International Conference on Cyber Security and Computer Science (ICONCS'18),
Oct 18-20, 2018 Safranbolu, Turkey

Information Security Risk Management and Risk Assessment Methodology and Tools

N.YALÇIN [1] ve B.KILIÇ [2]

[1] Gazi Üniversitesi, Gazi Eğitim Fakültesi, Ankara/Turkey, nyalcin@gazi.edu.tr
[2] Gazi Üniversitesi, Bilişim Enstitüsü, Ankara/Turkey, berker.kilic@gmail.com

Abstract - Nowadays risks related to information security are increasing each passing day. Both public enterprises and private sector are working on information security to provide information security. It is inevitable that the institutions must use the most appropriate methodology and tools for their own needs and legal responsibilities to provide information security.

Particularly Personal Data Protection Law, the legal regulations and the development of cybersecurity risks oblige the public institutions and enterprises to establish information security management systems.

In this study, methodology and tools covered under the Risk Management / Risk Assessment methodology and tools within the European Union Agency For Network and Information Security (ENISA)'s Threat and Risk Management studies are investigated. In the study, the seventeen methods and thirty one tools which are studied by ENISA on the inventory work are introduced on the basic level. The methods and tools are compared among themselves in different aspects such as the type of risk classification, the reference level, the definition of applicability, the lifecycle, the usage of them licensed.

Keywords - information security, cyber security, risk management, risk assessment

I. INTRODUCTION

The risk concept can be described as a circumstance which causes the ordinary flow to break down for any reason, at any time and causes waste of time-labour loss. In terms of information technologies, the fact almost all of today's business process and forms of work depend on partly automation systems based on information technologies makes the risks of information technologies unignorable. It is possible that loss and distortion in information assets related to information technologies lead to conclusions which ends up waste of time and labour loss.

Actions to be taken which are to ensure the integrity and correctness information assets which are processed in the sub-structures of information technologies can be ensured by improving the security requirements and business process of the sub-structure.

This requires the assessment of the foreseeable information security risks and the removing and managing the actions to be taken against these risks with a systematic approach and a sub-methodology.

An overview of the methodology and tools handled in the scope of Information Security Threat and Risk Management studies which are applied to the Europe Union (EU) countries in 2017 by European Union Agency for Network and Information Security (ENISA) related to information security risk assessment and management is brought out in this study.

II. METHOD

Cybercrime is also increasing in proportion to the increase in the number of users in the world [2]. This is not only because the increase in the abilities of the users, but also the increase of users who are not sufficiently informed and whose security can easily be violated.

In this study, national progress has been examined in the framework of the Protection of Personal Data Act, the Personal Data Protection Agency, and the Personal Data Protection Expertise Regulation which are on the agenda in our country.

In this study, national progress has been examined in the framework of the Protection of Personal Data Act, the Personal Data Protection Agency, and the Personal Data Protection Expertise Regulation which are on the agenda in our country.

Through the literature review, it has been found that especially the work on methodologies intensifies, the tools support one or more methodologies to support the application process of methodologies.

In the study, the data obtained from ENISA, the applications in our country and the ENISA inventory study are summarized and the models in the literature are briefly mentioned. Suggestions are made under the headings i) political, economic and educational ii) organizational practices ,in the light of the obtained and evaluated data.

III. RESULTS

A. European Union Agency for Network and Information (ENISA)

The ENISA – by its own definition in the annual reports- is a network and information security expertise center for the EU and the member countries, the private sector and European Citizens. The ENISA works for developing recommendations on good practices in the field of information security. It helps the EU member countries to implement the relevant EU legislation and works to improve the durability of Europe's critical information infrastructure and networks. The ENISA aims to develop the current expertise in the EU member countries by supporting the development of cross-border communities committed to promoting network and information security across the EU. This agency is in Greece and has offices in Creta and Athens [6, 7, 56].

