a very limited relevance to the activities of ENISA.

Therefore, in order to keep the result sufficiently focused to be of practical use, the focus of this report will be on texts which are relevant to ENISA's mission of striving to improve the security of communication networks and information systems. The focus will therefore be on norms which directly or indirectly relate to information/network RM/RA practices. Thus,

[3] See http://www.enisa.europa.eu/rmra/files/D1_Inventory_of_Methods_Risk_Management_Final.pdf, conducted by the Conducted by the Technical Department of ENISA, Section Risk Management, June 2006

the selection of normative texts included in this report will have a natural bias towards the ICT/telecommunications/data protection sectors. Other sectors will be included insofar as they are affected by norms which relate to information/network security, which is e.g. commonly the case for the financial sector.

2.2 Scope of the Report: relevant documents

It has been clear from the onset that the purpose of this report is not merely to provide an overview of formal legislative sources (such as directives, regulations, national laws with an international impact, etc.) with some relevance to RM/RA. Indeed, as was already noted above, the practices of corporate governance are not limited to such formally binding legal texts, but are increasingly dominated by private sector norms which provide guidance on how specific service providers are to meet their RM/RA obligations in practice.

While such standards are typically not legally binding, in many countries and in many sectors service providers risk liability when any damages result from disregarding them, on the grounds that ignoring established and well documented good practices is to be considered negligent conduct. Thus, in practice, certain codes of good practices/guidelines/generally accepted principles have attained the status of near-legal requirements or of informally codified customs of sound governance, which are equally significant to service providers as binding legislations. For this reason, the scope of the report is said to be ‘normative texts’, rather than ‘legislative’ or ‘regulatory texts’, which would suggest a limitation to formal sources of law.

For this same reason, it is also clear that the report cannot restrict its attention to purely European normative initiatives. In today’s increasingly expanding business market, the reality is that non-European initiatives (either international initiatives or national initiatives with an international impact) can be equally influential in RM/RA auditing practices as European norms. For all intents and purposes, such norms can be essential as a yardstick to measure the adequacy of corporate policies, and for this reason such documents will be included in the report as well.

Thus, to ensure the usability and validity of the report, this test should also be the final criterion to determine the relevance of any given normative text to the report: its value in assessing and measuring the adequacy of RM/RA practices and policies. The report will therefore include any influential text in the field of RM/RA which a suitably qualified auditor might rely upon to accept or criticise RM/RA practices and policies in the field of information/network security.

As a logical consequence of this criterion, the study excludes from its scope any document of which the principal goal is to state policy choices, without direct implications for specific parties other than calls for increased attention to RM/RA issues by public institutions.

2.3 Approach of the Report

The section below, which spans the bulk of this report, will provide an overview of the identified and analysed normative sources. It has to be mentioned, that the identification of the contents for this report has been based on further desk research, experience in auditing activities, and publications by established RM/RA linked organisations (including ENISA, the article 29 Working Party, ISACA, the Basel Committee, the NIST, etc.).

In order to efficiently identify the relevant sections of each normative instrument, most of the texts have undergone extensive examination to determine the context and scope of the relevant sections. For some of the more detailed or less known documents a key word based approach has been followed. Specifically, the analysis of the texts focused on a specific subset of keywords, including:

- Goal related keywords: security - protection - confidentiality - availability - integrity - confidence – assurance, etc.
- Challenge related keywords: risk - danger - threat - loss - incident - hazard – damage, etc.
- Infrastructure related keywords: information - data - network – connectivity, etc.
- Qualification related keywords: criminal - accidental - negligent – harmful, etc.

In this manner, the texts below have all undergone the analysis needed to create an overview document, as described below.

3. Template and structure of for the normative framework

The report contains an analysis of the main normative texts identified in the course of this study. For ease of reference, it has been split into six subsections: the present general overview, which contains an explanation table describing the template used for the collected information for each normative text; and sections, each of which contains the main provisions in a given subject field.

As previously mentioned, the subject fields used for classification of the normative texts is divided into horizontal categories according to the legal area of applicability of the normative text. The subject fields retained for the purposes of this report include:

- Data protection / privacy issues
- National security
- Civil and penal law
- Corporate governance and Operational Responsibility, (incl. continuity issues)
- E-Business
- RM/RA Standards

As stated above, these sections will always include both binding public sector initiatives (directives, regulations, national laws, etc.) and private sector norms (guidelines, codes of practice, etc.).

The vertical applicability according to application areas (e.g. Telecommunications, Financial Services, Health and Commerce Services) has not been considered. This was due to the fact the relevance of legal requirements to application areas may vary according to the security context of information being processed within the application. Thus, vertical aspects seemed not to be “stable” enough to be use as basis for the classification.

For the description of the normative texts, the following template is used (explanations of the particular fields are in *italics*):

Title:	*The full official title of the normative text; where multiple languages of the title exist, the English one is provided.*
Source reference:	*Reference to the source of the normative text. Hyperlinks are provided when available (in preference to paper sources), and official sources are used whenever possible.*
Topic:	*General description of the subject of the normative text.*
Scope:	*Description of the applicability of the normative text (which countries/enterprises/organisations are affected)*
Direct/indirect relevance	*Indication of direct or indirect relevance of the text to RM/RA (i.e. whether or not RM/RA is the direct focus of the text), and why.*
Legal force:	*Indication of the binding force: directive, directly binding, guideline, etc.*
Affected sectors:	*Description of the sectors affected by the normative text.*
Relevant provision(s):	*Direct and uncommented quote(s) from the relevant provision(s) of the normative text, when available (which may not be the case for closed standards or norms) and appropriate (which may not be the case for extensive documents which are relevant in their entirety to RM/RA). In cases where literal quotes would be unavailable or inappropriate, a summary of the norm’s main goals*

	and provisions will be provided.
Relevance to RM/RA:	*Brief explanation of why the normative text should be considered relevant for RM/RA purposes.*

A. Data Protection / Privacy

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Title:	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 (the 'Privacy Directive')
Source reference:	http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=Directive&an_doc=1995&nu_doc=46
Topic:	Generic personal data processing
Scope	Directly applicable to all EU Member States
Direct/ indirect relevance	Direct. The text directly prescribes an obligation to assess security measures with regard to data processing and to take the required security precautions.
Legal force:	EU Directive, requires transposition into national law
Affected sectors:	All sectors involved in personal data processing (including public sector, finance, health services, commerce, telecommunications, security management, etc.)
Relevant provision(s):	Article 17 - Security of processing 1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. 2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures. 3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that: - the processor shall act only on instructions from the controller, - the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor. 4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form. Article 19 - Contents of notification

	1. Member States shall specify the information to be given in the notification. It shall include at least: […] (f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing. […] CHAPTER IV TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES Article 25 - Principles 1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection. 2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country. […]
Relevance to RM/RA	The cited articles require that any personal data processing activity: undergoes a prior risk analysis in order to determine the privacy implications of the activity, and to determine the appropriate legal, technical and organisation measures to protect such activities; is effectively protected by such measures, which must be state of the art keeping into account the sensitivity and privacy implications of the activity (including when a third party is charged with the processing task) is notified to a national data protection authority, including the measures taken to ensure the security of the activity. Furthermore, article 25 and following of the Directive requires Member States to ban the transfer of personal data to non-Member States, unless such countries have provided adequate legal protection for such personal data, or barring certain other exceptions.

Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data

Title:	Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data
Source reference:	http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32001R0045&model=guichett
Topic:	Personal data processing by the Community institutions, including in the context of internal communication networks
Scope	Directly applicable to all Community institutions and bodies (including on a national scale)
Direct/ indirect relevance	Direct. The text directly prescribes an obligation to assess security measures with regard to data processing and to take the required security precautions.
Legal force:	Internal regulation, directly binding to the affected institutions
Affected sectors:	All Community institutions and bodies (including on a national scale)
Relevant provision(s):	Article 22 - Security of processing 1. Having regard to the state of the art and the cost of their implementation, the controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected. Such measures shall be taken in particular to prevent any unauthorised disclosure or access, accidental or unlawful destruction or accidental loss, or alteration, and to prevent all other unlawful forms of processing. 2. Where personal data are processed by automated means, measures shall be taken as appropriate in view of the risks in particular with the aim of: (a) preventing any unauthorised person from gaining access to computer systems processing personal data; (b) preventing any unauthorised reading, copying, alteration or removal of storage media; (c) preventing any unauthorised memory inputs as well as any unauthorised disclosure, alteration or erasure of stored personal data; (d) preventing unauthorised persons from using data-processing systems by means of data transmission facilities; (e) ensuring that authorised users of a data-processing system can access no personal data other than those to which their access right refers; (f) recording which personal data have been communicated, at what times and to whom; (g) ensuring that it will subsequently be possible to check which personal data have been processed, at what times and by whom; (h) ensuring that personal data being processed on behalf of third parties can be processed only in the manner prescribed by the contracting institution or body; (i) ensuring that, during communication of personal data and during transport of storage media, the data cannot be read, copied or erased without authorisation; (j) designing the organisational structure within an institution or body in

	such a way that it will meet the special requirements of data protection. Article 23 – Processing of personal data on behalf of controllers 1. Where a processing operation is carried out on its behalf, the controller shall choose a processor providing sufficient guarantees in respect of the technical and organisational security measures required by Article 22 and ensure compliance with those measures. 2. The carrying out of a processing operation by way of a processor shall be governed by a contract or legal act binding the processor to the controller and stipulating in particular that: (a) the processor shall act only on instructions from the controller; (b) the obligations set out in Articles 21 and 22 shall also be incumbent on the processor unless, by virtue of Article 16 or Article 17(3), second indent, of Directive 95/46/EC, the processor is already subject to obligations with regard to confidentiality and security laid down in the national law of one of the Member States. 3. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in Article 22 shall be in writing or in another equivalent form. […] Article 35 – Security 1. The Community institutions and bodies shall take appropriate technical and organisational measures to safeguard the secure use of the telecommunications networks and terminal equipment, if necessary in conjunction with the providers of publicly available telecommunications services or the providers of public telecommunications networks. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented. 2. In the event of any particular risk of a breach of the security of the network and terminal equipment, the Community institution or body concerned shall inform users of the existence of that risk and of any possible remedies and alternative means of communication.
Relevance to RM/RA	The cited articles provide an internal regulation which is a practical application of the principles of the Privacy Directive described above. They require that any personal data processing activity by Community institutions: undergoes a prior risk analysis in order to determine the privacy implications of the activity, and to determine the appropriate legal, technical and organisation measures to protect such activities; is effectively protected by such measures, which must be state of the art keeping into account the sensitivity and privacy implications of the activity; are governed by suitable and enforced agreements when a third party is charged with the processing task Furthermore, article 35 of the Regulation requires the Community institutions and bodies to take similar precautions with regard to their telecommunications infrastructure, and to properly inform the users of any specific risks of security breaches.

Safe Harbour Privacy Principles issued by the US Department of Commerce on July 21, 2000

Title:	Safe Harbour Privacy Principles
Source reference:	http://www.export.gov/safeharbor/SH_Documents.asp
Topic:	Export of personal data from a data controller who is subject to E.U. privacy regulations to a U.S. based destination
Scope	Voluntary adherence by the affected U.S. entities
Direct/ indirect relevance	Direct. Entities wishing to accede to the Safe Harbour are required to assess security measures with regard to data processing and to take the required security precautions.
Legal force:	Voluntary self-certification. The voluntary character is relative, since the data controller must comply with E.U. privacy regulations, but alternative methods of compliance (such as the model clauses discussed below) exist.
Affected sectors:	Generic export of personal data to a U.S. entity
Relevant provision(s):	SECURITY: Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction. […] ENFORCEMENT: Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.
Relevance to RM/RA	Before personal data may be exported from an entity subject to E.U. privacy regulations to a destination subject to U.S. law, the European entity must ensure that the receiving entity provides adequate safeguards to protect such data against a number of mishaps. One way of complying with this obligation is to require the receiving entity to join the Safe Harbour, by requiring that the entity self-certifies its compliance with the so-called Safe Harbour Principles. If this road is chosen, the data controller exporting the data must verify that the U.S. destination is indeed on the Safe Harbour list (see http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list)

UN Guidelines concerning computerized personal data files of 14 December 1990

Title:	Guidelines for the Regulation of Computerized Personal Data Files, as adopted by General Assembly resolution 45/95 of 14 December 1990
Source reference:	http://www.unhchr.ch/html/menu3/b/71.htm
Topic:	Generic data processing activities using digital processing methods
Scope	Nonbinding guideline to UN nations calling for national regulation in this field
Direct/ indirect relevance	Direct. The text directly prescribes a duty to assess security measures with regard to data processing and to take the required security precautions.
Legal force:	Not legally binding, neither to natural persons, legal entities or countries
Affected sectors:	Generic data processing activities using digital processing methods
Relevant provision(s):	7. Principle of security Appropriate measures should be taken to protect the files against both natural dangers, such as accidental loss or destruction and human dangers, such as unauthorized access, fraudulent misuse of data or contamination by computer viruses.
Relevance to RM/RA	The UN Guidelines are mostly of historical importance, as a background to more recent regulation, including (if not particularly) the aforementioned Privacy Directive. None the less, the Guidelines are a summary statement of basic principles with regard to automated data processing.

Organisation for Economic Co-operation and Development (OECD) Recommendation of the Council concerning guidelines governing the protection of privacy and trans-border flows of personal data

Title:	Recommendation of the council concerning guidelines governing the protection of privacy and trans-border flows of personal data (23 September 1980)
Source reference:	http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html
Topic:	Generic data processing activities, including the export of personal data
Scope	Nonbinding recommendation to OECD nations calling for national regulation in this field
Direct/ indirect relevance	Direct. The text directly prescribes a duty to assess security measures with regard to data processing and to take the required security precautions.
Legal force:	Not legally binding, neither to natural persons, legal entities or countries
Affected sectors:	Generic data processing activities using digital processing methods
Relevant provision(s):	Security Safeguards Principle 11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data. [...] 15. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data. 16. Member countries should take all reasonable and appropriate steps to ensure that trans-border flows of personal data, including transit through a Member country, are uninterrupted and secure. 17. A Member country should refrain from restricting trans-border flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.
Relevance to RM/RA	Similar to the UN Guidelines directly above, the OECD Recommendations are mostly of historical importance, as a background to more recent regulation, including (if not particularly) the aforementioned Privacy Directive. None the less, the Recommendations are a summary statement of basic principles with regard to automated data processing.

COE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

Title:	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981
Source reference:	http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm
Topic:	Automated data processing activities, including the export of personal data
Scope	Convention which is binding to the signatory states (which includes all E.U. Member States) after the entry into force of the convention, which occurred on 1 October 1985.
Direct/ indirect relevance	Direct. The text directly prescribes an obligation to assess security measures with regard to data processing and to take the required security precautions.
Legal force:	Requires signatory states to provide the necessary privacy protection provisions in their national regulatory frameworks.
Affected sectors:	Automated data processing activities
Relevant provision(s):	Article 7 – Data security Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.
Relevance to RM/RA	Similar to the UN Guidelines above, the COE Convention is mostly of historical importance, as a background to more recent regulation, including (if not particularly) the aforementioned Privacy Directive. None the less, the COE Convention is a summary statement of basic principles with regard to automated data processing.

The model contracts and clauses for the transfer of personal data to third countries established by Commission Decision

Title:	Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC; and the Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries
Source reference:	http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm
Topic:	Export of personal data to third countries, specifically non-E.U. countries which have not been recognised as having a data protection level that is adequate (i.e. equivalent to that of the E.U.)
Scope	The Commission Decisions both define a distinct set of model clauses which can be adopted on a voluntary basis by parties wishing to export personal data outside the E.U., in compliance with the Data Protection Directive
Direct/ indirect relevance	Direct. The text directly prescribes an obligation to assess security measures with regard to data processing and to take the required security precautions.
Legal force:	Model clauses, i.e. strictly voluntary.
Affected sectors:	Can be adopted on a voluntary basis by any parties wishing to export personal data outside the E.U.
Relevant provision(s):	Commission decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC – Annex – Standard Contractual Clauses – Appendix 2 to the Standard Contractual Clauses Clause 5 – Obligations of the data importer The data importer agrees and warrants: (b) to process the personal data in accordance with mandatory data protection principles set out in Appendix II; […] […] (d) at the request of the data exporter to submit its data processing facilities for which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications, selected by the data exporter, where applicable, in agreement with the supervisory authority. […] Appendix 2 to the standard contractual clauses – Mandatory data protection principles referred to in the first paragraph of Clause 5(b) […] 4. Security and confidentiality – technical and organisational measures must be taken by the data controller that are appropriate to the risks, such as unauthorised access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the controller.

	Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries – Annex - SET II - Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers) II. Obligations of the data importer The data importer warrants and undertakes that: (a) It will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected. […] (g) Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion. […] Annex A – Data processing principles 4. Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.
Relevance to RM/RA	Both Commission Decisions provide a set of voluntary model clauses which can be use to export personal data from a data controller (who is subject to E.U. data protection rules) to a data processor outside the E.U. who is not subject to these rules or to a similar set of adequate rules. Upon acceptance of the model clauses, the data controller must warrant that she has taken the appropriate legal, technical and organisational measures to ensure the protection of the personal data against (inter alia) accidental loss, destruction or unauthorised access, including by acts of the data processor. Furthermore, the data processor must agree to permit auditing of its security practices to ensure compliance with applicable European data protection rules.

