Annex A. Description of the existing risk analysis methodologies

ID	Method name	Issuer	Description	Standard Compliance
M01	Austrian IT Security Handbook	Austrian federal chancellery	Qualitative method. Consists of 8 steps: Definition of the analysis area, asset identification, impact analysis, threat assessment, vulnerability analysis, identification of existing security measures, risk assessment and result analysis.	ISO/IEC 27001:2013, ISO/IEC 13335-1, -2, ISO/IEC 17799
M02	CCTA Risk Analysis and Management Method (CRAMM)	BCCTA	Qualitative method. Consists of 3 stages: The establishment of the objectives, the assessment of the risks and identification and selection of countermeasures.	ISO/IEC 17799
M03	CORAS	SINTEF ICT	Qualitative method. Consists of 7 steps: introductory meeting, high-level analysis, approval, risk identification, risk estimation, risk evaluation and risk treatment. Has its' own modeling language and tool. Oriented towards software implementation.	AS/NZS 4360:2004, ISO/IEC 17799, ISO/IEC 13335
M04	Dutch A&K Analysis	Dutch ministry of internal affairs	Obsolete, last version update in 1996, available only in Dutch.	ISO/IEC 17799
M05	EBIOS	French National Information Systems Security Agency	Qualitative method. Consists of a cycle of 5 phases, where phase 1 deals with context analysis, phase 2 analyzes the security needs, phase 3 identifies the threats, phases 4 and 5 defines the security risks and objectives. The method is up-to-date.	ISO/IEC 27001, ISO/IEC 15408, ISO/IEC 17799, ISO/IEC 13335, ISO/IEC 21827
M06	Factor Analysis of Information Risk (FAIR)	RMI	Quantitative method. Consists of 4 stages: identification of scenario components, evaluation of loss event frequency, evaluation of probable loss magnitude, risk derivation and articulation.	ISO/IEC 27001
M07	Facilitated Risk Analysis Process (FRAP)	Auerbach	Qualitative method. Social process, where domain specific teams are gathered to discuss the identification of potential threats, vulnerabilities, and negative impacts on data integrity, confidentiality, and availability. Afterwards analysis of the effects of such impacts on business operations and broad categorization of the risks according to their priority level is performed.	–
M08	IRAM2	Information	Qualitative method. A business-oriented, less formal six stage approach consisting	ISO/IEC 17799

ID	Method name	Issuer	Description	Standard Compliance
		Security Forum	of: providing of a business-centric view of risk, assessment of realistic and worst-case business impact scenarios, understanding and modeling threats, understanding how well the environment can resist threats, evaluation of risk against the organization's risk appetite, development of pragmatic risk treatment plans.	
M09	OCTAVE	Carnegie Mellon University	Qualitative method. Consists of 4 stages: develop risk measurement criteria consistent with the organization's mission, goal objectives, and critical success factors, create a profile of each critical information asset that establishes clear boundaries for the asset, identifies its security requirements, and identifies all of its containers, identify threats to each information asset in the context of its containers, identify and analyze risks to information assets and begin to develop mitigation approaches.	–
	Magerit	Ministerio de Administraciones Publicas (Spanish Ministry for Public Administrations)	Qualitative method. Consists of three phases: risk identification, risk analysis and risk evaluation. Magerit is claimed to be an open methodology for Risk Analysis and Management.	ISO/IEC 27001:2005, ISO/IEC 15408:2005, ISO/IEC 17799:2005, ISO/IEC 13335:2004
M11	Marion (Methodology of Analysis of Computer Risks Directed by Levels)	CLUSIF	The level of security is estimated according to 27 indicators distributed in 6 large subjects, each of them assigns a grade between 0 and 4. The level 3 is the level to be reached to ensure a security considered as correct. At the conclusion of this analysis, a more detailed analysis of risk is carried out to identify the risks (threats and vulnerabilities) that face the company. Obsolete, replaced by MEHARI	–
M12	MEHARI	CLUSIF	Qualitative method. Consists of four stages: analyze the major stakes, analyze the vulnerabilities, decrease and manage the risks, monitor the security of information.	ISO/IEC 27001, ISO/IEC 27005
M13	MIGRA	AMTEC/vElsag Datamat S.p.A.	Qualitative method. Provides: a security and risk taxonomy for the two considered domains (information and tangible assets), a logical framework for generating a mod-	ISO 27000 series

ID	Method name	Issuer	Description	Standard Compliance
			el of the security perimeter to be analyzed, an algorithm (based on questionnaires) for assessing, on a four level qualitative scale (High, Medium, Low, Negligible/Not applicable), the value of both information and tangible assets relevant to the above perimeter, a scheme for performing threat and vulnerability analysis, a procedure for calculating (on a qualitative scale) risk, a mechanism to identify in every scenario a set of appropriate security measures, a procedure to perform gap and compliance analysis with reference to corporate security policies, norms, standards, guidelines and best practices.	
M14	RiskSafe Assessment	Platinum Squared	Qualitative method. Provided as a cloud-based tool. Consists of four phases: Business Impact Assessment (BIA), dentifying and assessing threats and vulnerabilities, assessing levels of risk, identifying required and justified controls on the basis of the risk assessment.	ISO/IEC 27001, ISO/IEC 27005
M15	IT-Grundschutz	German Federal Office for Information Security (BSI)	Qualitative method. Consists of twelve steps: initialization of the process, definition of IT security goals and business environment, establishment of an organizational structure for IT security, provision of necessary resources, creation of the IT security concept, IT-Structure analysis assessment of protection requirements, modeling IT security check, supplementary security analysis, implementation planning and fulfillment, maintenance, monitoring and improvement of the process.	ISO/IEC 17799, ISO/IEC 27001, KonTraG, Basel II, TKG, BDSG
M16	Information Security Assessment & Monitoring Method (IS-AMM)	Telindus N.V.	Quantitative type of risk management methodology where the assessed risks are expressed, through their Annual Loss Expectancy (ALE), in monetary units. ALE being the annual expected loss or cost should a threat or a group of threats being materialised.	ISO/IEC 27001, ISO/IEC 27002