Information security is a process which is required to be implemented in the overall information system, not in a single information technology unit. Thusly, an agency has been established across the EU and the EU agency has been established to promote good practise, to improve the critical infrastructure and to support the work in this field.

The ENISA -with the annual report it publishes- has informs and warns the countries around the EU on the cyber threats.

The diagram shown in figure 1 which is used to visualize the risk elements in the report is taken from ISO 15408:2005.

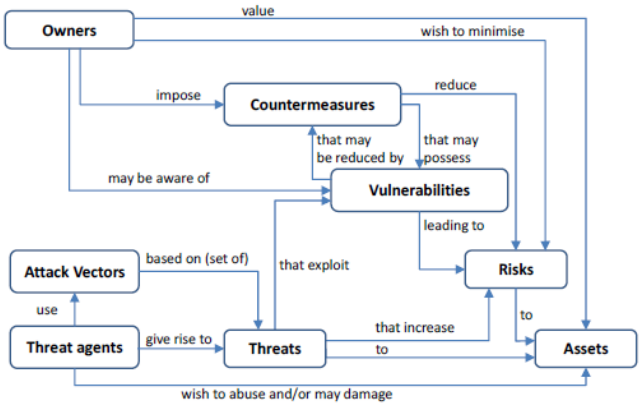

Figure-1: The risk elements and associations to ISO 15408:2005 in the ENISA 2017 report, it includes the threats listed in list-1 as the top 15 threats.

The threats in Table-1 are included as the top 15 threats in ENISA 2017 [7]

Table-1: The top 15 threats to the ENISA for 2017

SN	Cyber Threat
1	Malware
2	Web-Based Attacks
3	Web Application Attacks
4	Phishing
5	Spam
6	Denial of Service
7	Ransomware
8	Botnets
9	Insider Threat
10	Physical Manipulation, Damage, Theft, Loss
11	Data Breaches
12	Identity Theft
13	Information Leakage
14	Exploit Kits
15	Cyber-Espionag

For each of the mentioned threats, the description of the cyber threat, the focal point, the trends, the basic numerical indicators, the top 10 cases related to this thread, and the similar diagnostic information take place in detail in the report [7].

B. Protection of Personal Data Institution (PPDI)

The fact the establishment of PPDI with the publication of the Law No. 6988 on Protection of Personal Data in the Official Gazette dated 07/04/2016 and The Personal Data Protection Expertise Regulation published in the Official Gazette dated 09/02/2018 indicates that a number of current studies on information security have been carried out in our country.

Although, when the intent and content of the law are examined, it is mentioned that the purpose is to regulate the liabilities of natural and legal people which process the personal data and the procedures and principles of people which is required to obey, it is seen that - there is an emphasis on the content with the organization and function of PPDI- there is no mention about information security and management processes which is required to obey by institutions and legal person for the sake of protecting personal data and is required to be applied.Likewise, when the purpose and the content of the legislation are examined, it has been stated that the selection and appointment of Expert and Expert Assistance for Personal Data Protection is required and that these experts and expert assistants must have a bachelor's degree in social sciences [63, 67].

The booklets and guides in list-2 in 2018 are published by PPDI.

Table-2: PPDI booklets and guides

SN	Booklets / Guides
1	100 questions on personal data protection laws
2	Personal Data Security Guide (Technical and Administrative Measures)
3	Frequently Asked Questions About the Law on the Protection of Personal Data
4	Implementation Guide for the Protection of Personal Data
5	Guide to Personal Data Deletion, Destruction or Anonymization

When the booklets and guides are reviewed, it is seen that the protection of personal data is perceived as an administrative act and there is superficial information about a set of deletion, destruction and anonymization methods in just Personal Information Deletion, Destruction or Anonymization Guide [58-62].

C. Risk Assessment and Risk Management Methodology and Tools

Briefly-if the risk is defined as a possible negative situation- the risk analysis will be the realization conditions of that negativity while the risk management will be the measures to be taken to avoid these conditions happen and will be the simple but correct approach in the context of what to do if it happens.