The Article 29 Working Party recommendations, consultations and policy documents

Title:	Article 29 Working Party opinions (no specific document)
Source reference:	http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_en.htm (no specific document)
Topic:	Opinions of the Working Party regarding specific aspects of data protection
Scope	The scope is determined by the subject of the opinion, and can vary widely
Direct/ indirect relevance	Direct or indirect, depending on the scope and contents of the opinion.
Legal force:	While not strictly legally binding, non-compliance with an opinion of the Working Party is highly indicative of violation of European data protection regulations. The opinions are authoritative, but not binding.
Affected sectors:	The affected sectors are determined by the subject of the opinion, and can vary widely.
Relevant provision(s):	Relevant provisions depend on the specific opinion.
Relevance to RM/RA	The Working Group frequently voices its opinion on controversial issues in the field of data protection, such as data retention (Opinion 1/2007), flight passenger data (Opinion 9/2006), and the Safe Harbour arrangements (Opinion 4/2000). While the opinions are principally relevant for regulatory initiatives (as they often evaluate the adequacy of proposed or existing regulation, or of their application in practice), the opinions can also be relevant for the evaluation of RM/RA practices in the field concerned, since issues highlighted by the Working Party may prove to be problematic in practice, even if no further regulatory initiatives have followed the opinion.

Health Insurance Portability and Accountability Act

Title:	Health Insurance Portability and Accountability Act (HIPAA; often misquoted as 'HIPPA') of 1996
Source reference:	http://www.legalarchiver.org/hipaa.htm
Topic:	U.S. Act with regard to health insurance coverage, electronic health, and requirements with regard to the security and privacy of health data
Scope	Directly applicable to the practices governed by the U.S. Act, including in particular health insurance plans, administrative simplification in the health sector, and the processing of personal health care data
Direct/ indirect relevance	Direct. The norm directly prescribes an obligation to assess security measures with regard to data processing and to take the required security precautions.
Legal force:	U.S. legislation; not applicable to health service organisations which are not subject to U.S. law. Violations are subject to civil and penal sanctions
Affected sectors:	Health care services
Relevant provision(s):	From an RM/RA perspective, the Act is particularly known for its provisions with regard to Administrative Simplification (Title II of HIPAA). This title required the U.S. Department of Health and Human Services (HHS) to draft specific rulesets, each of which would provide specific standards which would improve the efficiency of the health care system and prevent abuse. As a result, the HHS has adopted five principal rules: the Privacy Rule, the Transactions and Code Sets Rule, the Unique Identifiers Rule, the Enforcement Rule, and the Security Rule. The latter, published in the Federal Register on 20 February 2003 (see: http://www.cms.hhs.gov/SecurityStandard/Downloads/securityfinalrule.pdf), is specifically relevant, as it specifies a series of administrative, technical, and physical security procedures to assure the confidentiality of electronic protected health information. These aspects have been further outlined in a set of Security Standards on Administrative, Physical, Organisational and Technical Safeguards, all of which have been published, along with a guidance document on the basics of HIPAA risk management and risk assessment (see http://www.cms.hhs.gov/EducationMaterials/04_SecurityMaterials.asp). HIPAA security standards include the following: Administrative safeguards: Security Management Process Assigned Security Responsibility Workforce Security Information Access Management Security Awareness and Training Security Incident Procedures Contingency Plan Evaluation Business Associate Contracts and Other Arrangements Physical safeguards Facility Access Controls Workstation Use Workstation Security

	Device and Media Controls Technical safeguards Access Control Audit Controls Integrity Person or Entity Authentication Transmission Security Organisational requirements Business Associate Contracts & Other Arrangements Requirements for Group Health Plans
Relevance to RM/RA	European health care service providers will generally not be affected by HIPAA obligations if they are not active on the U.S. market. However, since their data processing activities are subject to similar obligations under general European law (including the Privacy Directive), and since the underlying trends of modernisation and evolution towards electronic health files are the same, the HHS safeguards can be useful as an initial yardstick for measuring RM/RA strategies put in place by European health care service providers, specifically with regard to the processing of electronic health information.

Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector[4]

Title:	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)
Source reference:	http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=32002L0058&model=guichett
Topic:	Personal data processing in the telecommunications sector
Scope	Directly applicable to all EU Member States
Direct/ indirect relevance	Direct. The text directly prescribes an obligation to assess security measures with regard to data processing and to take the required security precautions.
Legal force:	EU Directive, requires transposition into national law
Affected sectors:	Publicly available electronic communications services in public communications networks in the Community
Relevant provision(s):	Article 4 - Security 1. The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented. 2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.
Relevance to RM/RA	The cited article requires that any provider of publicly available electronic communications services: Takes the appropriate legal, technical and organisational measures to ensure the security of its services. It should be noted that this extends beyond the scope of the Privacy Directive described elsewhere, since article 4 is not limited to the protection of personal data; Informs his subscribers of any particular risks of security breaches, takes the necessary measures to prevent such breaches, and indicates the likely costs of security breaches to the subscribers.

[4] This Directive repealed and replaced Directive 97/66/EC of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector; the latter of which shall therefore not be commented in this report.

B. National Security

Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC ('Data Retention Directive')

Title:	Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC
Source reference:	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:NOT
Topic:	Requirement for the providers of public electronic telecommunications service providers to retain certain information for the purposes of the investigation, detection and prosecution of serious crime
Scope	Applicable to the providers of publicly available electronic communications service providers in the E.U.
Direct/ indirect relevance	Direct. The text directly prescribes an obligation to ensure the availability and quality of the retained data.
Legal force:	EU Directive, requires transposition into national law. The deadline for transposition depends on the activity of the service provider (a later deadline is provided for ISPs) and on the Member State (certain Member States have announced that they require more time for ISPs); but the earliest deadline for transposition is 15 September 2007
Affected sectors:	Providers of publicly available electronic communications services in the E.U., including ISPs
Relevant provision(s):	Article 3 – Obligation to retain data 1. By way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned. 2. The obligation to retain data provided for in paragraph 1 shall include the retention of the data specified in Article 5 relating to unsuccessful call attempts where those data are generated or processed, and stored (as regards telephony data) or logged (as regards Internet data), by providers of publicly available electronic communications services or of a public communications network within the jurisdiction of the Member State concerned in the process of supplying the communication services concerned. This Directive shall not require data relating to unconnected calls to be retained. Article 4 – Access to data Member States shall adopt measures to ensure that data retained in accordance with this Directive are provided only to the competent national authorities in specific cases and in accordance with national law. The procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in

	its national law, subject to the relevant provisions of European Union law or public international law, and in particular the ECHR as interpreted by the European Court of Human Rights. Article 7 – Data protection and data security Without prejudice to the provisions adopted pursuant to Directive 95/46/EC and Directive 2002/58/EC, each Member State shall ensure that providers of publicly available electronic communications services or of a public communications network respect, as a minimum, the following data security principles with respect to data retained in accordance with this Directive: (a) the retained data shall be of the same quality and subject to the same security and protection as those data on the network; (b) the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure; (c) the data shall be subject to appropriate technical and organisational measures to ensure that they can be accessed by specially authorised personnel only; and (d) the data, except those that have been accessed and preserved, shall be destroyed at the end of the period of retention. Article 8 – Storage requirements for retained data Member States shall ensure that the data specified in Article 5 are retained in accordance with this Directive in such a way that the data retained and any other necessary information relating to such data can be transmitted upon request to the competent authorities without undue delay.
Relevance to RM/RA	The cited articles require the affected providers of publicly accessible electronic telecommunications networks: To retain certain communications data (including unsuccessful call attempts) to be specified in their national regulations, for a specific amount of time, under secured circumstances in compliance with applicable privacy regulations; To provide access to this data to competent national authorities. This requires that the providers is aware of the locally competent authorities, and that it is capable of assessing the validity of the request; To ensure data quality and security through appropriate technical and organisational measures, shielding it from access by unauthorised individuals; and to ensure its destruction when it is no longer required; To ensure that stored data can be promptly delivered upon request from the competent authorities.

Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection ('ECI Directive')

Title:	Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection **Note: the present overview describes a norm in draft stage, which is susceptible to significant change in the course of finalisation!**
Source reference:	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0787:FIN:EN:HTML
Topic:	Identification and protection of European Critical Infrastructures
Scope	Applicable to Member States and to the operators of European Critical Infrastructure (defined by the draft directive as 'critical infrastructures the disruption or destruction of which would significantly affect two or more Member States, or a single Member State if the critical infrastructure is located in another Member State. This includes effects resulting from cross-sector dependencies on other types of infrastructure').
Direct/ indirect relevance	Direct. The text directly prescribes an obligation to identify European Critical Infrastructures and to draft adequate plans for their continuity.
Legal force:	None; the norm is currently only in draft stage. Upon finalisation: an EU Directive, requires transposition into national law.
Affected sectors:	Member States and to the operators of European Critical Infrastructure
Relevant provision(s):	Article 3 - Identification of European Critical Infrastructure […] 3. Each Member State shall identify the critical infrastructures located within its territory as well as critical infrastructures outside its territory that may have an impact on it, which satisfy the criteria adopted pursuant to paragraphs 1 and 2. Each Member State shall notify the Commission of the critical infrastructures thus identified at the latest one year after the adoption of the relevant criteria and thereafter on an ongoing basis. Article 4 - Designation of European Critical Infrastructure 1. On the basis of the notifications made pursuant to the second paragraph of Article 3(3) and any other information at its disposal, the Commission shall propose a list of critical infrastructures to be designated as European Critical Infrastructures. […] Article 5 - Operator Security Plans 1. Each Member State shall require the owners/operators of each European Critical Infrastructure located on its territory to establish and update an Operator Security Plan and to review it at least every two years. 2. The Operator Security Plan shall identify the assets of the European Critical Infrastructure and establish relevant security solutions for their

	protection in accordance with Annex II. Sector specific requirements concerning the Operator Security Plan taking into account existing Community measures may be adopted in accordance with the procedure referred to in Article 11(3). Acting in accordance with the procedure referred to in Article 11(2), the Commission may decide that compliance with measures applicable to specific sectors listed in Annex I satisfies the requirement to establish and update an Operator Security Plan. 3. The owner/operator of a European Critical Infrastructure shall submit the Operator Security Plan to the relevant Member State authority within one year following designation of the critical infrastructure as a European Critical Infrastructure. Where sector specific requirements concerning the Operator Security Plan are adopted based on paragraph 2, the operator security plan shall only be submitted to the relevant Member State authority within 1 year following the adoption of the sector specific requirements. 4. Each Member State shall set up a system ensuring adequate and regular supervision of the Operator Security Plans and their implementation based on the risk and threat assessments conducted pursuant to Article 7(1). 5. Compliance with Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security satisfies the requirement to establish an Operator Security Plan. Article 6 Security Liaison Officers 1. Each Member State shall require the owners/operators of European Critical Infrastructures on their territory to designate a Security Liaison Officer as the point of contact for security related issues between the owner/operator of the infrastructure and the relevant critical infrastructure protection authorities in the Member State. The Security Liaison Officer shall be designated within one year following the designation of the critical infrastructure as a European Critical Infrastructure. 2. Each Member State shall communicate relevant information concerning identified risks and threats to the Security Liaison Officers of the European Critical Infrastructure concerned. Article 7 Reporting 1. Each Member State shall conduct a risk and threat assessment in relation to ECI situated on their territory within one year following the designation of the critical infrastructure as an ECI. […]
Relevance to RM/RA	The cited articles require Member States to identify critical infrastructures on their territories, and to designate them as ECIs. Following this designation, the owners/operators of ECIs are required to create Operator Security Plans (OSPs), which should establish relevant security solutions for their protection.

Regulation (EC) No 1907/2006 of 18 December 2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH)

Title:	Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), establishing a European Chemicals Agency, amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC
Source reference:	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:396:0001:0849:EN:PDF
Topic:	Regulation establishing an agency to monitor chemicals in the E.U., and creating principles for the registration and evaluation of such chemicals
Scope	Directly applicable to the practices governed by the regulation
Direct/ indirect relevance	Indirect. The focus of the text is on biochemical safety, which indirectly implies ICT-RM/RA obligations.
Legal force:	Directly binding to the affected bodies
Affected sectors:	Biochemical sector (including both manufacturers and importers of the substances involved)
Relevant provision(s):	The regulation, spanning 849 pages, includes a multitude of provisions directly related to risk management. Since risk management is a continuous consideration in this document, it would be infeasible to provide a representative overview in a reasonable manner. Relevant provisions include the following (by way of non-exhaustive example): Article 14 - Chemical safety report and duty to apply and recommend risk reduction measures 1. Without prejudice to Article 4 of Directive 98/24/EC, a chemical safety assessment shall be performed and a chemical safety report completed for all substances subject to registration in accordance with this Chapter in quantities of 10 tonnes or more per year per registrant. The chemical safety report shall document the chemical safety assessment which shall be conducted in accordance with paragraphs 2 to 7 and with Annex I for either each substance on its own or in a preparation or in an article or a group of substances. 2. A chemical safety assessment in accordance with paragraph 1 need not be performed for a substance which is present in a preparation if the concentration of the substance in the preparation is less than the lowest of any of the following: […] 3. A chemical safety assessment of a substance shall include the following steps: (a) human health hazard assessment; (b) physicochemical hazard assessment; (c) environmental hazard assessment; (d) persistent, bio-accumulative and toxic (PBT) and very persistent and very bio-accumulative (vPvB) assessment. 4. If, as a result of carrying out steps (a) to (d) of paragraph 3, the registrant concludes that the substance meets the criteria for classification as dangerous in accordance with Directive 67/548/EEC or

	is assessed to be a PBT or vPvB, the chemical safety assessment shall include the following additional steps: (a) exposure assessment including the generation of exposure scenario(s) (or the identification of relevant use and exposure categories if appropriate) and exposure estimation; (b) risk characterisation. The exposure scenarios (where appropriate the use and exposure categories), exposure assessment and risk characterisation shall address all identified uses of the registrant. 5. The chemical safety report need not include consideration of the risks to human health from the following end uses: (a) in food contact materials within the scope of Regulation (EC) No 1935/2004 of the European Parliament and of the Council of 27 October 2004 on materials and articles intended to come into contact with food; (b) in cosmetic products within the scope of Directive 76/768/EEC. 6. Any registrant shall identify and apply the appropriate measures to adequately control the risks identified in the chemical safety assessment, and where suitable, recommend them in the safety data sheets which he supplies in accordance with Article 31. 7. Any registrant required to conduct a chemical safety assessment shall keep his chemical safety report available and up to date. Article 44 – Criteria for substance evaluation 1. In order to ensure a harmonised approach, the Agency shall in cooperation with the Member States develop criteria for prioritising substances with a view to further evaluation. Prioritisation shall be on a risk-based approach. The criteria shall consider: (a) hazard information, for instance structural similarity of the substance with known substances of concern or with substances which are persistent and liable to bio-accumulate, suggesting that the substance or one or more of its transformation products has properties of concern or is persistent and liable to bio-accumulate; (b) exposure information; (c) tonnage, including aggregated tonnage from the registrations submitted by several registrants. 2. The Agency shall use the criteria in paragraph 1 for the purpose of compiling a draft Community rolling action plan which shall cover a period of three years and shall specify substances to be evaluated each year. Substances shall be included if there are grounds for considering (either on the basis of a dossier evaluation carried out by the Agency or on the basis of any other appropriate source, including information in the registration dossier) that a given substance constitutes a risk to human health or the environment. The Agency shall submit the first draft rolling action plan to the Member States by 1 December 2011. The Agency shall submit draft annual updates to the rolling action plan to the Member States by 28 February each year. […]
Relevance to RM/RA	The regulation implants RM/RA obligations by: Imposing a reporting obligation, including on producers and importers of articles covered by the Regulation, with regard to the qualities of certain chemical substances, which includes a risk assessment and obligation to examine how such risks can be managed. This information is to be registered in a central database. A European Chemicals Agency will act

	as the central point in the REACH system (Registration, Evaluation, Authorisation and restrictions of Chemicals; Establishing a Committee for Risk Assessment within the European Chemicals Agency established by the Regulation; Requiring that the information provided is kept up to date with regard to potential risks to human health or the environment, and that such risks are adequately managed; (See also: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/06/488&format=HTML&aged=0&language=EN&guiLanguage=en

C. Civil and Penal Law

Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems

Title:	Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems
Source reference:	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:EN:NOT
Topic:	General decision aiming to harmonise national provisions in the field of cyber crime, encompassing material criminal law (i.e. definitions of specific crimes), procedural criminal law (including investigative measures and international cooperation) and liability issues.
Scope	Requires Member States to implement the provisions of the Framework Decision in their national legal frameworks.
Direct/ indirect relevance	Indirect. The legal liability rules imply an indirect obligation to assess one's legal risk in the applicable jurisdictions.
Legal force:	The Council Decision is binding, and requires Member States to ensure compliance of their national legal frameworks with the Framework Decision by 16 March 2007.
Affected sectors:	Generic; the provisions can be relevant to any entity involved with information systems and data processing, in view of the topic of the normative text.
Relevant provision(s):	Article 8 – Liability of legal persons 1. Each Member State shall take the necessary measures to ensure that legal persons can be held liable for offences referred to in Articles 2, 3, 4 and 5, committed for their benefit by any person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on: (a) a power of representation of the legal person, or (b) an authority to take decisions on behalf of the legal person, or (c) an authority to exercise control within the legal person. 2. Apart from the cases provided for in paragraph 1, Member States shall ensure that a legal person can be held liable where the lack of supervision or control by a person referred to in paragraph 1 has made possible the commission of the offences referred to in Articles 2, 3, 4 and 5 for the benefit of that legal person by a person under its authority. 3. Liability of a legal person under paragraphs 1 and 2 shall not exclude criminal proceedings against natural persons who are involved as perpetrators, instigators or accessories in the commission of the offences referred to in Articles 2, 3, 4 and 5. Article 9 - Penalties for legal persons 1. Each Member State shall take the necessary measures to ensure that a legal person held liable pursuant to Article 8(1) is punishable by effective, proportionate and dissuasive penalties, which shall include criminal or non-criminal fines and may include other penalties, such as: (a) exclusion from entitlement to public benefits or aid; (b) temporary or permanent disqualification from the practice of commercial activities; (c) placing under judicial supervision; or

	(d) a judicial winding-up order. 2. Each Member State shall take the necessary measures to ensure that a legal person held liable pursuant to Article 8(2) is punishable by effective, proportionate and dissuasive penalties or measures. Article 10 – Jurisdiction 1. Each Member State shall establish its jurisdiction with regard to the offences referred to in Articles 2, 3, 4 and 5 where the offence has been committed: (a) in whole or in part within its territory; or (b) by one of its nationals; or (c) for the benefit of a legal person that has its head office in the territory of that Member State. 2. When establishing its jurisdiction in accordance with paragraph (1)(a), each Member State shall ensure that the jurisdiction includes cases where: (a) the offender commits the offence when physically present on its territory, whether or not the offence is against an information system on its territory; or (b) the offence is against an information system on its territory, whether or not the offender commits the offence when physically present on its territory.
Relevance to RM/RA	Apart from the definitions of a series of criminal offences in articles 2 to 5, the Framework decision is relevant to RM/RA because it contains the conditions under which legal liability can be imposed on legal entities for conduct of certain natural persons of authority within the legal entity. Thus, the Framework decision requires that the conduct of such figures within an organisation is adequately monitored, also because the Decision states that a legal entity can be held liable for acts of omission in this regard. Additionally, article 10 defines a series of criteria under which jurisdictional competence can be established. These include the competence of a jurisdiction when a criminal act is conducted against an information system within its borders (art.10, 2, (b)). Thus, legal entities need to be aware of the applicable laws in countries where their infrastructure is established, even if they conduct no further business there.