Information is a salient asset for institutions and also reducing information security risks is an another salient issue [1].

Nowadays, there are risk analysis and management methods which that are accepted as standard and still in development.

The risk analysis methodologies conducted in the scope of ENISA's Threat and Risk Management studies are given in table-3, table-4 and table-5 [9, 17, 20, 22, 26-31, 33, 34, 36, 38, 40, 48, 52].

Table-3: Evaluation and management features of Risk Assessment and Management Methodologies

		Risk Assessment Method			Risk Management Method					
Methodologies	Origin	Identification	Analysis	Evaluation	Assessment	Treatment	Acceptance	Communication	Last Version/Date	Price
Austrian IT Security Handbook		X			X	X	X	X	v2.2 2004	free
Cramm	United Kingdom	X	X	X					v5 2003	unknown
Dutch A&K Analysis	The Netherlands	X	X	X					v1.01 1996	free
Ebios	France	X	X	X	X	X	X	X	r2	free

									2004	
ISAMM	Belgium								unknown	unknown
ISF Methods	ISF members	X	X	X	X	X	X	X	2005	membership
ISO/IEC 13335-2	International	X	X	X	X	X	X	X	2006	100 Euro
ISO/IEC 17799	International	X				X			v2 2005	200 Euro
ISO/IEC 27001	International	X			X	X	X		2005	130 Euro
IT-Grundschutz	Germany	X	X	X	X	X	X	X	2005	free
Magerit	Spain	X	X	X	X	X	X	X	v2 2005	free
Marion	France	X	X	X				X	1998	free
Mehari	France	X	X	X	X	X	X	X	2017	free
MIGRA	Italy								v2.1 2006	support fee
Octave	USA	X	X	X	X	X	X	X	v2.0 2005	free
RiskSafe Assessment	United Kingdom	X	X	X	X	X	X	X	v1.0 2012	support fee
SP800-30	USA	X	X		X	X	X		2002	free

When looking at the methodologies from table-3, it is seen that the definition based on the risk indicates the focus is on the improvement in terms of risk management.

Table-4: Target organization and level of implementation of Risk Assessment and Management Methodologies

	Target Organisations						Level of Detail		
Methodologies	Goverment and agencies	Large companies	SMEs	Commercial companies	Non-profit	Specific-sector	Management	Operational	Technical
Austrian IT Security Handbook	X	X	X	X	X		X	X	
Cramm	X	X					X	X	X
Dutch A&K Analysis	X	X	X	X	X		X	X	X
Ebios	X	X	X	X	X		X	X	
ISAMM	X	X	X	X	X		X	X	
ISF Methods	X	X		X	X		X	X	X
ISO/IEC 13335-2	X	X	X	X	X		X	X	
ISO/IEC 17799	X	X	X	X	X		X	X	
ISO/IEC 27001	X	X					X	X	
IT-Grundschutz	X	X	X	X	X		X	X	X
Magerit	X	X	X	X	X	X	X	X	X
Marion	X						X	X	
Mehari	X		X	X	NGOs, education, health, public services, etc.	X	X	X	X
MIGRA	X	X					X	X	X
Octave			X				X	X	
RiskSafe Assessment	X	X	X	X	X		X	X	X
SP800-30	X	X	X	X	X			X	X

When looking at the methodologies from table-4, it is seen that the target group of public and large enterprises and the level of implementation are administrative and operational.

Table-5: Competencies in Risk Assessment and Management Methodologies and compliance with IT standards

	Skills Needed			Compliance to IT Standards							
Methodologies	To introduce	To use	To maintain	ISO/IEC 13335-1	ISO/IEC 13335-2	ISO/IEC 17799	ISO/IEC 27001	ISO/IEC 27002	ISO/IEC 27005	ISO/IEC 15408	ISO/IEC 21827
Austrian IT Security Handbook	2	2	2	X	X	X					
Cramm	3	3	3			X					
Dutch A&K Analysis	1	2	1			X					
Ebios	2	2	2	X	X	X	X			X	X
ISAMM	2	2	2					X			
ISF Methods	3	3	3			X					
ISO/IEC 13335-2	2	2	2	X		X	X				
ISO/IEC 17799	2	2	2	X	X						
ISO/IEC 27001	3	2	2			X					
IT-Grundschutz	2	2	2			X	X				
Magerit	2	3	3	X	X	X	X			X	
Marion	1	2	1								
Mehari	2	2	2	X			X	X	X		
MIGRA	1	3	3				X	X	X		
Octave	2	2	2								
RiskSafe Assessment	2	2	3				X		X		
SP800-30	2	2	2								

1: basic, 2: standard, 3: specialist

When looking at the methodologies from table-5, it is seen that standard qualifications are often sufficient to implement the methodology, predominantly in accordance with ISO / IEC 17799 and ISO / IEC 27001 standards.

Particularly, various tools are used to support one or more methodologies in order to be able to consider risk analysis in a holistic approach.

The risk analysis tools used in the scope of ENISA's Threat and Risk Management studies are given in table-6 and table-7 [8, 10-16, 18, 19, 21, 23-25, 32, 35, 37, 39, 41-47, 49-51, 53-55].

Table-6: Evaluation and management features of Risk Assessment and Management Tools

				Risk Assessment Method			Risk Management Method			
Tools	Origin	Coverage	Support	Identification	Analysis	Evaluation	Assessment	Treatment	Acceptance	Communication
Callio	Canada	1	X		X		X		X	X
Casis	Belgium	1								
CCS Risk Manager	USA	2	X	X	X	X	X	X	X	X
CloudeAssurance	USA	2	X	X	X					X
Cobra	United Kingdom	1	X		X		X		X	X
Countermeasures	USA	2	X	X	X		X	X	X	X
Cramm	United Kingdom	1	X	X	X		X			X
EAR / PILAR	Spain	1	X	X	X	X	X	X	X	X
Ebios	France	1	X	X	X		X	X	X	X
GSTool	Germany	1	X	X	X		X	X	X	X
KRiO	Spain	1, 2, 3	X	X	X	X	X	X	X	X
ISAMM	Belgium	2								
Mehari Expert (2010) RM tool	France - Canada	2	X	X	X	X	X		X	X
MIGRA Tool	Italy	1	X	X	X	X	X	X	X	X
Modulo Risk Manager	Brazil	2	X	X	X	X	X	X	X	X
Octave	USA	3	X	X	X		X	X		X
Proteus	United Kingdom	2	X	X	X	X	X	X	X	X
Ra2	Germany	1	X	X			X		X	X
REAL ISMS	USA	2								
Resolver Ballot	Canada	2								
Resolver Risk	Canada	2								
Risicare	France	2	X	X	X	X	X		X	X
Riskwatch	USA	1	X	X	X		X	X		X
RM Studio	Iceland	1,2, 3	X	X	X	X	X	X	X	X
SISMS	Turkey	2	X	X	X	X	X	X	X	X

TRICK Light	Luxembourg	1,2,3	X	X	X	X	X	X	X	X
TRICK Service	Luxembourg	1,2,3	X	X	X	X	X		X	X
Acuity Stream	United Kingdom	2	X	X	X	X	X	X	X	X
Axur ISMS	USA	2								
WCK	Israel	1,2,3								
CyberWISER Light	Europe	2	X	X	X	X				X

1: local, 2: world-wide, 3: regional

When looking at the tools at the figure-6, it is seen that they are mostly local and regional and they are promoter with being developer. It is seen that in terms of risk assessment almost all of them are supporting identification, analysis and development while is based on communication in terms of risk management.