COE Convention on Cyber Crime

Title:	Council of Europe Convention on Cybercrime, Budapest, 23.XI.2001, European Treaty Series-No. 185
Source reference:	http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm
Topic:	General treaty aiming to harmonise national provisions in the field of cyber crime, encompassing material criminal law (i.e. definitions of specific crimes), procedural criminal law (including investigative measures and international cooperation), liability issues and data retention.
Scope	Convention which is binding to the signatory states (which includes all E.U. Member States) after the entry into force of the convention, which occurred on 1 July 2004.
Direct/ indirect relevance	Indirect. The liability and cooperation rules imply an indirect obligation to implement adequate RM/RA practices to ensure that one's legal liability can be assessed and controlled.
Legal force:	Requires signatory states to update their national regulatory frameworks to include certain anti-cyber crime provisions.
Affected sectors:	Generic; the provisions can be relevant to any entity involved with information systems and data processing, in view of the topic of the normative text.
Relevant provision(s):	Article 12 – Corporate liability 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence. Article 13 – Sanctions and measures […] 2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including

	monetary sanctions. Title 2 – Expedited preservation of stored computer data Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. Article 17 – Expedited preservation and partial disclosure of traffic data 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. Title 3 – Production order Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

	b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. […] Title 5 – Real-time collection of computer data Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of

	technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. Section 3 – Jurisdiction Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. […]
Relevance to RM/RA	Apart from the definitions of a series of criminal offences in articles 2 to 10, the Convention is relevant to RM/RA because it states the conditions under which legal liability can be imposed on legal entities for conduct of certain natural persons of authority within the legal entity. Thus, the Convention requires that the conduct of such figures within an organisation is adequately monitored, also because the Convention states that a legal entity can be held liable for acts of omission in this regard. Furthermore, articles 16 and following of the Convention establish an early form of data retention requirements. Additionally, article 22 defines a series of criteria under which jurisdictional competence can be established. These include the competence of a jurisdiction when a criminal act is conducted by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State (art.22, 1, (d)). Thus, legal entities need to be aware of the applicable laws in any countries with which they have a formal link, even if they conduct no specific business there. It should be noted that these same obligations were also encapsulated in a number of E.U. initiatives, specifically the Framework decision commented directly above, and the Data Retention Directive, commented elsewhere in this text.

Additional Protocol to the Convention on cyber crime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems

Title:	Additional Protocol to the Convention on cyber crime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (28 January 2003)
Source reference:	http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm
Topic:	Amendment to the Convention on Cyber Crime, integrating provisions on racist and xenophobic expressions through computer systems. However, this protocol is only binding to the signatory states of the protocol itself, which does not include all signatory states to the main Convention (see http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=8&DF=2/20/2007&CL=ENG).
Scope	Convention which is binding to the signatory states (which does not include all E.U. Member States, unlike the Convention) after the entry into force of the convention, which occurred on 1 March 2006.
Direct/ indirect relevance	Indirect. The liability and jurisdiction principles of the text indirectly imply an obligation to assess one's risk with regard to the subject matter.
Legal force:	Requires signatory states to provide the necessary privacy protection provisions in their national regulatory frameworks.
Affected sectors:	Generic; the provisions can be relevant to any entity involved with information systems and data processing, in view of the topic of the normative text.
Relevant provision(s):	Chapter III – Relations between the Convention and this Protocol Article 8 – Relations between the Convention and this Protocol Articles 1, 12, 13, 22, 41, 44, 45 and 46 of the Convention shall apply, mutatis mutandis, to this Protocol. […]
Relevance to RM/RA	Due to article 8, the Convention's provisions on legal liability of legal entities and jurisdiction apply. As a result, legal liability can be imposed on legal entities for conduct in violation of the Protocol of certain natural persons of authority within the legal entity. Thus, the Convention requires that the conduct of such figures within an organisation is adequately monitored, also because the Convention states that a legal entity can be held liable for acts of omission in this regard. Additionally, article 22 defines a series of criteria under which jurisdictional competence can be established. These include the competence of a jurisdiction when a criminal act is conducted by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State (art.22, 1, (d)). Thus, legal entities need to be aware of the applicable racism and xenophobia laws in any countries with which they have a formal link, even if they conduct no specific business there.

Amendments to the Federal Rules of Civil Procedure with regard to electronic discovery

Title:	Amendments to the Federal Rules of Civil Procedure with regard to electronic discovery
Source reference:	http://www.law.cornell.edu/rules/frcp/
Topic:	U.S. Federal rules with regard to the production of electronic documents in civil proceedings
Scope	Relevant to any undertaking whose activities imply a risk of civil litigation before a U.S. court.
Direct/ indirect relevance	Indirect. The obligation to cooperate in discovery before a U.S. court implies that adequate measures must be taken to ensure that compliance with these requirements is possible.
Legal force:	U.S. Federal rules which apply to all civil proceedings before U.S. courts (regardless of the parties' place of establishment)
Affected sectors:	All sectors (any undertaking whose activities imply a risk of civil litigation before a U.S. court)
Relevant provision(s):	Rule 16. Pretrial Conferences; Scheduling; Management (a) Pretrial Conferences; Objectives. […] (b) Scheduling and Planning. Except in categories of actions exempted by district court rule as inappropriate, the district judge, or a magistrate judge when authorized by district court rule, shall, after receiving the report from the parties under Rule 26(f) or after consulting with the attorneys for the parties and any unrepresented parties by a scheduling conference, telephone, mail, or other suitable means, enter a scheduling order that limits the time (1) to join other parties and to amend the pleadings; (2) to file motions; and (3) to complete discovery. The scheduling order may also include (4) […] (5) provisions for disclosure or discovery of electronically stored information; […] Rule 34. Production of Documents and Things and Entry Upon Land for Inspection and Other Purposes (a) Scope. Any party may serve on any other party a request (1) to produce and permit the party making the request, or someone acting on the requestor's behalf, to inspect, copy, test, or sample any designated documents or electronically stored information — including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium from which information can be obtained — translated, if necessary, by the respondent into reasonably usable form, or to inspect, copy, test, or sample any designated tangible things which constitute or contain matters within the scope of Rule 26(b) and which are in the possession,

	custody or control of the party upon whom the request is served; or (2) to permit entry upon designated land or other property in the possession or control of the party upon whom the request is served for the purpose of inspection and measuring, surveying, photographing, testing, or sampling the property or any designated object or operation thereon, within the scope of Rule 26(b). (b) Procedure. The request shall set forth, either by individual item or by category, the items to be inspected, and describe each with reasonable particularity. The request shall specify a reasonable time, place, and manner of making the inspection and performing the related acts. The request may specify the form or forms in which electronically stored information is to be produced. Without leave of court or written stipulation, a request may not be served before the time specified in Rule 26(d). The party upon whom the request is served shall serve a written response within 30 days after the service of the request. A shorter or longer time may be directed by the court or, in the absence of such an order, agreed to in writing by the parties, subject to Rule 29. The response shall state, with respect to each item or category, that inspection and related activities will be permitted as requested, unless the request is objected to, including an objection to the requested form or forms for producing electronically stored information, stating the reasons for the objection. If objection is made to part of an item or category, the part shall be specified and inspection permitted of the remaining parts. If objection is made to the requested form or forms for producing electronically stored information — or if no form was specified in the request — the responding party must state the form or forms it intends to use. The party submitting the request may move for an order under Rule 37(a) with respect to any objection to or other failure to respond to the request or any part thereof, or any failure to permit inspection as requested. Unless the parties otherwise agree, or the court otherwise orders: (i) a party who produces documents for inspection shall produce them as they are kept in the usual course of business or shall organize and label them to correspond with the categories in the request; (ii) if a request does not specify the form or forms for producing electronically stored information, a responding party must produce the information in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable; and (iii) a party need not produce the same electronically stored information in more than one form. […]
Relevance to RM/RA	The discovery rules allow a party in civil proceedings to demand that the opposing party produce all relevant documentation (to be defined by the requesting party) in its possession, so as to allow the parties and the court to correctly assess the matter. Through the e-discovery amendment, which entered into force on 1 December 2006, such information may now include electronic information. This implies that any party being brought before a U.S. court in civil proceedings can be asked to produce such documents, which includes

	finalised reports, working documents, internal memos and e-mails with regard to a specific subject, which may or may not be specifically delineated. Any party whose activities imply a risk of being involved in such proceedings must therefore take adequate precautions for the management of such information, including the secure storage. Specifically: The party must be capable of initiating a 'litigation hold', a technical/organisational measure which must ensure that no relevant information can be modified any longer in any way. Storage policies must be responsible: while deletion of specific information of course remains allowed when this is a part of general information management policies ('routine, good-faith operation of the information system', Rule 37 (f)), the wilful destruction of potentially relevant information can be punished by extremely high fines (in one specific case of 1.6 billion US$). Thus, in practice, any businesses who risk civil litigation before U.S. courts must implement adequate information management policies, and must implement the necessary measures to initiate a litigation hold.

D. Corporate Governance and Operational Responsibility

OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security

Title:	OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (25 July 2002)
Source reference:	http://www.oecd.org/dataoecd/16/22/15582260.pdf
Topic:	General information security
Scope	Nonbinding guidelines to any OECD entities (governments, businesses, other organisations and individual users who develop, own, provide, manage, service, and use information systems and networks)
Direct/ indirect relevance	Direct. The text explicitly recommends RM/RA practices to be applied as a part of general security management.
Legal force:	Not legally binding, neither to natural persons, legal entities or countries
Affected sectors:	All sectors (since they contain general security principles for information systems)
Relevant provision(s):	III. PRINCIPLES The following nine principles are complementary and should be read as a whole. They concern participants at all levels, including policy and operational levels. Under these Guidelines, the responsibilities of participants vary according to their roles. All participants will be aided by awareness, education, information sharing and training that can lead to adoption of better security understanding and practices. Efforts to enhance the security of information systems and networks should be consistent with the values of a democratic society, particularly the need for an open and free flow of information and basic concerns for personal privacy. 1) Awareness Participants should be aware of the need for security of information systems and networks and what they can do to enhance security. Awareness of the risks and available safeguards is the first line of defence for the security of information systems and networks. Information systems and networks can be affected by both internal and external risks. Participants should understand that security failures may significantly harm systems and networks under their control. They should also be aware of the potential harm to others arising from interconnectivity and interdependency. Participants should be aware of the configuration of, and available updates for, their system, its place within networks, good practices that they can implement to enhance security, and the needs of other participants. 2) Responsibility All participants are responsible for the security of information systems and networks. Participants depend upon interconnected local and global information systems and networks and should understand their responsibility for the security of those information systems and networks. They should be accountable in a manner appropriate to their individual roles. Participants should review their own policies, practices, measures, and procedures regularly and assess whether these are appropriate to their environment. Those who develop, design and supply products and services should address system and network security and distribute

	appropriate information including updates in a timely manner so that users are better able to understand the security functionality of products and services and their responsibilities related to security. 3) Response Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents. Recognising the interconnectivity of information systems and networks and the potential for rapid and widespread damage, participants should act in a timely and co-operative manner to address security incidents. They should share information about threats and vulnerabilities, as appropriate, and implement procedures for rapid and effective co-operation to prevent, detect and respond to security incidents. Where permissible, this may involve cross-border information sharing and co-operation. 4) Ethics Participants should respect the legitimate interests of others. Given the pervasiveness of information systems and networks in our societies, participants need to recognise that their action or inaction may harm others. Ethical conduct is therefore crucial and participants should strive to develop and adopt best practices and to promote conduct that recognises security needs and respects the legitimate interests of others. 5) Democracy The security of information systems and networks should be compatible with essential values of a democratic society. Security should be implemented in a manner consistent with the values recognised by democratic societies including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency. 6) Risk assessment Participants should conduct risk assessments. Risk assessment identifies threats and vulnerabilities and should be sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications. Risk assessment will allow determination of the acceptable level of risk and assist the selection of appropriate controls to manage the risk of potential harm to information systems and networks in light of the nature and importance of the information to be protected. Because of the growing interconnectivity of information systems, risk assessment should include consideration of the potential harm that may originate from others or be caused to others. 7) Security design and implementation Participants should incorporate security as an essential element of information systems and networks. Systems, networks and policies need to be properly designed, implemented and co-ordinated to optimise security. A major, but not exclusive, focus of this effort is the design and adoption of appropriate safeguards and solutions to avoid or limit potential harm from identified threats and vulnerabilities. Both technical and non-technical safeguards and solutions are required and should be proportionate to the value of the information on the organisation's systems and networks. Security should be a fundamental

	element of all products, services, systems and networks, and an integral part of system design and architecture. For end users, security design and implementation consists largely of selecting and configuring products and services for their system. 8) Security management Participants should adopt a comprehensive approach to security management. Security management should be based on risk assessment and should be dynamic, encompassing all levels of participants' activities and all aspects of their operations. It should include forward-looking responses to emerging threats and address prevention, detection and response to incidents, systems recovery, ongoing maintenance, review and audit. Information system and network security policies, practices, measures and procedures should be co-ordinated and integrated to create a coherent system of security. The requirements of security management depend upon the level of involvement, the role of the participant, the risk involved and system requirements. 9) Reassessment Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures. New and changing threats and vulnerabilities are continuously discovered. Participants should continually review, reassess and modify all aspects of security to deal with these evolving risks.
Relevance to RM/RA	The OECD Guidelines state the basic principles underpinning risk management and information security practices. While no part of the text is binding as such, non-compliance with any of the principles is indicative of a serious breach of RM/RA good practices that can potentially incur liability.

Directive 2006/48/EC of 14 June 2006 relating to the taking up and pursuit of the business of credit institutions

Title:	Directive 2006/48/EC of the European Parliament and of the Council of 14 June 2006 relating to the taking up and pursuit of the business of credit institutions Note: this Directive is commonly referred to as the Capital Requirements Directive in conjunction with Directive 2006/49/EC of the European Parliament and of the Council of 14 June 2006 on the capital adequacy of investment firms and credit institutions (both of which were published simultaneously).
Source reference:	http://eur-lex.europa.eu/LexUriServ/site/en/oj/2006/l_177/l_17720060630en00010200.pdf
Topic:	Financial stability of credit institutions
Scope	Directly applicable to all EU Member States
Direct/ indirect relevance	Indirect. A large part of the text focuses on financial RM/RA practices, which implies an obligation to implement appropriate RM/RA measures with regard to network/information security.
Legal force:	EU Directive, requires transposition into national law
Affected sectors:	Credit institutions
Relevant provision(s):	A large part of the 200 page Directive is directly related to RM/RA for European credit institutions. Of specific interest is Title V of the Directive, related to principles and technical instruments for prudential supervision and disclosure. This Title covers five specific chapters, including: Principles of prudential supervision, including provisions with regard to professional secrecy and responsibility for the legal control of annual and consolidated accounts Technical instruments of prudential supervision, including an obligation to maintain provisions against risks and minimum own fund levels to cover credit risk and operational risk Credit institutions' assessment processes Supervision and disclosure by competent authorities Disclosure by credit institutions
Relevance to RM/RA	The scope of the provisions of the Directive reflects the supervisory rules introduced by Basel II, and provides a European perspective on requirements for the stability of credit institutions. In addition to the general subjects indicated above, the Annexes to the Directive contain more specific guidance on how the relevant risks should be managed, including through: Annex III – The treatment of counterparty credit risk of derivative instruments, repurchase transactions, securities or commodities lending or borrowing transactions, long settlement transactions and margin lending transactions Annex V – Technical criteria concerning the organisation and treatment of risks Annex VI – Standardised approach on risk weights Annex VII – Internal Ratings Based (IRB) approach Annex VIII – Credit Risk Mitigation Annex IX – Securisation Annex X – Operational Risk

Directive 2006/49/EC of 14 June 2006 on the capital adequacy of investment firms and credit institutions

Title:	Directive 2006/49/EC of the European Parliament and of the Council of 14 June 2006 on the capital adequacy of investment firms and credit institutions Note: this Directive is commonly referred to as the Capital Requirements Directive in conjunction with Directive 2006/48/EC of the European Parliament and of the Council of 14 June 2006 relating to the taking up and pursuit of the business of credit institutions (both of which were published simultaneously).
Source reference:	http://eur-lex.europa.eu/LexUriServ/site/en/oj/2006/l_177/l_17720060630en02010255.pdf
Topic:	Financial stability through capital adequacy of investment firms and credit institutions
Scope	Directly applicable to all EU Member States
Direct/ indirect relevance	Indirect. A large part of the text focuses on financial RM/RA practices, which implies an obligation to implement appropriate RM/RA measures with regard to network/information security.
Legal force:	EU Directive, requires transposition into national law
Affected sectors:	Investment firms and credit institutions
Relevant provision(s):	A large part of the 55 page Directive is directly related to RM/RA for European investment firms and credit institutions. Of specific interest is Chapter V of the Directive, which includes provisions with regard to minimum fund requirements and valid methods for their calculation, for credit institutions and for investment firms. Additionally, it details requirements on how the provisions of Directive 2006/48/EC apply to these organisations.
Relevance to RM/RA	The scope of the provisions of the Directive reflects the supervisory rules introduced by Basel II, and provides a European perspective on requirements for the stability through capital adequacy of investment firms and credit institutions. In addition to the general subjects indicated above, the Annexes to the Directive contain more specific guidance on how the relevant risks should be managed, including through: Annex I – Calculating capital requirements for position risk Annex II – Calculating capital requirements for settlement and counterparty credit risk Annex III – Calculating capital requirements for foreign-exchange risk Annex IV – Calculating capital requirements for commodities risk Annex V – Use of internal models to calculate capital requirements Annex VI – Calculating capital requirements for large exposures Annex VII – Trading activity

Directive 2000/46/EC of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions

Title:	Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions
Source reference:	http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_275/l_27520001027en00390043.pdf
Topic:	Supervision and stability of electronic money institutions
Scope	Directly applicable to all EU Member States
Direct/ indirect relevance	Indirect. A large part of the text focuses on financial RM/RA practices, which implies an obligation to implement appropriate RM/RA measures with regard to network/information security.
Legal force:	EU Directive, requires transposition into national law
Affected sectors:	Providers of electronic money solutions (i.e. monetary value used as a substitute for currency which is stored on an electronic carrier such as a chip card or computer memory)
Relevant provision(s):	Article 4 - Initial capital and ongoing own funds requirements 1. Electronic money institutions shall have an initial capital, as defined in Article 34(2), subparagraphs (1) and (2) of Directive 2000/12/EC, of not less than EUR 1 million. Notwithstanding paragraphs 2 and 3, their own funds, as defined in Directive 2000/12/EC, shall not fall below that amount. 2. Electronic money institutions shall have at all times own funds which are equal to or above 2 % of the higher of the current amount or the average of the preceding six months' total amount of their financial liabilities related to outstanding electronic money. 3. Where an electronic money institution has not completed a six months' period of business, including the day it starts up, it shall have own funds which are equal to or above 2 % of the higher of the current amount or the six months' target total amount of its financial liabilities related to outstanding electronic money. The six months' target total amount of the institution's financial liabilities related to outstanding electronic money shall be evidenced by its business plan subject to any adjustment to that plan having been required by the competent authorities. Article 5 - Limitations of investments 1. Electronic money institutions shall have investments of an amount of no less than their financial liabilities related to outstanding electronic money in the following assets only: [...] Article 6 - Verification of specific requirements by the competent authorities The competent authorities shall ensure that the calculations justifying compliance with Articles 4 and 5 are made, not less than twice each year, either by electronic money institutions themselves, which shall communicate them, and any component data required, to the competent authorities, or by competent authorities, using data supplied by the electronic money institutions.

	Article 7 - Sound and prudent operation Electronic money institutions shall have sound and prudent management, administrative and accounting procedures and adequate internal control mechanisms. These should respond to the financial and non-financial risks to which the institution is exposed including technical and procedural risks as well as risks connected to its cooperation with any undertaking performing operational or other ancillary functions related to its business activities.
Relevance to RM/RA	The provisions of the Directive imply certain basic RM/RA obligations for service providers in the electronic money market, including: Initial capital and investment limitation requirements, aiming to ensure their financial stability; Related to this, an obligation to maintain sufficient documentation to be able to demonstrate compliance with these obligations to the competent national authorities upon audit; A high level corporate governance requirement to implement 'sound and prudent management, administrative and accounting procedures and adequate internal control mechanisms' to cover general operational risks. However, the Directive offers little guidance on how this requirement should be met.

Risk Management Principles for Electronic Banking, July 2003

Title:	Basel Committee on Banking Supervision – Risk Management Principles for Electronic Banking *Note: an earlier version of this document was released in May 2001, but has since been superseded.*
Source reference:	http://www.bis.org/publ/bcbs98.pdf *(For the superseded version of May 2001: see http://www.bis.org/publ/bcbs82.pdf)*
Topic:	Risk Management principles issued by the Basel Committee, specifically with regard to e-banking applications being offered.
Scope	The document is a statement of principles from the Basel Committee, whose members hail from Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, the Netherlands, Spain, Sweden, Switzerland, the United Kingdom and the United States. However, the Committee has no formal authority (not even to banking institutions within these countries), and its decisions are not legally binding.
Direct/ indirect relevance	Direct. The text focuses on financial RM/RA practices, with a specific emphasis on the resulting obligations with regard to information/network security.
Legal force:	Not legally binding, but considered highly authoritative
Affected sectors:	e-Banking sector
Relevant provision(s):	The document is relevant in its entirety, and states a number of guiding principles on how general rules of RM/RA (as already formulated and applied by banks) apply to e-banking. It calls upon the banks' management to ensure that the principles are observed in practice. The document states fourteen high level RM/RA principles, but does not define specific rules, technologies or standards, to ensure that the principles can be applied throughout the sector, regardless of an institute's risk profile. The principles are divided into three broad categories: Board and Management Oversight; Security Controls; and Legal and Reputational Risk Management: *"Board and Management Oversight* *Because the Board of Directors and senior management are responsible for developing the institution's business strategy and establishing an effective management oversight over risks, they are expected to take an explicit, informed and documented strategic decision as to whether and how the bank is to provide e-banking services. The initial decision should include the specific accountabilities, policies and controls to address risks, including those arising in a cross-border context. Effective management oversight is expected to encompass the review and approval of the key aspects of the bank's security control process, such as the development and maintenance of a security control infrastructure that properly safeguards e-banking systems and data from both internal and external threats. It also should include a comprehensive process for managing risks associated with increased complexity of and increasing reliance on outsourcing relationships and third-party dependencies to perform critical e-banking functions.* *Security Controls*

	While the Board of Directors has the responsibility for ensuring that appropriate security control processes are in place for e-banking, the substance of these processes needs special management attention because of the enhanced security challenges posed by e-banking. This should include establishing appropriate authorisation privileges and authentication measures, logical and physical access controls, adequate infrastructure security to maintain appropriate boundaries and restrictions on both internal and external user activities and data integrity of transactions, records and information. In addition, the existence of clear audit trails for all e-banking transactions should be ensured and measures to preserve confidentiality of key e-banking information should be appropriate with the sensitivity of such information. *Although customer protection and privacy regulations vary from jurisdiction to jurisdiction, banks generally have a clear responsibility to provide their customers with a level of comfort regarding information disclosures, protection of customer data and business availability that approaches the level they can expect when using traditional banking distribution channels. To minimise legal and reputational risk associated with e-banking activities conducted both domestically and cross-border, banks should make adequate disclosure of information on their web sites and take appropriate measures to ensure adherence to customer privacy requirements applicable in the jurisdictions to which the bank is providing e-banking services.* *Legal and Reputational Risk Management* *To protect banks against business, legal and reputation risk, e-banking services must be delivered on a consistent and timely basis in accordance with high customer expectations for constant and rapid availability and potentially high transaction demand. The bank must have the ability to deliver e-banking services to all end-users and be able to maintain such availability in all circumstances. Effective incident response mechanisms are also critical to minimise operational, legal and reputational risks arising from unexpected events, including internal and external attacks, that may affect the provision of e-banking systems and services. To meet customers' expectations, banks should therefore have effective capacity, business continuity and contingency planning. Banks should also develop appropriate incident response plans, including communication strategies, that ensure business continuity, control reputation risk and limit liability associated with disruptions in their e-banking services."* (Source: see http://www.bis.org/publ/bcbs98.htm)
Relevance to RM/RA	The document is not legally binding as such. However, due to its authoritative source, public renown and general applicability, failure to pay sufficient attention to any of the fourteen principles or to any of the three categories should be considered indicative of serious negligence in RM/RA practices.

Basel II

Title:	Basel Committee on Banking Supervision – Revised international capital framework for monetary and financial stability *Note: the most recent version is dated June 2006, following earlier versions of November 2005 and June 2004. The initial version (the so called Basel I) is largely considered superseded.*
Source reference:	http://www.bis.org/publ/bcbs128.htm
Topic:	Financial risk and minimal capital requirements, as issued by the Basel Committee with regard to banking activities.
Scope	The document is a statement of requirements to be met for banking institutions in order to sufficiently ensure their financial stability from the Basel Committee, whose members hail from Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, the Netherlands, Spain, Sweden, Switzerland, the United Kingdom and the United States. While the Committee has no formal authority, Basel I was adopted through legislation in the G-10 countries (Belgium, Canada, France, Germany, Italy, Japan, the Netherlands, Sweden, the United Kingdom, and the United States), and its principles were directly or indirectly subscribed to in a multitude of other countries' legislations. Basel II is not yet as widely adopted; its legal binding force therefore varies from country to country.
Direct/ indirect relevance	Indirect. A large part of the text focuses on financial RM/RA practices, which implies an obligation to implement appropriate RM/RA measures with regard to network/information security.
Legal force:	Not universally legally binding, but always considered highly authoritative
Affected sectors:	Banking institutions.
Relevant provision(s):	The document is relevant in its entirety to internationally active banking institutions, and prescribes a number of requirements for such institutions in three basic pillars: Minimum Capital Requirements (covering credit risk, operational risk and market risk), Supervisory Review Processes (covering reputation risk, liquidity risk and legal risk, under the joint title 'residual risk'), and Market Discipline (including disclosure of risk position). (See also http://www.bis.org/publ/bcbs107.htm)
Relevance to RM/RA	Assessing the relevance of Basel II is complicated, since it is partially dependant on whether or not local governments have adopted it into their local regulations (or if Basel I has), and how this adoption has occurred. At any rate, Basel II is considered to be highly authoritative as a yardstick for measuring the RM/RA practices of banking institutions in ensuring their financial stability, even without considering legal imperatives to adhere to its provisions. Specifically, Basel II is considered by the Basel Committee to be instrumental in assessments of risk provided by banks' internal systems as inputs to capital calculations.

Commission Recommendation 87/598/EEC concerning a European code of conduct relating to electronic payments

Title:	Commission Recommendation 87/598/EEC of 8 December 1987, concerning a European code of conduct relating to electronic payments *Note: this recommendation was further elaborated in Recommendation 97/489/EC, with regard to the relationship between issuer and holder; see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997H0489:EN:HTML .*
Source reference:	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31987H0598:EN:HTML
Topic:	Good practices for electronic payment systems (carried out by means of a card incorporating a magnetic strip or microcircuit used at an electronic payment terminal (EPT) or point-of-sale (POS) terminal)
Scope	Nonbinding recommendation to issuers of electronic payment solutions, specifically card issuers
Direct/ indirect relevance	Direct. The text focuses on electronic payments, and includes specific provisions on data protection and information security.
Legal force:	Not legally binding, neither to natural persons, legal entities or countries
Affected sectors:	Providers of electronic payment solutions, specifically card issuers
Relevant provision(s):	4. Data protection and security (a) Electronic payments are irreversible. An order given by means of a payment card shall be irrevocable and may not be countermanded. (b) The information transmitted, at the time of payment, to the trader's bank and subsequently to the issuer must not in any circumstances prejudice the protection of privacy. It shall be strictly limited to that normally laid down for cheques and transfers. (c) Any problems whatsoever that arise in connection with the protection of information or with security must be openly acknowledged and cleared up at whatever stage in the contract between the parties. (d) Contracts must not restrict trader's freedom of operation or freedom to compete. […] IV. SUPPLEMENTARY PROVISIONS […] 2. Relations between issuers and consumers Cardholders shall take all reasonable precautions to ensure the safety of the card issued and shall observe the special conditions (loss or theft) in the contract which they have signed. […]
Relevance to RM/RA	The document provides a number of general non-binding recommendations, including an obligation to ensure that privacy is respected and that the system is transparent with regard to potential security or confidentiality risks, which must obviously be mitigated by all reasonable means. The abstract and generic character of the recommendations (many of

	which have been further developed in more specific norms, e.g. the Privacy Directive) imply that they are of relative use in assessing the validity of existing RM/RA practices. None the less, it is one of the few norms which contain a clear obligation to inform users of any security and/or confidentiality risks.

U.S. Sarbanes-Oxley Act of 2002

Title:	Public Company Accounting Reform and Investor Protection Act of 30 July 2002 (commonly referred to as 'Sarbanes-Oxley' after the bill's sponsors, Senator Paul Sarbanes (D-Md.) and Representative Michael G. Oxley (R-Oh.); and commonly abbreviated to 'SOX' or 'Sarbox')
Source reference:	http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.tst.pdf
Topic:	U.S. Federal legislation with regard to corporate governance, auditing requirements, public disclosure, financial management and general reporting obligations for U.S. public enterprises.
Scope	Applicable only to U.S. public enterprises, the latter being understood as any company which offers its securities (i.e., stock, options, bonds, etc.) for sale to the general public in the U.S., or from a formal perspective, a company which has filed a Form S-1 with the Securities and Exchange Commission (SEC - http://www.sec.gov/) and raises money from the public on the U.S. markets.
Direct/ indirect relevance	Indirect. The text focuses on corporate governance, including auditing, disclosure and reporting, which implies an obligation to implement appropriate RM/RA measures with regard to network/information security.
Legal force:	U.S. Federal legislation, which applies directly to any public companies in the U.S. as described above.
Affected sectors:	Any public companies in the U.S. as described above.
Relevant provision(s):	In the field of RM/RA, the main provisions are generally considered to be Sections 302 and 404. SEC. 302. CORPORATE RESPONSIBILITY FOR FINANCIAL REPORTS. (a) REGULATIONS REQUIRED.—The Commission shall, by rule, require, for each company filing periodic reports under section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m, 78o(d)), that the principal executive officer or officers and the principal financial officer or officers, or persons performing similar functions, certify in each annual or quarterly report filed or submitted under either such section of such Act that— (1) the signing officer has reviewed the report; (2) based on the officer's knowledge, the report does not contain any untrue statement of a material fact or omit to state a material fact necessary in order to make the statements made, in light of the circumstances under which such statements were made, not misleading; (3) based on such officer's knowledge, the financial statements, and other financial information included in the report, fairly present in all material respects the financial condition and results of operations of the issuer as of, and for, the periods presented in the report; (4) the signing officers— (A) are responsible for establishing and maintaining internal controls; (B) have designed such internal controls to ensure that material information relating to the issuer and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared; (C) have evaluated the effectiveness of the issuer's internal controls as of a date within 90 days prior to the report; and (D) have presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation as of that date;

	(5) the signing officers have disclosed to the issuer's auditors and the audit committee of the board of directors (or persons fulfilling the equivalent function)— (A) all significant deficiencies in the design or operation of internal controls which could adversely affect the issuer's ability to record, process, summarize, and report financial data and have identified for the issuer's auditors any material weaknesses in internal controls; and (B) any fraud, whether or not material, that involves management or other employees who have a significant role in the issuer's internal controls; and (6) the signing officers have indicated in the report whether or not there were significant changes in internal controls or in other factors that could significantly affect internal controls subsequent to the date of their evaluation, including any corrective actions with regard to significant deficiencies and material weaknesses. (b) FOREIGN REINCORPORATIONS HAVE NO EFFECT.—Nothing in this section 302 shall be interpreted or applied in any way to allow any issuer to lessen the legal force of the statement required under this section 302, by an issuer having reincorporated or having engaged in any other transaction that resulted in the transfer of the corporate domicile or offices of the issuer from inside the United States to outside of the United States. (c) DEADLINE.—The rules required by subsection (a) shall be effective not later than 30 days after the date of enactment of this Act. SEC. 404. MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS. (a) RULES REQUIRED.—The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall— (1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and (2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting. (b) INTERNAL CONTROL EVALUATION AND REPORTING.—With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.
Relevance to RM/RA	Specific accounting standards for public accounting firms are created and supervised by the Public Company Accounting Oversight Board (http://www.pcaobus.org/), established by Sarbanes-Oxley. Apart from increased penalties for corporate fraud cases, Sarbanes-Oxley is specifically relevant because of its introduction of a set of obligations for the targeted public companies, including: A requirement that they evaluate and disclose the effectiveness of their internal controls with regard to financial reporting. Independent auditors are required to attest to the validity of this disclosure (Section 302); A requirement to have certain financial reports certified by chief executive officers and chief financial officers (Section 404); Affected companies must install the appropriate procedures and take

	appropriate measures to ensure compliance with these requirements. As indicated above, this includes all companies which offer their securities (i.e., stock, options, bonds, etc.) for sale to the general public in the U.S. Thus, the scope of Sarbanes-Oxley can include non-U.S. established companies. See also http://thecaq.aicpa.org/Resources/Sarbanes+Oxley/Summary+of+the+Provisions+of+the+Sarbanes-Oxley+Act+of+2002.htm

OCC Electronic Banking Guidance

Title:	Office of the Comptroller of the Currency (OCC) – Electronic Banking Guidance
Source reference:	http://www.occ.treas.gov/netbank/ebguide.htm *Note: the OCC Electronic Banking Guidance covers a variety of documents of varying relevance to this study. This profile will summarise only the key tenets of these documents.*
Topic:	Good practices disseminated by the U.S. Office of the Comptroller of the Currency (OCC) on a variety of documents in connection with electronic banking.
Scope	The documents contain a number of recommendations and good practices with regard to common risks for e-banking services. The guidance is specifically targeted towards U.S. banking institutions, given the OCC's status as a bureau of the U.S. Department of the Treasury (albeit with an office in London to supervise the international activities of these U.S. banks).
Direct/ indirect relevance	Direct. The text focuses on financial RM/RA practices in electronic banking, including a variety of subjects with regard to network/information security.
Legal force:	Not legally binding to non-U.S. banks
Affected sectors:	Electronic banking institutions.
Relevant provision(s):	The OCC Electronic Banking Guidance covers a variety of documents of varying relevance to this study, all of which can be accessed through http://www.occ.treas.gov/netbank/ebguide.htm. Covered topics include: On-line identity theft, phishing mails and spoofed web sites Software licensing policies (specifically the use of free and open source (FOSS) software Customer authentication Electronic record keeping Wireless networking Web linking Third party service providers Privacy and safeguarding customer information Technology risk management
Relevance to RM/RA	The OCC acts as a supervisory authority to U.S. banks, but has no legal authority over European institution. None the less, given the global character of financial services, compliance with OCC Guidance documents is recommended. It should be noted that most of the OCC Guidance documents are fairly high level, and should be indicative of the subject matter to be analysed and assessed by banking institutions, rather than serving as a yardstick to identify actual problems.