Table-7: Risk Assessment and Management Tools, target organization and level of implementation

		Target Organisations						Level of Detail		
Tools	Last Version Date	Goverment and agencies	Large companies	SMEs	Commercial companies	Non-profit	Specific-sector	Management	Operational	Technical
Callio	v2 2005	X	X	X	X	X				
Casis			X	X						
CCS Risk Manager		X	X	X	X	X		X	X	X
CloudeAssurance	v1.3 2014	X	X	X	X	X	X			
Cobra	v3			X	X					
Countermeasures	v8 2006	X	X				X			
Cramm	v5.1 2005	X	X	X						
EAR / PILAR	v3.3 2006	X	X	X	X	X	X	X	X	X
Ebios	v2 2004	X	X	X	X	X				
GSTool	v3.1 2004	X	X	X	X	X				
KRiO	2016	X	X	X	X	X				
ISAMM	2008							X	X	X
Mehari Expert (2010) RM tool	2016	X	X	X	X	X	X	X	X	X
MIGRA Tool	v2 2007	X	X					X	X	X
Modulo Risk Manager	v5.0 2007	X	X	X	X	X		X	X	X
Octave		X	X	X	X	X				
Proteus	2007	X	X	X			X	X	X	
Ra2	v1.1 2005		X	X	X	X				
REAL ISMS	v1.2 2008	X	X	X	X	X	X	X	X	X
Resolver Ballot	v6.0 2008	X	X	X	X	X	X	X	X	
Resolver Risk	v6.0 2008	X	X	X	X	X	X	X	X	X
Risicare	v6.0 2007	X	X	X	X	X	X	X	X	X
Riskwatch	v9 2002	X	X	X	X	X				
RM Studio	v5.1 2016	X	X	X	X	X	X			
SISMS	v1 2011	X	X	X	X	X		X	X	X
TRICK Light	v1.3 2012	X	X	X	X	X	X	X	X	X
TRICK Service	v2.0 2017	X	X	X	X	X	X	X	X	X
Acuity Stream	v1.6.11 2011	X	X	X			X	X	X	X
Axur ISMS	v1.0 2008	X	X	X	X	X		X	X	X
WCK	v2.44 2013	X	X	X						
CyberWISER Light		X	X	X						

When looking at the tools from table-7, it is seen that almost all of the public and large-scale enterprises are targeted and the level of application is administrative and operational.

D. Sample Risk Analysis and Management Process

Security is a process which starts with the realization of the need for security. As the need for security has been recognized and addressed as part of business processes, it has been described as a series of processes and a security system can be modeled.

Organizations should define the criteria to be used to assess the importance of risk. Criteria should reflect the values, objectives and resources of the organization [64].

The goals of the risk analysis process should help to supply a dynamic set of tools with identifying new threats and weak points, anticipating business activity and checking the level of security of the information systems in information system safety [66].

Cyber-physical security systems are real-time, stand-alone, robust systems with high performance requirements [57]. A sample process plan is given in table-8. This process can be extended to the application requirements.

Table-8: A sample security model for cyber-physical systems

Risk Management Context
1: Identify the system and components and existing risk management practice 2: Determine goals and key performance indicators (KPI) 3: Risk acceptance level
Assets Identification and Criticality
1: Criticality identification 2: Asset weight
Vulnerability Assessment and Threat Identification
1: Vulnerability Impact Rating 2: Asset Vulnerability Impact Assessment Model (A-VIAM) 3: Identify threats
Risk Assessment
1: Generate cyber-security attack scenario 2: Determine the likelihood of a cyber-security attack scenario 3: Attackers' skill and location 4: Determine the impact of the cyber-security attack scenario 5: Identify the risk level
Risk Control
Risk Monitor and Residual Risk

The easiest approaches to implement in security management; i) do not do anything when the accepted risks occur, ii) avoid the emergence of threats, iii) reduce the possibility of the threat, iv) reduce the effect when the threat occurs [3].