PCI DSS

Title:	Payment Card Industry (PCI) Security Standards Council – Data Security Standard
Source reference:	https://www.pcisecuritystandards.org/tech/download_the_pci_dss.htm
Topic:	Requirements for the management of data security of payment accounts
Scope	The document contains a number of requirements aiming to improve data security of payment accounts. It was drafted and maintained by the PCI Security Standards Council, whose members include American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International.
Direct/ indirect relevance	Direct. While a private sector initiative, the text directly deals with information security in the financial sector.
Legal force:	Not legally binding
Affected sectors:	Members of the payment card industry and related service providers
Relevant provision(s):	PCI DSS contains high level requirements for security management, including policies, procedural recommendations, architectural recommendations, software design and other critical protective measures. The content of PCI DSS is summarily described as follows: *"The core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the DSS are organized:* *Build and Maintain a Secure Network* *Requirement 1: Install and maintain a firewall configuration to protect cardholder data* *Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters* *Protect Cardholder Data* *Requirement 3: Protect stored cardholder data* *Requirement 4: Encrypt transmission of cardholder data across open, public networks* *Maintain a Vulnerability Management Program* *Requirement 5: Use and regularly update anti-virus software* *Requirement 6: Develop and maintain secure systems and applications* *Implement Strong Access Control Measures* *Requirement 7: Restrict access to cardholder data by business need-to-know* *Requirement 8: Assign a unique ID to each person with computer access* *Requirement 9: Restrict physical access to cardholder data* *Regularly Monitor and Test Networks*

	Requirement 10: Track and monitor all access to network resources and cardholder data *Requirement 11: Regularly test security systems and processes* *Maintain an Information Security Policy* *Requirement 12: Maintain a policy that addresses information security"* (Source: https://www.pcisecuritystandards.org/tech/index.htm)
Relevance to RM/RA	The main purpose of PCI DSS was to provide central guidance allowing financial service providers relying on payment cards to implement the necessary policies, procedures and infrastructure to adequately safeguard their customer account data. Thus, the document is one of the major RM/RA resources in the payment card industry. PCI DSS has no formal binding legal power. None the less, considering its origins and the key participants, it holds significant moral authority, and non-compliance with the PCI DSS by a payment card service provider may be indicative of inadequate RM/RA practices.

GAAP and IFRS/IAS

Title:	Generally Accepted Accounting Principles, as elaborated by the U.S. Federal Accounting Standards Advisory Board (FASAB); and International Financial Reporting Standards, as elaborated by the International Accounting Standards Committee (IASC) *Note: before 2001, standards from the IASC were called 'International Accounting Standards' (IAS), rather than IFRS. However, IASes remain relevant until/unless replaced by an IFRS.*
Source reference:	http://www.fasab.gov/accepted.html and http://www.iasb.org/Summaries+of+International+Financial+Reporting+Standards/Technical+Summaries+of+International+Financial+Reporting+Standards.htm, respectively.
Topic:	Both are sets of standards related to good accounting practices (which are also generically referred to as Generally Accepted Accounting Practices, without specifically meaning the U.S. version), the first being issued by a U.S. institute (but with international following), and the second being international from the onset.
Scope	Sets of practices to be observed by accountants affected by them.
Direct/ indirect relevance	Indirect. The observance of accounting standards implies an obligation to implement appropriate RM/RA measures with regard to network/information security.
Legal force:	Legal force depends from country to country. In some countries GAAPs (in a generic sense) are not emphatically included in their legislation, although supervisory authorities may require that they be followed e.g. for publicly traded companies. In the E.U., adherence with the IFRS is mandatory for publicly traded companies since 2005, at least for IASC standards which have been adopted by the Commission following the opinion from the Accounting Regulatory Committee (ARC – see http://ec.europa.eu/internal_market/accounting/committees_en.htm#arc); see also http://www.iasplus.com/country/useias.htm
Affected sectors:	Any organisation or enterprise legally required to keep accounting documents.
Relevant provision(s):	Given that the entire purpose of GAAPs (in a generic sense) is to prescribe the accounting practices to be observed, all standards within a GAAP are relevant for the evaluation of an undertaking's RM/RA policies. IFRS/IAS presently cover the following topics: IFRSs: IFRS 1 First-time Adoption of International Financial Reporting Standards IFRS 2 Share-based Payment IFRS 3 Business Combinations IFRS 4 Insurance Contracts IFRS 5 Non-current Assets Held for Sale and Discontinued Operations IFRS 6 Exploration for and evaluation of Mineral Resources IFRS 7 Financial Instruments: Disclosures IFRS 8 Operating Segments IASs: IAS 1 Presentation of Financial Statements IAS 2 Inventories

	IAS 7 Cash Flow Statements IAS 8 Accounting Policies, Changes in Accounting Estimates and Errors IAS 10 Events After the Balance Sheet Date IAS 11 Construction Contracts IAS 12 Income Taxes IAS 16 Property, Plant and Equipment IAS 17 Leases IAS 18 Revenue IAS 19 Employee Benefits IAS 20 Accounting for Government Grants and Disclosure of Government Assistance IAS 21 The Effects of Changes in Foreign Exchange Rates IAS 23 Borrowing Costs IAS 24 Related Party Disclosures IAS 26 Accounting and Reporting by Retirement Benefit Plans IAS 27 Consolidated and Separate Financial Statements IAS 28 Investments in Associates IAS 29 Financial Reporting in Hyperinflationary Economies IAS 31 Interests in Joint Ventures IAS 32 Financial Instruments: Presentation IAS 33 Earnings per Share IAS 34 Interim Financial Reporting IAS 36 Impairment of Assets IAS 37 Provisions, Contingent Liabilities and Contingent Assets IAS 38 Intangible Assets IAS 39 Financial Instruments: Recognition and Measurement IAS 40 Investment Property IAS 41 Agriculture (Source: http://www.iasb.org/Summaries+of+International+Financial+Reporting+Standards/IFRS+and+IAS+Summaries+-+English/IFRS+and+IAS+Summaries-+English.htm)
Relevance to RM/RA	Depending on their legal force, GAAPs (in a generic sense) either require or recommend companies to respect certain standards and interpretations with regard to their accounting practices. Companies are therefore required/recommended (depending on the legal framework) to assess whether or not their existing practices are in full compliance with whatever GAAP are applicable to their business processes.

Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services (Framework Directive)

Title:	Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)
Source reference:	http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_108/l_10820020424en00330050.pdf
Topic:	General framework for the regulation of electronic communications services, electronic communications networks, associated facilities and associated services.
Scope	Directly applicable to all EU Member States
Direct/ indirect relevance	Indirect. The text contains certain transparency and governance requirements which imply an obligation to implement appropriate RM/RA measures with regard to network/information security.
Legal force:	EU Directive, requires transposition into national law
Affected sectors:	Providers of electronic communications services, electronic communications networks, associated facilities and associated services in the Community
Relevant provision(s):	Article 5 - Provision of information 1. Member States shall ensure that undertakings providing electronic communications networks and services provide all the information, including financial information, necessary for national regulatory authorities to ensure conformity with the provisions of, or decisions made in accordance with, this Directive and the Specific Directives. These undertakings shall provide such information promptly on request and to the timescales and level of detail required by the national regulatory authority. The information requested by the national regulatory authority shall be proportionate to the performance of that task. The national regulatory authority shall give the reasons justifying its request for information. […] Article 13 - Accounting separation and financial reports 1. Member States shall require undertakings providing public communications networks or publicly available electronic communications services which have special or exclusive rights for the provision of services in other sectors in the same or another Member State to: (a) keep separate accounts for the activities associated with the provision of electronic communications networks or services, to the extent that would be required if these activities were carried out by legally independent companies, so as to identify all elements of cost and revenue, with the basis of their calculation and the detailed attribution methods used, related to their activities associated with the provision of electronic communications networks or services including an itemised breakdown of fixed asset and structural costs, or (b) have structural separation for the activities associated with the provision of electronic communications networks or services. Member States may choose not to apply the requirements referred to in the first subparagraph to undertakings the annual turnover of which in activities associated with electronic communications networks or

	services in the Member States is less than EUR 50 million. 2. Where undertakings providing public communications networks or publicly available electronic communications services are not subject to the requirements of company law and do not satisfy the small and medium-sized enterprise criteria of Community law accounting rules, their financial reports shall be drawn up and submitted to independent audit and published. The audit shall be carried out in accordance with the relevant Community and national rules. This requirement shall also apply to the separate accounts required under paragraph 1(a).
Relevance to RM/RA	The cited articles impose certain information management obligations on the providers of public communications networks or publicly available electronic communications services. Specifically, they should: Ensure that they collect and retain the required information to demonstrate their compliance with applicable regulations, including financial information. Given that this information must be provided within a reasonable timeframe and to the extent required by the request, this implies the implementation of suitable RM/RA practices to ensure that such data can be reliably managed and made available within a (relatively) short timeframe. Ensure that their accounting practices conform to the standards of good corporate governance, including by separating their accounting activities according to the distinct activities undertaken by the service provider, so that their financial information can be evaluated as if a distinct service provider were providing the relevant service.

Directive 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive)

Title:	Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive)
Source reference:	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0019:EN:HTML
Topic:	General framework for the regulation of access to, and interconnection of, electronic communications networks and associated facilities.
Scope	Directly applicable to all EU Member States
Direct/ indirect relevance	Indirect. The text contains certain transparency and governance requirements which imply an obligation to implement appropriate RM/RA measures with regard to network/information security.
Legal force:	EU Directive, requires transposition into national law
Affected sectors:	Providers of electronic communications services, electronic communications networks, associated facilities and associated services in the Community
Relevant provision(s):	Article 9 - Obligation of transparency 1. National regulatory authorities may, in accordance with the provisions of Article 8, impose obligations for transparency in relation to interconnection and/or access, requiring operators to make public specified information, such as accounting information, technical specifications, network characteristics, terms and conditions for supply and use, and prices. 2. In particular where an operator has obligations of non-discrimination, national regulatory authorities may require that operator to publish a reference offer, which shall be sufficiently unbundled to ensure that undertakings are not required to pay for facilities which are not necessary for the service requested, giving a description of the relevant offerings broken down into components according to market needs, and the associated terms and conditions including prices. The national regulatory authority shall, inter alia, be able to impose changes to reference offers to give effect to obligations imposed under this Directive. 3. National regulatory authorities may specify the precise information to be made available, the level of detail required and the manner of publication. […] Article 10 – Obligation of non-discrimination 1. A national regulatory authority may, in accordance with the provisions of Article 8, impose obligations of non-discrimination, in relation to interconnection and/or access. 2. Obligations of non-discrimination shall ensure, in particular, that the operator applies equivalent conditions in equivalent circumstances to other undertakings providing equivalent services, and provides services and information to others under the same conditions and of the same quality as it provides for its own services, or those of it subsidiaries or partners.

	Article 11 – Obligation of accounting separation 1. A national regulatory authority may, in accordance with the provisions of Article 8, impose obligations for accounting separation in relation to specified activities related to interconnection and/or access. In particular, a national regulatory authority may require a vertically integrated company to make transparent its wholesale prices and its internal transfer prices inter alia to ensure compliance where there is a requirement for non-discrimination under Article 10 or, where necessary, to prevent unfair cross-subsidy. National regulatory authorities may specify the format and accounting methodology to be used. 2. Without prejudice to Article 5 of Directive 2002/21/EC (Framework Directive), to facilitate the verification of compliance with obligations of transparency and non-discrimination, national regulatory authorities shall have the power to require that accounting records, including data on revenues received from third parties, are provided on request. National regulatory authorities may publish such information as would contribute to an open and competitive market, while respecting national and Community rules on commercial confidentiality. Article 12 - Obligations of access to, and use of, specific network facilities 1. A national regulatory authority may, in accordance with the provisions of Article 8, impose obligations on operators to meet reasonable requests for access to, and use of, specific network elements and associated facilities, inter alia in situations where the national regulatory authority considers that denial of access or unreasonable terms and conditions having a similar effect would hinder the emergence of a sustainable competitive market at the retail level, or would not be in the end-user's interest. Operators may be required inter alia: (a) to give third parties access to specified network elements and/or facilities, including unbundled access to the local loop; (b) to negotiate in good faith with undertakings requesting access; (c) not to withdraw access to facilities already granted; (d) to provide specified services on a wholesale basis for resale by third parties; (e) to grant open access to technical interfaces, protocols or other key technologies that are indispensable for the interoperability of services or virtual network services; (f) to provide co-location or other forms of facility sharing, including duct, building or mast sharing; (g) to provide specified services needed to ensure interoperability of end-to-end services to users, including facilities for intelligent network services or roaming on mobile networks; (h) to provide access to operational support systems or similar software

	systems necessary to ensure fair competition in the provision of services; (i) to interconnect networks or network facilities. National regulatory authorities may attach to those obligations conditions covering fairness, reasonableness and timeliness. […] Article 13 – Price control and cost accounting obligations 1. A national regulatory authority may, in accordance with the provisions of Article 8, impose obligations relating to cost recovery and price controls, including obligations for cost orientation of prices and obligations concerning cost accounting systems, for the provision of specific types of interconnection and/or access, in situations where a market analysis indicates that a lack of effective competition means that the operator concerned might sustain prices at an excessively high level, or apply a price squeeze, to the detriment of end-users. National regulatory authorities shall take into account the investment made by the operator and allow him a reasonable rate of return on adequate capital employed, taking into account the risks involved. […]
Relevance to RM/RA	The cited articles impose certain information management obligations on the providers of public communications networks or publicly available electronic communications services in order to ensure the accessibility and interconnectivity of the underlying infrastructure in compliance with European free movement of service principles. Specifically, they should: Ensure that sufficient transparency is provided, e.g. by making publicly available the requirements for connectivity to their infrastructure in accordance with applicable national regulations; Ensure that the principle of non-discrimination is observed with regard to access or connectivity, by ensuring that equivalent conditions apply in equivalent circumstances; Verify whether they are obliged to maintain separate accounting systems under applicable law for their activities with regard to ensuring compliance with their access/interconnectivity obligations; Verify whether they are obliged to open (part of) their infrastructure to third parties under applicable law, and if so under what conditions; Verify whether they are subject to cost recovery and price controls schemes to comply with access/interconnectivity obligations under applicable law, and if so under what conditions; From an RM/RA perspective, the obligations above imply that the affected providers must assess their policies and practices to ensure that they can comply with these obligations.

Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive)

Title:	Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive)
Source reference:	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0022:EN:HTML
Topic:	General framework for the regulation of the provision of electronic communications networks and services to end-users, and specifically with a view of ensuring good quality publicly available services
Scope	Directly applicable to all EU Member States
Direct/ indirect relevance	Indirect. The text contains certain quality and governance requirements which imply an obligation to implement appropriate RM/RA measures with regard to network/information security.
Legal force:	EU Directive, requires transposition into national law
Affected sectors:	Providers of electronic communications services, electronic communications networks, associated facilities and associated services in the Community
Relevant provision(s):	Article 11 - Quality of service of designated undertakings 1. National regulatory authorities shall ensure that all designated undertakings with obligations under Articles 4, 5, 6, 7 and 9(2) publish adequate and up-to-date information concerning their performance in the provision of universal service, based on the quality of service parameters, definitions and measurement methods set out in Annex III. The published information shall also be supplied to the national regulatory authority. 2. National regulatory authorities may specify, inter alia, additional quality of service standards, where relevant parameters have been developed, to assess the performance of undertakings in the provision of services to disabled end-users and disabled consumers. National regulatory authorities shall ensure that information concerning the performance of undertakings in relation to these parameters is also published and made available to the national regulatory authority. 3. National regulatory authorities may, in addition, specify the content, form and manner of information to be published, in order to ensure that end-users and consumers have access to comprehensive, comparable and user-friendly information. 4. National regulatory authorities shall be able to set performance targets for those undertakings with universal service obligations at least under Article 4. In so doing, national regulatory authorities shall take account of views of interested parties, in particular as referred to in Article 33. 5. Member States shall ensure that national regulatory authorities are able to monitor compliance with these performance targets by designated undertakings. 6. Persistent failure by an undertaking to meet performance targets may result in specific measures being taken in accordance with Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications

	networks and services (Authorisation Directive)(13). National regulatory authorities shall be able to order independent audits or similar reviews of the performance data, paid for by the undertaking concerned, in order to ensure the accuracy and comparability of the data made available by undertakings with universal service obligations. Article 13 – Financing of universal service obligations 1. Where, on the basis of the net cost calculation referred to in Article 12, national regulatory authorities find that an undertaking is subject to an unfair burden, Member States shall, upon request from a designated undertaking, decide: (a) to introduce a mechanism to compensate that undertaking for the determined net costs under transparent conditions from public funds; and/or (b) to share the net cost of universal service obligations between providers of electronic communications networks and services. […] Article 21 – Transparency and publication of information 1. Member States shall ensure that transparent and up-to-date information on applicable prices and tariffs, and on standard terms and conditions, in respect of access to and use of publicly available telephone services is available to end-users and consumers, in accordance with the provisions of Annex II. 2. National regulatory authorities shall encourage the provision of information to enable end-users, as far as appropriate, and consumers to make an independent evaluation of the cost of alternative usage patterns, by means of, for instance, interactive guides. Article 22 – Quality of service 1. Member States shall ensure that national regulatory authorities are, after taking account of the views of interested parties, able to require undertakings that provide publicly available electronic communications services to publish comparable, adequate and up-to-date information for end-users on the quality of their services. The information shall, on request, also be supplied to the national regulatory authority in advance of its publication. 2. National regulatory authorities may specify, inter alia, the quality of service parameters to be measured, and the content, form and manner of information to be published, in order to ensure that end-users have access to comprehensive, comparable and user-friendly information. Where appropriate, the parameters, definitions and measurement methods given in Annex III could be used. Article 23 –Integrity of the network Member States shall take all necessary steps to ensure the integrity of the public telephone network at fixed locations and, in the event of catastrophic network breakdown or in cases of force majeure, the availability of the public telephone network and publicly available telephone services at fixed locations. Member States shall ensure that

	undertakings providing publicly available telephone services at fixed locations take all reasonable steps to ensure uninterrupted access to emergency services.
Relevance to RM/RA	The cited articles impose certain obligations on the providers of public communications networks or publicly available electronic communications services and on the Member States, in order to ensure that the end users have access to good quality electronics communications services, specifically when market developments cannot ensure that certain basic needs are met. Specifically: Service providers must ensure that they have sufficient information available to show how the applicable universal service standards are being met, and to what extent; Member States may impose additional requirements and audit for compliance; Member States may decide to intervene financially when the provision of universal service to the general public carries a disproportionate cost for the service provider(s); Member States must ensure that sufficient transparency is guaranteed with regard to cost and pricing information to comply with universal service requirements, as well as with regard to the quality of such services; Member States must ensure the integrity of the public telephone network; and they must ensure that public telephony service providers take all reasonable steps to ensure uninterrupted access to emergency services. From an RM/RA perspective, the obligations above imply that the affected providers must assess their policies and practices to ensure that they can comply with these obligations.

E. E-Business

Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards

Title:	Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations; as modified and amended by Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998
Source reference:	http://europa.eu.int/eur-lex/pri/en/oj/dat/1998/l_204/l_20419980721en00370048.pdf (unofficial coordinated version: see http://portal.etsi.org/public-interest/Documents/Directives/Standardization/Directive_98_34amended.doc)
Topic:	Regulatory practices with regard to standardisation
Scope	Directly applicable to all EU Member States
Direct/ indirect relevance	Indirect. The text contains standardisation requirements, some of which imply an obligation to implement certain RM/RA measures.
Legal force:	EU Directive, requires transposition into national law
Affected sectors:	For the relevant provision: only the chemical sector
Relevant provision(s):	Article 8 1. Subject to Article 10, Member States shall immediately communicate to the Commission any draft technical regulation, except where it merely transposes the full text of an international or European standard, in which case information regarding the relevant standard shall suffice; they shall also let the Commission have a statement of the grounds which make the enactment of such a technical regulation necessary, where these have not already been made clear in the draft. […] Where, in particular, the draft seeks to limit the marketing or use of a chemical substance, preparation or product on grounds of public health or of the protection of consumers or the environment, Member States shall also forward either a summary or the references of all relevant data relating to the substance, preparation or product concerned and to known and available substitutes, where such information may be available, and communicate the anticipated effects of the measure on public health and the protection of the consumer and the environment, together with an analysis of the risk carried out as appropriate in accordance with the general principles for the risk evaluation of chemical substances as referred to in Article 10(4) of Regulation (EEC) No 793/9317 in the case of an existing substance or in Article 3(2) of Directive 67/548/EEC18, in the case of a new substance. The Commission shall immediately notify the other Member States of the draft and all documents which have been forwarded to it; it may also refer this draft, for an opinion, to the Committee referred to in Article 5 and, where appropriate, to the committee responsible for the field in question. […]
Relevance to	The cited article requires that a Member State considering a restriction

RM/RA	on the marketing or use of a chemical substance, preparation or product on grounds of public health or of the protection of consumers or the environment, must notify the Commission of this, along with certain additional information, including a risk evaluation.

New approach directives

Title:	The New Approach Directives include a large number of Directives, whose common element is that they rely principally on self-certification through the application of the well known CE-marking on compliant products. A full list of Directives can be found here: http://ec.europa.eu/enterprise/newapproach/standardization/harmstds/reflist.html Since most of these Directives are applicable only to very specific product categories which are out of scope for this Report, this overview will focus on only one sample New Approach Directive, specifically the Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity
Source reference:	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0005:EN:HTML (for other New Approach Directives: see http://ec.europa.eu/enterprise/newapproach/standardization/harmstds/reflist.html)
Topic:	Conformity assessment of radio equipment and telecommunications equipment
Scope	Directly applicable to all EU Member States
Direct/ indirect relevance	Indirect. The text requires the manufacturers, distributors or importers of radio equipment and telecommunications equipment to assess their suitability and safety prior to bringing them to the market, which may imply an obligation to conduct an RM/RA assessment with regard to product safety, non-interference and interconnectivity.
Legal force:	EU Directive, requires transposition into national law
Affected sectors:	For the relevant provision: only the chemical sector
Relevant provision(s):	Article 3 – Essential requirements 1. The following essential requirements are applicable to all apparatus: (a) the protection of the health and the safety of the user and any other person, including the objectives with respect to safety requirements contained in Directive 73/23/EEC, but with no voltage limit applying; (b) the protection requirements with respect to electromagnetic compatibility contained in Directive 89/336/EEC. 2. In addition, radio equipment shall be so constructed that it effectively uses the spectrum allocated to terrestrial/space radio communication and orbital resources so as to avoid harmful interference. 3. In accordance with the procedure laid down in Article 15, the Commission may decide that apparatus within certain equipment classes or apparatus of particular types shall be so constructed that: (a) it inter-works via networks with other apparatus and that it can be connected to interfaces of the appropriate type throughout the Community; and/or that (b) it does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service; and/or that (c) it incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected; and/or that (d) it supports certain features ensuring avoidance of fraud; and/or that

	(e) it supports certain features ensuring access to emergency services; and/or that (f) it supports certain features in order to facilitate its use by users with a disability. […] Article 6 - Placing on the market 1. Member States shall ensure that apparatus is placed on the market only if it complies with the appropriate essential requirements identified in Article 3 and the other relevant provisions of this Directive when it is properly installed and maintained and used for its intended purpose. It shall not be subject to further national provisions in respect of placing on the market. […] 3. Member States shall ensure that the manufacturer or the person responsible for placing the apparatus on the market provides information for the user on the intended use of the apparatus, together with the declaration of conformity to the essential requirements. […] 4. In the case of radio equipment using frequency bands whose use is not harmonised throughout the Community, the manufacturer or his authorised representative established within the Community or the person responsible for placing the equipment on the market shall notify the national authority responsible in the relevant Member State for spectrum management of the intention to place such equipment on its national market. This notification shall be given no less than four weeks in advance of the start of placing on the market and shall provide information about the radio characteristics of the equipment (in particular frequency bands, channel spacing, type of modulation and RF-power) and the identification number of the notified body referred to in Annex IV or V. Article 7 - Putting into service and right to connect 1. Member States shall allow the putting into service of apparatus for its intended purpose where it complies with the appropriate essential requirements identified in Article 3 and the other relevant provisions of this Directive. […] Article 10 - Conformity assessment procedures 1. The conformity assessment procedures identified in this Article shall be used to demonstrate the compliance of the apparatus with all the relevant essential requirements identified in Article 3. […]
Relevance to RM/RA	The cited articles require that any apparatus (i.e. radio or telecommunications terminal equipment as defined in the Directive) meets specific safety standards. Furthermore, the Commission may decide to impose additional requirements on specific product types,

	including non-interference and data protection requirements. Thus, before introducing such apparatus on the EU market or putting it into service, the producer/importer/distributor of the product will need to assess which requirements apply, and if the product conforms to them following the prescribed conformity assessment procedures, followed (if successful) by the application of the well known CE marking. In specific cases, radio equipment must also be notified to the competent national authority in order to ascertain any spectrum issues. Finally, the end user must be duly informed of the intended use of the product, and of its compliance with applicable requirements.

Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information

Title:	Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information (also the 'Public Sector Information Directive' or briefly the 'PSI Directive')
Source reference:	http://ec.europa.eu/information_society/policy/psi/docs/pdfs/directive/psi_directive_en.pdf
Topic:	Re-use of public sector information
Scope	Directly applicable to all EU Member States
Direct/ indirect relevance	Indirect. The text requires public administrations to conduct RM/RA analyses before making documents available for re-use, which implies an obligation to implement appropriate RM/RA practices with regard to information security.
Legal force:	EU Directive, requires transposition into national law
Affected sectors:	All sectors of e-government
Relevant provision(s):	Article 1 – Subject matter and scope 1. This Directive establishes a minimum set of rules governing the re-use and the practical means of facilitating reuse of existing documents held by public sector bodies of the Member States. 2. This Directive shall not apply to: (a) documents the supply of which is an activity falling outside the scope of the public task of the public sector bodies concerned as defined by law or by other binding rules in the Member State, or in the absence of such rules as defined in line with common administrative practice in the Member State in question; (b) documents for which third parties hold intellectual property rights; (c) documents which are excluded from access by virtue of the access regimes in the Member States, including on the grounds of: — the protection of national security (i.e. State security), defence, or public security, — statistical or commercial confidentiality; (d) documents held by public service broadcasters and their subsidiaries, and by other bodies or their subsidiaries for the fulfilment of a public service broadcasting remit; (e) documents held by educational and research establishments, such as schools, universities, archives, libraries and research facilities including, where relevant, organisations established for the transfer of research results; (f) documents held by cultural establishments, such as museums, libraries, archives, orchestras, operas, ballets and theatres. 3. This Directive builds on and is without prejudice to the existing access regimes in the Member States. This Directive shall not apply in cases in which citizens or companies have to prove a particular interest under the access regime to obtain access to the documents. […] Article 11 – Prohibition of exclusive arrangements 1. The re-use of documents shall be open to all potential actors in the market, even if one or more market players already exploit added-value products based on these documents.

	Contracts or other arrangements between the public sector bodies holding the documents and third parties shall not grant exclusive rights. 2. However, where an exclusive right is necessary for the provision of a service in the public interest, the validity of the reason for granting such an exclusive right shall be subject to regular review, and shall, in any event, be reviewed every three years. The exclusive arrangements established after the entry into force of this Directive shall be transparent and made public. 3. Existing exclusive arrangements that do not qualify for the exception under paragraph 2 shall be terminated at the end of the contract or in any case not later than 31 December 2008.
Relevance to RM/RA	While the principle of a right to re-use public sector information may not appear to have clear RA/RM implications, the provisions above show that such considerations are relevant on at least two fronts: When determining if a document is susceptible to re-use, the public sector body controlling it will have to assess risks of third party intellectual property rights claims, as well as potential threats to defence and public security, in addition to private interests. Thus, this implies a first RM/RA test which is certainly nontrivial. Secondly, when making documents available for re-use, an assessment needs to be made of whether the omission of exclusivity arrangements might prove to be a barrier to the provision of public services. While this may appear counterintuitive, in certain cases it is only economically viable to offer a specific service if one service provider is given exclusive rights to the information involved.

Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market

Title:	Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)
Source reference:	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:NOT
Topic:	Regulation with regard to information society services, in particular electronic commerce; including the legal liability of intermediary service providers,
Scope	Directly applicable to all EU Member States
Direct/ indirect relevance	Indirect. The text contains liability provisions for intermediary service providers which imply an obligation to implement appropriate RM/RA measures with regard to network/information security.
Legal force:	EU Directive, requires transposition into national law
Affected sectors:	Most forms of information society services, although a number of subject field (e.g. activities of notaries public) and contract types (e.g. the transfer of property rights to real estate) are emphatically excluded from the scope of the Directive.
Relevant provision(s):	Article 3 – Internal market 1. Each Member State shall ensure that the information society services provided by a service provider established on its territory comply with the national provisions applicable in the Member State in question which fall within the coordinated field. […] Section 4: Liability of intermediary service providers Article 12 - "Mere conduit" 1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider: (a) does not initiate the transmission; (b) does not select the receiver of the transmission; and (c) does not select or modify the information contained in the transmission. 2. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission. 3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

	Article 13 - "Caching" 1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that: (a) the provider does not modify the information; (b) the provider complies with conditions on access to the information; (c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry; (d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and (e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement. 2. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement. Article 14 – Hosting 1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that: (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information. 2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider. 3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information. Article 15 No general obligation to monitor 1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to

	monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity. 2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.
Relevance to RM/RA	The cited provisions of the Directive are relevant to RM/RA, because: Jurisdictional competence of information society service providers is dominated by the country of origin principle, meaning that in principle competence is allocated to the jurisdiction in which the service provider is established. This means that information society service providers can shield themselves from a certain degree of harm by adequately assessing the risks following from this rule (and if warranted, to find a new establishment in a different legal regime). The Directive presents a specific set of rules for the liability (both civil and penal) of certain intermediary services providers. Briefly summarised, they are exempted from a general obligation to monitor the activities of their customer base, and will not be held liable for any unlawful activities occurring through their services, provided that they are not aware of them or of any specific facts which are indicative of them, and that the service provider acts promptly to halt the unlawful activity when its existence is signalled. Proper RM/RA implies that intermediary service providers must install adequate procedures for assessing claims of unlawful activities, and for putting a halt to them in compliance with local law. From a secondary perspective, they must also be able to assess if the signalled activity is indeed prima facie unlawful, which also implies that sufficient RM/RA policies are installed (to avoid liability for claims of customers whose services have been unduly halted).

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

Title:	Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (e-Signatures Directive)
Source reference:	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:NOT
Topic:	Regulation with regard to the use of electronic signatures and electronic certification services, including conditions for their equivalence to handwritten signatures, liability and technical/organisational requirements to providers of qualified certificates.
Scope	Directly applicable to all EU Member States
Direct/ indirect relevance	Indirect. The text contains liability provisions for certification service providers (CSPs), along with a series of annexes describing inter alia RM/RA requirements for CSPs involved in issuing qualified certificates and requirements imposed on secure signature creation devices.
Legal force:	EU Directive, requires transposition into national law
Affected sectors:	Any sector relying on electronic signatures or electronic certification service providers.
Relevant provision(s):	Article 5 – Legal effects of electronic signatures 1. Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device: (a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and (b) are admissible as evidence in legal proceedings. 2. Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is: - in electronic form, or - not based upon a qualified certificate, or - not based upon a qualified certificate issued by an accredited certification-service-provider, or - not created by a secure signature-creation device. Article 6 – Liability 1. As a minimum, Member States shall ensure that by issuing a certificate as a qualified certificate to the public or by guaranteeing such a certificate to the public a certification-service-provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate: (a) as regards the accuracy at the time of issuance of all information contained in the qualified certificate and as regards the fact that the certificate contains all the details prescribed for a qualified certificate; (b) for assurance that at the time of the issuance of the certificate, the signatory identified in the qualified certificate held the signature-creation data corresponding to the signature-verification data given or identified in the certificate; (c) for assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases

	where the certification-service-provider generates them both; unless the certification-service-provider proves that he has not acted negligently. 2. As a minimum Member States shall ensure that a certification-service-provider who has issued a certificate as a qualified certificate to the public is liable for damage caused to any entity or legal or natural person who reasonably relies on the certificate for failure to register revocation of the certificate unless the certification-service-provider proves that he has not acted negligently. 3. Member States shall ensure that a certification-service-provider may indicate in a qualified certificate limitations on the use of that certificate. provided that the limitations are recognisable to third parties. The certification-service-provider shall not be liable for damage arising from use of a qualified certificate which exceeds the limitations placed on it. 4. Member States shall ensure that a certification-service-provider may indicate in the qualified certificate a limit on the value of transactions for which the certificate can be used, provided that the limit is recognisable to third parties. The certification-service-provider shall not be liable for damage resulting from this maximum limit being exceeded. 5. The provisions of paragraphs 1 to 4 shall be without prejudice to Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts(8). ANNEX II Requirements for certification-service-providers issuing qualified certificates Certification-service-providers must: (a) demonstrate the reliability necessary for providing certification services; (b) ensure the operation of a prompt and secure directory and a secure and immediate revocation service; (c) ensure that the date and time when a certificate is issued or revoked can be determined precisely; (d) verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued; (e) employ personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic signature technology and familiarity with proper security procedures; they must also apply administrative and management procedures which are adequate and correspond to recognised standards; (f) use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them; (g) take measures against forgery of certificates, and, in cases where the certification-service-provider generates signature-creation data, guarantee confidentiality during the process of generating such data; (h) maintain sufficient financial resources to operate in conformity with

	the requirements laid down in the Directive, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance; (i) record all relevant information concerning a qualified certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically; (j) not store or copy signature-creation data of the person to whom the certification-service-provider provided key management services; (k) before entering into a contractual relationship with a person seeking a certificate to support his electronic signature inform that person by a durable means of communication of the precise terms and conditions regarding the use of the certificate, including any limitations on its use, the existence of a voluntary accreditation scheme and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in redily understandable language. Relevant parts of this information must also be made available on request to third-parties relying on the certificate; (l) use trustworthy systems to store certificates in a verifiable form so that: - only authorised persons can make entries and changes, - information can be checked for authenticity, - certificates are publicly available for retrieval in only those cases for which the certificate-holder's consent has been obtained, and - any technical changes compromising these security requirements are apparent to the operator. ANNEX III Requirements for secure signature-creation devices 1. Secure signature-creation devices must, by appropriate technical and procedural means, ensure at the least that: (a) the signature-creation-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured; (b) the signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology; (c) the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others. 2. Secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.
Relevance to RM/RA	The cited provisions of the Directive are relevant to RM/RA, because: Firstly, the Directive installs a tiered system of electronic signatures, ranging from basic over advanced to qualified. The legal value of a signature depends on its qualification. Any entity wishing to rely on electronic signatures therefore needs to assess the legal status of its signature, based on its qualities (and to a much lesser extent the jurisdiction in which it will be presented), to determine if it can be expected to hold up in a court of law. Secondly, the Directive installs liability rules for certification service providers who issue qualified certificates. Among other obligations, they are generally liable if damage results from a third party's reliance on

	inaccurate information stored in the certificate, or from untimely certificate revocation practices. Thus, issues of qualified certificates need to install appropriate procedures to manage these risks. Thirdly, the Annexes to the Directive specify a number of requirements, including with regard to the issuers of qualified certificates (Annex II) and to secure signature creation devices (SSCDs). Any aspiring certification service provider wishing to deliver qualified certificates therefore needs to ensure that the appropriate procedures are put in place to meet the requirements presented in Annex II; and providers of qualified signature solutions must ensure that the signature creation devices they rely upon are actually SSCDs.

Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services and amending Council Directive 90/619/EEC and Directives 97/7/EC and 98/27/EC

Title:	Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services and amending Council Directive 90/619/EEC and Directives 97/7/EC and 98/27/EC (the 'Financial Distance Marketing Directive')
Source reference:	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0065:EN:NOT
Topic:	Marketing to consumers of consumer financial services
Scope	Directly applicable to all EU Member States
Direct/ indirect relevance	Direct. The text contains a direct obligation to inform customers of any risks involved in the financial services being offered.
Legal force:	EU Directive, requires transposition into national law
Affected sectors:	Financial services
Relevant provision(s):	Article 3 – Information to the consumer prior to the conclusion of the distance contract 1. In good time before the consumer is bound by any distance contract or offer, he shall be provided with the following information concerning: (1) the supplier […] (2) the financial service (a) a description of the main characteristics of the financial service; (b) the total price to be paid by the consumer to the supplier for the financial service, including all related fees, charges and expenses, and all taxes paid via the supplier or, when an exact price cannot be indicated, the basis for the calculation of the price enabling the consumer to verify it; (c) where relevant notice indicating that the financial service is related to instruments involving special risks related to their specific features or the operations to be executed or whose price depends on fluctuations in the financial markets outside the supplier's control and that historical performances are no indicators for future performances; […] 2. The information referred to in paragraph 1, the commercial purpose of which must be made clear, shall be provided in a clear and comprehensible manner in any way appropriate to the means of distance communication used, with due regard, in particular, to the principles of good faith in commercial transactions, and the principles governing the protection of those who are unable, pursuant to the legislation of the Member States, to give their consent, such as minors. […]
Relevance to	The cited article requires that, as a part of the minimum information to be

RM/RA	provided to a consumer prior to concluding a distance financial services contract, the consumer must be clearly and comprehensibly informed of any specific risks related to the service concerned.

Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax

Title:	Directive 2001/115/EC of 20 December 2001 amending Directive 77/388/EEC with a view to simplifying, modernising and harmonising the conditions laid down for invoicing in respect of value added tax (the 'e-Invoicing Directive'). The provisions of this Directive and others have since been bundled in the Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax; however, this coordination has brought no material changes with regard to electronic invoicing. Article numbers below refer to Directive 2006/112/EC.
Source reference:	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001L0115:EN:HTML and http://eur-lex.europa.eu/JOHtml.do?uri=OJ:L:2006:347:SOM:en:HTML
Topic:	VAT harmonisation, specifically with regard to electronic invoicing
Scope	Directly applicable to all EU Member States
Direct/ indirect relevance	Indirect. The text couples the acceptability and validity of electronic invoices to certain objectives which will need to be assessed by the issuers and recipients of electronic invoices.
Legal force:	EU Directive, requires transposition into national law
Affected sectors:	Any commercial transactions subject to VAT regulations
Relevant provision(s):	Article 233 1. Invoices sent or made available by electronic means shall be accepted by Member States provided that the authenticity of the origin and the integrity of their content are guaranteed by one of the following methods: (a) by means of an advanced electronic signature within the meaning of point (2) of Article 2 of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (1); (b) by means of electronic data interchange (EDI), as defined in Article 2 of Commission Recommendation 1994/820/EC of 19 October 1994 relating to the legal aspects of electronic data interchange (2), if the agreement relating to the exchange provides for the use of procedures guaranteeing the authenticity of the origin and integrity of the data. Invoices may, however, be sent or made available by other electronic means, subject to acceptance by the Member States concerned. […] Article 246 The authenticity of the origin and the integrity of the content of the invoices stored, as well as their legibility, must be guaranteed throughout the storage period. In respect of the invoices referred to in the second subparagraph of Article 233(1), the details they contain may not be altered and must remain legible throughout the storage period. Article 247 1. Each Member State shall determine the period throughout which

	taxable persons must ensure the storage of invoices relating to the supply of goods or services in its territory and invoices received by taxable persons established in its territory. 2. In order to ensure that the conditions laid down in Article 246 are met, the Member State referred to in paragraph 1 may require that invoices be stored in the original form in which they were sent or made available, whether paper or electronic. Additionally, in the case of invoices stored by electronic means, the Member State may require that the data guaranteeing the authenticity of the origin of the invoices and the integrity of their content, as provided for in the first paragraph of Article 246, also be stored. [...]
Relevance to RM/RA	The cited articles require that, in a general sense, electronic invoices are considered acceptable if the technologies involved in their use can guarantee their integrity and authenticity. While EDI and advanced signatures are referred to as one possibility, the Directive leaves room for alternative solutions. In such cases, the parties involved will have to assess the permissibility of such solutions under their respective legal frameworks, and keeping into account the goals of authenticity and integrity. Secondly, the electronic storage of electronic invoices is permissible provided that authenticity, integrity and legibility of the document is guaranteed, both for the main document and the relevant metadata. This implies due consideration of such elements as the involvement of trusted third parties, time stamping and signature solutions, and data format decisions.

F Risk Management / Risk Assessment Standards

ISO/IEC Standard 13335 - Information technology -- Security techniques -- Management of information and communications technology security

Title:	ISO/IEC 13335-1:2004 - Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management
Source reference:	http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39066 (Note: this is a reference to the ISO page where the standard can be acquired. However, the standard is not free of charge, and its provisions are not publicly available. For this reason, specific provisions cannot be quoted).
Topic:	Standard containing generally accepted descriptions of concepts and models for information and communications technology security management.
Scope	Not publicly available ISO standard, which can be voluntarily implemented.
Direct/ indirect relevance	Direct. The text is a direct resource for the implementation of security management.
Legal force:	Nonbinding ISO standard.
Affected sectors:	Generic. The standard can be implemented in any sector confronted by technology security management.
Relevant provision(s):	The standard is not free of charge, and its provisions are not publicly available. For this reason, specific provisions cannot be quoted.
Relevance to RM/RA	The standard is a commonly used code of practice, and serves as a resource for the implementation of security management practices and as a yardstick for auditing such practices. (See also http://csrc.nist.gov/publications/secpubs/otherpubs/reviso-faq.pdf)

BS 25999 – Business continuity management

Title:	BS 25999-1:2006 - Business continuity management Part 1: Code of practice Note: this is only part one of BS 25999, which was published in November 2006. Part two (which should contain more specific criteria with a view of possible accreditation) is yet to appear.
Source reference:	http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=000000000030157563 (Note: this is a reference to the BSI page where the standard can be acquired. However, the standard is not free of charge, and its provisions are not publicly available. For this reason, specific provisions cannot be quoted).
Topic:	Standard containing a business continuity code of practice.
Scope	Not publicly available BSI standard, which can be voluntarily implemented.
Direct/ indirect relevance	Direct. The text is a direct code of practice for business continuity management.
Legal force:	Nonbinding BSI standard.
Affected sectors:	Generic. The standard can be implemented in any sector confronted by business continuity requirements.
Relevant provision(s):	The standard is not free of charge, and its provisions are not publicly available. For this reason, specific provisions cannot be quoted. The publicly available BSI abstract describes the standard as follows: *"BS 25999-1:2006 is a code of practice that takes the form of guidance and recommendations. It establishes the process, principles and terminology of business continuity management (BCM), providing a basis for understanding, developing and implementing business continuity within an organization and to provide confidence in business-to-business and business-to-customer dealings."* Source: http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=000000000030157563
Relevance to RM/RA	The standard is intended as a code of practice for business continuity management, and will be extended by a second part that should permit accreditation for adherence with the standard. Given its relative newness, the potential impact of the standard is difficult to assess, although it could be very influential to RM/RA practices, given the general lack of universally applicable standards in this regard and the increasing attention to business continuity and contingency planning in regulatory initiatives. Application of this standard can be complemented by other norms, in particular PAS 77:2006 - IT Service Continuity Management Code of Practice (see http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=000000000030141858).

ISO/IEC Standard 15443 - Information technology -- Security techniques -- A framework for IT security assurance

Title:	ISO/IEC TR 15443-1:2005 – Information technology -- Security techniques -- A framework for IT security assurance
Source reference:	http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39733 (Note: this is a reference to the ISO page where the standard can be acquired. However, the standard is not free of charge, and its provisions are not publicly available. For this reason, specific provisions cannot be quoted).
Topic:	Security assurance – the Technical Report (TR) contains generally accepted guidelines which can be used to determine an appropriate assurance method for assessing a security service, product or environmental factor
Scope	Not publicly available ISO TR, which can be voluntarily applied.
Direct/ indirect relevance	Direct. The text allows security professionals to determine a suitable methodology for assessing a security service, product or environmental factor (a deliverable) and for assessing compliance with the chosen security level.
Legal force:	Nonbinding ISO Technical Report.
Affected sectors:	Generic. The TR can be applied by security professionals in any sector confronted by technology security management.
Relevant provision(s):	The TR is not free of charge, and its provisions are not publicly available. For this reason, specific provisions cannot be quoted. The publicly available abstract describes the TR as follows: *"ISO/IEC TR 15443 is a multi-part type 3 Technical Report to guide the IT security professional in the selection of an appropriate assurance method when specifying, selecting, or deploying a security service, product, or environmental factor such as an organization or personnel (known as a deliverable). The aim is to understand the assurance type and amount required to achieve confidence that the deliverable satisfies the stated IT security assurance requirements and consequently its security policy.* *ISO/IEC TR 15443-1:2005 describes the fundamentals of security assurance and its relation to other security concepts. This is to clarify why security assurance is required and dispel common misconceptions such as that increased assurance is gained by increasing the strength of a security mechanism. The framework includes a categorization of assurance types and a generic lifecycle model to identify the appropriate assurance types required for the deliverable with respect to the deliverable's lifecycle. The model also demonstrates how security assurance must be managed throughout the deliverable's lifecycle requiring assurance decisions to be made by several assurance authorities for the lifecycle stage relevant to their organization (i.e. developer, standards, consumer). The framework has been developed to be general enough to accommodate different assurance types and map into any lifecycle approach so as not to dictate any particular design. Advanced security assurance concepts, such as combining security assurance methods, are addressed briefly as they are to be addressed in later parts of ISO/IEC TR 15443.* *ISO/IEC TR 15443 targets IT security managers and other security professionals responsible for developing a security assurance program, engineering security into a deliverable, determining the security assurance of their deliverable, entering an assurance assessment audit*

	(e.g. ISO 9000, SSE-CMM (ISO/IEC 21827), ISO/IEC 15408-3), or other assurance activities." Source: http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39733
Relevance to RM/RA	The TR allows security professionals to determine a suitable methodology for assessing a security service, product or environmental factor (a deliverable). Following this TR, it can be determined which level of security assurance a deliverable is intended to meet, and if this threshold is actually met by the deliverable.

ISO/IEC Standard 15816 – Information technology -- Security techniques -- Security information objects for access control

Title:	ISO/IEC 15816:2002 - Information technology -- Security techniques -- Security information objects for access control
Source reference:	http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=29139 (Note: this is a reference to the ISO page where the standard can be acquired. However, the standard is not free of charge, and its provisions are not publicly available. For this reason, specific provisions cannot be quoted).
Topic:	Security management – Access control
Scope	Not publicly available ISO standard, which can be voluntarily applied.
Direct/ indirect relevance	Indirect. The text is a basic resource which can be used in access control issues, but contains no RM/RA obligations/methodologies as such.
Legal force:	Nonbinding ISO standard.
Affected sectors:	Generic. The standard can be applied by security professionals in any sector confronted by access control difficulties.
Relevant provision(s):	The standard is not free of charge, and its provisions are not publicly available. For this reason, specific provisions cannot be quoted. Generically, it is described as containing: a) the definition of guidelines for specifying the abstract syntax of generic and specific Security Information Objects (SIOs) for Access Control; b) the specification of generic SIOs for Access Control; c) the specification of specific SIOs for Access Control. The scope of this Recommendation | International Standard covers only the "statics" of SIOs through syntactic definitions in terms of ASN.1 descriptions and additional semantic explanations. It does not cover the "dynamics" of SIOs, for example rules relating to their creation and deletion. The dynamics of SIOs are a local implementation issue.
Relevance to RM/RA	The standard allows security professionals to rely on a specific set of syntactic definitions and explanations with regard to SIOs, thus avoiding duplication or divergence in other standardisation efforts.

ISO/IEC TR 15947 – Information technology -- Security techniques -- IT intrusion detection framework

Title:	ISO/IEC TR 15947:2002 - Information technology -- Security techniques -- IT intrusion detection framework
Source reference:	http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=29580 (Note: this is a reference to the ISO page where the standard can be acquired. However, the standard is not free of charge, and its provisions are not publicly available. For this reason, specific provisions cannot be quoted).
Topic:	Security management – Intrusion detection in IT systems
Scope	Not publicly available ISO Technical Report (TR), which can be voluntarily applied.
Direct/ indirect relevance	Indirect. The text allows security professionals to rely on a specific set of concepts and methodologies for describing and assessing security risks with regard to potential intrusions in IT systems. It can be used as a tool for RM/RA.
Legal force:	Nonbinding ISO TR.
Affected sectors:	Generic. The TR can be applied by security professionals in any sector confronted by IT intrusion detection difficulties.
Relevant provision(s):	The TR is not free of charge, and its provisions are not publicly available. For this reason, specific provisions cannot be quoted. The publicly available abstract describes the TR as follows: *"ISO/IEC TR 15947:2002 defines a framework for detection of intrusions into IT systems. It establishes common definitions for intrusion detection terms and concepts. It describes the methodologies, concepts and relationships among them, addresses possible orderings of intrusion detection tasks and related activities, and attempts to relate these tasks and processes to an organization's or enterprise's procedures to demonstrate the practical integration of intrusion detection within an organization or enterprise security policy."* Source: http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=29580
Relevance to RM/RA	The standard allows security professionals to rely on a specific set of concepts and methodologies for describing and assessing security risks with regard to potential intrusions in IT systems. It does not contain any RM/RA obligations as such, but it is rather a tool for facilitating RM/RA activities in the affected field.