When we look at the security model only from the perspective of information security, a two-part model which is composed of modeling and analysis can be used, as well [4].The main headings for this model are shown in List-9.

Table-9: A sample security model for cyber systems

Social modeling: identification of use cases of hardware, software and systems as information assets.
Entity modeling: Classification of the entire information assets used as direct and indirect and management of them.
Authority modeling: Use of assets and determination of user authorizations.
Threat modeling: Determination of possible threats through risk analysis.

In terms of an enterprise, risk is generally considered to be a commercial approach.In the past, security risks were caused by commercial loss and ignored due to fact that the probability of occurrence was low. Nowadays, cyber risks are an important part of agenda for every company, but they are inadequate in practice due to lack of reliable data and analysis [5]. Risk analysis, risk assessment and risk assessment definitions vary for each of the selected analyzes [65].

IV. SUGGESTIONS

A. Political, economic and educational

Information security is one of the main components of the industry 4.0 as seen as the next generation of industry, and therefore it is a field to be invested in- not being ignored -in terms of politics, economics and education.

Risk assessment and risk management processes should be convert into publicly supported sectoral policy. This will ensure the determination of standards for qualifications for businesses at the point of enforcement of the Law on the Protection of Personal Data.

Cyber security is a global issue, not a national issue, since there are is border in cyber space. However- in practice- each country has its own standards will ensure the development of the cyber security issue quickly.The fact that our country has its own standards in this respect will enable us to become the country which has an economic impact in the process and has a say in international standards at the end of the process.

The fact that the information assets are already above the manageable level in terms of many enterprises, this provides predictable information for the required fields of education and employment.

Appropriate staff training and employment projects should be initiated by meeting essential sectoral needs and supplying communication between educational institutions due to the fact that information security sector is a new developing field.

B. Organizational

The obligation for implementing information security standards will ensure that organizations are lead to protect their personal information assets as well as their personal information.

Making the information security management of the organizations integrated with the network management artificial intelligence assisted will reduce the application costs to a minimum.

The fact critical infrastructure enterprises facing with compelling sanction on cyber security infrastructures will cause increased service continuity.

It is possible to increase the integrity and verifiability capacities of the individual information owned by the organizations, or the technologies based on the block chain of other information assets.

REFERENCES

[1] Agrawal, V. (2015). A Comparative Study on Information Security Risk Analysis Methods, Journal of Computers (12), 57-67, DOI: 10.17706/jcp.12.1.57-67

[2] Akinwumi, D.A., Iwasokun, G.B., Alese, B.K., Oluwadare, S.A. (2017). A Review of Game Theory Approach to Cyber Security Risk Management, Nigerian Journal of Technology (NIJOTECH) (36), 1271-1285, DOI: 10.4314/njt.v36i4.38

[3] Chmielecki, T., Cholda, P., Pacyna, P., Potrawka, P., Papacz, N., Stankiewicz, R., Wydrych, P. (2014). Enterprise-oriented Cybersecurity Management. Proceedings of the 2014 Federated Conference on Computer Science and Information Systems (2), 863-870, DOI:10.15439/2014F38.

[4] Dashti, S., Giorgini, P., Paja, E. (2017). Information Security Risk Management, International Federation for Information Processing 2017, 18-33, DOI: 10.1007/978-3-319-70241-4_2.

[5] Eling, M., Wirfsi J.H. (2015). Modelling and Management of Cyber Risk, IAA Colloquium 2015.

[6] ENISA. (2017). ENISA Threat Landscape Report 2016. DOI: 10.2824/92184.

[7] ENISA. (2018). ENISA Threat Landscape Report 2017. DOI: 10.2824/967192.