ISO/IEC Standard 15408 - Information technology -- Security techniques -- Evaluation criteria for IT security

Title:	ISO/IEC 15408-1/2/3:2005 - Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model (15408-1) Part 2: Security functional requirements (15408-2) Part 3: Security assurance requirements (15408-3)
Source reference:	http://isotc.iso.org/livelink/livelink/fetch/2000/2489/Ittf_Home/PubliclyAvailableStandards.htm
Topic:	Standard containing a common set of requirements for the security functions of IT products and systems and for assurance measures applied to them during a security evaluation.
Scope	Publicly available ISO standard, which can be voluntarily implemented.
Direct/ indirect relevance	Indirect. The text is a resource for the evaluation of the security of IT products and systems, and can thus be used as a tool for RM/RA.
Legal force:	Nonbinding ISO standard.
Affected sectors:	Generic. The standard can be implemented in any sector confronted by the need to test the security of IT products and systems.
Relevant provision(s):	The standard is made up of three parts: a) Part 1, Introduction and general model, is the introduction to ISO/IEC 15408. It defines general concepts and principles of IT security evaluation and presents a general model of evaluation. Part 1 also presents constructs for expressing IT security objectives, for selecting and defining IT security requirements, and for writing high-level specifications for products and systems. In addition, the usefulness of each part of ISO/IEC 15408 is described in terms of each of the target audiences. b) Part 2, Security functional requirements, establishes a set of functional components as a standard way of expressing the functional requirements for TOEs [Targets Of Evaluation). Part 2 catalogues the set of functional components, families, and classes. c) Part 3, Security assurance requirements, establishes a set of assurance components as a standard way of expressing the assurance requirements for TOEs. Part 3 catalogues the set of assurance components, families and classes. Part 3 also defines evaluation criteria for PPs and STs and presents evaluation assurance levels that define the predefined ISO/IEC 15408 scale for rating assurance for TOEs, which is called the Evaluation Assurance Levels (EALs). *(source:* http://standards.iso.org/ittf/PubliclyAvailableStandards/c040612_ISO_IEC_15408-1_2005(E).zip)
Relevance to RM/RA	The standard is commonly used as a resource for the evaluation of the security of IT products and systems; including (if not specifically) for procurement decisions with regard to such products. The standard can thus be used as an RM/RA tool to determine the security of an IT product or system during its design, manufacturing or marketing, or before procuring it.

ISO/IEC Standard 17799 - Information technology -- Security techniques -- Code of practice for information security management

Title:	ISO/IEC 17799:2005 - Information technology -- Security techniques -- Code of practice for information security management
Source reference:	http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39612&ICS1=35&ICS2=40&ICS3= (Note: this is a reference to the ISO page where the standard can be acquired. However, the standard is not free of charge, and its provisions are not publicly available. For this reason, specific provisions cannot be quoted).
Topic:	Standard containing generally accepted guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization, including business continuity management.
Scope	Not publicly available ISO standard, which can be voluntarily implemented.
Direct/ indirect relevance	Direct. While not legally binding, the text is a direct resource towards sound information security management.
Legal force:	Nonbinding ISO standard.
Affected sectors:	Generic. The standard can be implemented in any sector confronted by information security management.
Relevant provision(s):	The standard is not free of charge, and its provisions are not publicly available. For this reason, specific provisions cannot be quoted. Generally, the contents of the abstract are described as follows: *'ISO/IEC 17799:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC 17799:2005 contains best practices of control objectives and controls in the following areas of information security management:* ** security policy;* ** organization of information security;* ** asset management;* ** human resources security;* ** physical and environmental security;* ** communications and operations management;* ** access control;* ** information systems acquisition, development and maintenance;* ** information security incident management;* ** business continuity management;* ** compliance.* *The control objectives and controls in ISO/IEC 17799:2005 are intended to be implemented to meet the requirements identified by a risk assessment. ISO/IEC 17799:2005 is intended as a common basis and practical guideline for developing organizational security standards and effective security management practices, and to help build confidence in inter-organizational activities.' (source:* http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39612&ICS1=35&ICS2=40&ICS3=)
Relevance to RM/RA	The standard is a commonly used code of practice, and serves as a resource for the implementation of information security management practices and as a yardstick for auditing such practices. (See also http://en.wikipedia.org/wiki/ISO/IEC_17799)

ISO/IEC TR 15446 – Information technology -- Security techniques -- Guide for the production of Protection Profiles and Security Targets

Title:	ISO/IEC TR 15446:2004 – Information technology -- Security techniques -- Guide for the production of Protection Profiles and Security Targets
Source reference:	http://isotc.iso.org/livelink/livelink/fetch/2000/2489/Ittf_Home/PubliclyAvailableStandards.htm
Topic:	Technical Report (TR) containing guidelines for the construction of Protection Profiles (PPs) and Security Targets (STs) that are intended to be compliant with ISO/IEC 15408 (the "Common Criteria"). Note: PPs and STs are described in the TR as follows: *"The purpose of a Protection Profile (PP) is to state a security problem rigorously for a given collection of systems or products - known as the Target Of Evaluation (TOE) - and to specify security requirements to address that problem without dictating how these requirements will be implemented.* *[…]* *A Security Target (ST) is similar to PP, except that it contains additional implementation-specific information detailing how the security requirements are realised in a particular product or system."* (Source: http://standards.iso.org/ittf/PubliclyAvailableStandards/c039690_ISO_IEC_TR_15446_2004(E).zip)
Scope	Publicly available ISO TR, which can be voluntarily adhered to.
Direct/ indirect relevance	Indirect. The text is a resource for the definition of security concepts, but has no direct implications for RM/RA as such.
Legal force:	Nonbinding ISO TR.
Affected sectors:	Generic. The standard can be adhered to by any security professional involved in creating PPs and STs.
Relevant provision(s):	The standard describes how PPs and STs should be created, including a description of which information should be provided; and provides a number of practical examples of complaints PPs and STs.
Relevance to RM/RA	The standard is predominantly used as a tool for security professionals to develop PPs and STs, but can also be used to assess the validity of the same (by using the TR as a yardstick to determine if its standards have been obeyed). Thus, it is a (nonbinding) normative tool for the creation and assessment of RM/RA practices.

ISO/IEC Standard 18028 - Information technology -- Security techniques -- IT network security

Title:	ISO/IEC 18028:2006 - Information technology -- Security techniques -- IT network security
Source reference:	http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=40008 (Note: this is a reference to the ISO page where the standard can be acquired. However, the standard is not free of charge, and its provisions are not publicly available. For this reason, specific provisions cannot be quoted).
Topic:	Five part standard (ISO/IEC 18028-1 to 18028-5) containing generally accepted guidelines on the security aspects of the management, operation and use of information technology networks. The standard is considered an extension of the guidelines provided in ISO/IEC 13335 and ISO/IEC 17799 focusing specifically on network security risks.
Scope	Not publicly available ISO standard, which can be voluntarily implemented.
Direct/ indirect relevance	Direct. While not legally binding, the text is a direct resource for RM/RA with regard to network operation.
Legal force:	Nonbinding ISO standard.
Affected sectors:	Generic. The standard can be followed in any sector, as the only criterion for applicability is the ownership, use or operation of a network.
Relevant provision(s):	The standard is not free of charge, and its provisions are not publicly available. For this reason, specific provisions cannot be quoted.
Relevance to RM/RA	The standard is a commonly used code of practice, and serves as a resource for the implementation of security management practices and as a yardstick for auditing such practices.

ISO/IEC Standard 27001 - Information technology -- Security techniques -- Information security management systems

Title:	ISO/IEC 27001:2005 - Information technology -- Security techniques -- Information security management systems -- Requirements
Source reference:	http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=42103 (Note: this is a reference to the ISO page where the standard can be acquired. However, the standard is not free of charge, and its provisions are not publicly available. For this reason, specific provisions cannot be quoted).
Topic:	Standard containing generally accepted guidelines for the implementation of an Information Security Management System within any given organisation.
Scope	Not publicly available ISO standard, which can be voluntarily implemented.
Direct/ indirect relevance	Direct. While not legally binding, the text contains direct guidelines for the creation of sound information security practices.
Legal force:	Nonbinding ISO standard.
Affected sectors:	Generic. The standard can be implemented in any sector confronted by information security management.
Relevant provision(s):	The standard is not free of charge, and its provisions are not publicly available. For this reason, specific provisions cannot be quoted. Generally, the contents of the abstract are described as follows: *'ISO/IEC 27001:2005 covers all types of organizations (e.g. commercial enterprises, government agencies, not-for profit organizations). ISO/IEC 27001:2005 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof.* *ISO/IEC 27001:2005 is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties.* *ISO/IEC 27001:2005 is intended to be suitable for several different types of use, including the following:* *use within organizations to formulate security requirements and objectives;* *use within organizations as a way to ensure that security risks are cost effectively managed;* *use within organizations to ensure compliance with laws and regulations;* *use within an organization as a process framework for the implementation and management of controls to ensure that the specific security objectives of an organization are met;* *definition of new information security management processes;* *identification and clarification of existing information security management processes;* *use by the management of organizations to determine the status of information security management activities;* *use by the internal and external auditors of organizations to determine the degree of compliance with the policies, directives and standards adopted by an organization;*

	use by organizations to provide relevant information about information security policies, directives, standards and procedures to trading partners and other organizations with whom they interact for operational or commercial reasons; *implementation of business-enabling information security;* *use by organizations to provide relevant information about information security to customers.'* *(source:* http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=42103)
Relevance to RM/RA	The standard is a very commonly used code of practice, and serves as a resource for the implementation of information security management systems and as a yardstick for auditing such systems and/or the surrounding practices. (See also http://en.wikipedia.org/wiki/ISO/IEC_27001) Its application in practice is often combined with related standards, such as BS 7799-3:2006 which provides additional guidance to support the requirements given in ISO/IEC 27001:2005 (see http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=000000000030125022&recid=2491)

BS 7799-3 – Information security management systems -- Guidelines for information security risk management

Title:	BS 7799-3:2006 - Information security management systems -- Guidelines for information security risk management
Source reference:	http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=0000000000030125022&recid=2491 (Note: this is a reference to the BSI page where the standard can be acquired. However, the standard is not free of charge, and its provisions are not publicly available. For this reason, specific provisions cannot be quoted).
Topic:	Standard containing general guidelines for information security risk management.
Scope	Not publicly available BSI standard, which can be voluntarily implemented.
Direct/ indirect relevance	Direct. While not legally binding, the text contains direct guidelines for the creation of sound information security practices.
Legal force:	Nonbinding BSI standard.
Affected sectors:	Generic. The standard can be implemented in any sector confronted by information security requirements.
Relevant provision(s):	The standard is not free of charge, and its provisions are not publicly available. For this reason, specific provisions cannot be quoted. The publicly available BSI abstract describes the standard as follows: *"Identifying, evaluating, treating and managing information security risks are key processes if businesses want to keep their information safe and secure. Whilst these processes are specified in the information security standard BS ISO/IEC 27001:2005, further guidance is required on how to manage these risks as well as to put them into context with other business risks.* *BS 7799-3:2006 provides this guidance and covers:* *risk assessment* *risk treatment* *management decision making* *risk re-assessment* *monitoring and reviewing of risk profile* *information security risk in the context of corporate governance* *compliance with other risk based standards and regulations."* Source: http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=0000000000030125022&recid=2491
Relevance to RM/RA	The standard is mostly intended as a guiding complementary document to the application of the aforementioned ISO 27001:2005, and is therefore typically applied in conjunction with this standard in risk assessment practices.

ISO/IEC TR 18044 – Information technology -- Security techniques -- Information security incident management

Title:	ISO/IEC TR 18044:2004 – Information technology -- Security techniques -- Information security incident management
Source reference:	http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=35396 (Note: this is a reference to the ISO page where the standard can be acquired. However, the standard is not free of charge, and its provisions are not publicly available. For this reason, specific provisions cannot be quoted).
Topic:	Technical Report (TR) containing generally accepted guidelines and general principles for information security incident management in an organization.
Scope	Not publicly available ISO TR, which can be voluntarily used.
Direct/ indirect relevance	Direct. While not legally binding, the text contains direct guidelines for incident management.
Legal force:	Nonbinding ISO TR.
Affected sectors:	Generic. The TR can be used in any sector confronted by information security incident management needs.
Relevant provision(s):	The TR is not free of charge, and its provisions are not publicly available. For this reason, specific provisions cannot be quoted. Generally, the abstract describes the TR's content as follows: *"ISO/IEC TR 18044:2004 provides advice and guidance on information security incident management for information security managers and for information system managers.* *ISO/IEC TR 18044:2004 provides* *information on the benefits to be obtained from and the key issues associated with a good information security incident management approach (to convince senior corporate management and those personnel who will report to and receive feedback from a scheme that the scheme should be introduced and used);* *information on examples of information security incidents, and an insight into their possible causes;* *a description of the planning and documentation required to introduce a good structured information security incident management approach;* *a description of the information security incident management process*.* ** Quick, co-ordinated and effective responses to an information security incident require extensive technical and procedural preparations. Information security incident responses may consist of immediate, short- and long-term actions. Any actions undertaken as the response to an incident should be based on previously developed, documented and accepted security incident response procedures and processes, including those for post-response analysis.'* *(source:* http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=35396)
Relevance to RM/RA	The standard is a high level resource introducing basic concepts and considerations in the field of incident response. As such, it is mostly useful as a catalyst to awareness raising initiatives in this regard.

ISO/IEC 18045 – Information technology -- Security techniques -- Methodology for IT security evaluation

Title:	ISO/IEC 18045:2005 - Information technology -- Security techniques -- Methodology for IT security evaluation
Source reference:	http://isotc.iso.org/livelink/livelink/fetch/2000/2489/Ittf_Home/PubliclyAvailableStandards.htm
Topic:	Standard containing auditing guidelines for assessment of compliance with ISO/IEC 15408 (Information technology -- Security techniques -- Evaluation criteria for IT security)
Scope	Publicly available ISO standard, to be followed when evaluating compliance with ISO/IEC 15408 (Information technology --Security techniques -- Evaluation criteria for IT security)
Direct/ indirect relevance	Indirect. The text is a meta-norm providing guidelines for compliance evaluation based on the criteria of another standard; not for RM/RA as such.
Legal force:	Nonbinding ISO standard.
Affected sectors:	Generic. The standard can be followed by any auditor involved in evaluating compliance with ISO/IEC 15408 (Information technology -- Security techniques -- Evaluation criteria for IT security).
Relevant provision(s):	ISO/IEC 18045:2005 is a companion document to ISO/IEC 15408, Information technology --Security techniques -- Evaluation criteria for IT security. ISO/IEC 18045 specifies the minimum actions to be performed by an evaluator in order to conduct an ISO/IEC 15408 evaluation, using the criteria and evaluation evidence defined in ISO/IEC 15408. *(source:* http://iso.nocrew.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=30830&ICS1=35&ICS2=40&ICS3=)
Relevance to RM/RA	The standard is a 'companion document', which is thus primarily of used for security professionals involved in evaluating compliance with ISO/IEC 15408 (Information technology --Security techniques -- Evaluation criteria for IT security). Since it describes minimum actions to be performed by such auditors, compliance with ISO/IEC 15408 is impossible if ISO/IEC 18045 has been disregarded.

Initiatives of the Information Security Forum, including the Standard of Good Practice and their auditing standards

Title:	The ISF Standard of Good Practice
Source reference:	http://www.isfsecuritystandard.com/ (Note: this is a link to the ISF page where the standard can be freely downloaded after registration.)
Topic:	High level standard disseminating a series of good practice standards in the field of information security.
Scope	Publicly available standard, drafted and maintained based on biannual surveys by the Information Security Forum (ISF), an international non profit organisation focusing on monitoring, charting and best practices in information security. The standard can be voluntarily adhered to by any interested party.
Direct/ indirect relevance	Direct. While not legally binding, the text contains direct guidelines for sound information security practices.
Legal force:	Nonbinding private body standard.
Affected sectors:	Generic. The standard can be implemented in any sector confronted by information security. Specific areas of focus in the standard include Computer Installations, Networks (i.e. infrastructure), Critical Business Applications, Systems Development and Security Management.
Relevant provision(s):	Given its subject matter, the standard can be considered relevant in its entirety (247p.) to RM/RA practices. The standard is built around the five main aspects, i.e. Computer Installations, Networks (i.e. infrastructure), Critical Business Applications, Systems Development and Security Management. A sixth aspect, User Environment, has been announced but not yet published at the time of writing. Each of these is split into a series of areas. E.g. for Networks, areas include Network Management, Traffic Management, Network Operations, Local Security Management, and Voice Networks. Finally, area is split into sections. E.g. for Traffic Management, sections include Configuring Network Devices, Firewalls, External Access and Wireless Access. In each section, the standard indicates the key principles and objectives, followed by a series of specific rules in order to adhere to these.
Relevance to RM/RA	The standard is a commonly quoted source of good practices, and serves as a resource for the implementation of information security policies and as a yardstick for auditing such systems and/or the surrounding practices.

ISO Standard 13569 - Financial services -- Information security guidelines

Title:	ISO/TR 13569:2005 - Financial services -- Information security guidelines
Source reference:	http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=37245 (Note: this is a reference to the ISO page where the standard can be acquired. However, the standard is not free of charge, and its provisions are not publicly available. For this reason, specific provisions cannot be quoted).
Topic:	Standard containing guidelines for the implementation and assessment of information security policies in financial services institutions.
Scope	Not publicly available ISO standard, which can be voluntarily implemented.
Direct/ indirect relevance	Direct. The text focuses on information security obligations in financial RM/RA practices, which includes aspects of information/network security.
Legal force:	Nonbinding ISO standard.
Affected sectors:	Specifically written for financial institutions.
Relevant provision(s):	The standard is not free of charge, and its provisions are not publicly available. For this reason, specific provisions cannot be quoted. The standard is described by ISO as follows: *"ISO TR 13569:2005 provides guidelines on the development of an information security programme for institutions in the financial services industry. It includes discussion of the policies, organization and the structural, legal and regulatory components of such a programme. Considerations for the selection and implementation of security controls, and the elements required to manage information security risk within a modern financial services institution are discussed. Recommendations are given that are based on consideration of the institutions' business environment, practices and procedures. Included in this guidance is a discussion of legal and regulatory compliance issues, which should be considered in the design and implementation of the programme."* (Source: http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=37245)
Relevance to RM/RA	The standard is a commonly referenced guideline, and serves as a resource for the implementation of information security management programmes in institutions of the financial sector, and as a yardstick for auditing such programmes. (See also http://csrc.nist.gov/publications/secpubs/otherpubs/reviso-faq.pdf)