[8] ENISA. (2017). Acuity Stream. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_stream.html

[9] ENISA. (2017). Austrian IT Security Handbook. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_au_it_security_handbook.html

[10] ENISA. (2017). Axur ISMS. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_axur.html

[11] ENISA. (2017). Callio. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_callio.html

[12] ENISA. (2017). Casis. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_casis.html

[13] ENISA. (2017). CCS Risk Manager. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_ccs.html

[14] ENISA. (2017). CloudeAssurance. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_cloudeassurance.html

[15] ENISA. (2017). Cobra. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_cobra.html

[16] ENISA. (2017). CounterMeasures. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_countermeasures.html

[17] ENISA. (2017). CRAMM. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html

[18] ENISA. (2017). Cramm. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_cramm.html

[19] ENISA. (2017). CyberWISER Light. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_wiser.html

[20] ENISA. (2017). Dutch A&K Analysis. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_dutch_ak_analysis.html

[21] ENISA. (2017). EAR/PILAR. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_EAR_Pilar.html

[22] ENISA. (2017). EBIOS. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_ebios.html

[23] ENISA. (2017). Ebios. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_ebios.html

[24] ENISA. (2017). GSTool. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_gstool.html
[25] ENISA. (2017). ISAMM Tool. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_isamm.html
[26] ENISA. (2017). ISAMM. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_isamm.html
[27] ENISA. (2017). ISF Methods. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_isf_methods.html
[28] ENISA. (2017). ISO/IEC 13335-2. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_iso133352.html
[29] ENISA. (2017). ISO/IEC 17799. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_iso17799.html
[30] ENISA. (2017). ISO/IEC 27001. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_iso27001.html
[31] ENISA. (2017). IT Grundschutz. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_it_grundschutz.html
[32] ENISA. (2017). KRiO. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_gxsgsi.html
[33] ENISA. (2017). Magerit. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_magerit.html
[34] ENISA. (2017). Marion. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_marion.html
[35] ENISA. (2017). Mehari Expert (2010) RM Tool. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_mehari.html
[36] ENISA. (2017). Mehari. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_mehari.html
[37] ENISA. (2017). MIGRA Tool. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_migra.html
[38] ENISA. (2017). MIGRA. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_migra.html
[39] ENISA. (2017). Modulo Risk Manager. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_modulo.html
[40] ENISA. (2017). Octave. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_octave.html
[41] ENISA. (2017). Octave. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_octave.html
[42] ENISA. (2017). Proteus. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_proteus.html
[43] ENISA. (2017). Ra2. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_ra2.html
[44] ENISA. (2017). Real ISMS. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_real.html
[45] ENISA. (2017). Resolver Ballot. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_resolver_ballot.html
[46] ENISA. (2017). Resolver Risk. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_resolver_risk.html
[47] ENISA. (2017). Risicare. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_risicare.html
[48] ENISA. (2017). RiskSafe Assessment. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_risksafe-assessment
[49] ENISA. (2017). Riskwatch. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_riskwatch.html
[50] ENISA. (2017). RM Studio. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_rm_studio.html
[51] ENISA. (2017). SISMS. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_sisms.html
[52] ENISA. (2017). SP800-30. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_sp800_30.html
[53] ENISA. (2017). TRICK Light. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/trick-light
[54] ENISA. (2017). TRICK Service. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_trick_service.html
[55] ENISA. (2017). WCK. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_wck.html
[56] ENISA. (2018). About ENISA. Date of Access: 15/08/2018, https://www.enisa.europa.eu/about-enisa
[57] Kure, H.I., Islam, S., Razzaque, M.A. (2018). An Integrated Cyber Security Risk Management Approach for Cyber-Physical System, Applied Science, 8-898, DOI: 10.3390/app8060898.
[58] KVKK (2018). 100 Soruda Kişisel Verilerin Korunması Kanunu, Ankara: KVKK Yayınları.
[59] KVKK (2018). Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler), Ankara: KVKK Yayınları.
[60] KVKK (2018). Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular, Ankara: KVKK Yayınları.
[61] KVKK (2018). Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, Ankara: KVKK Yayınları,
[62] KVKK (2018). Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi, Ankara: KVKK Yayınları.
[63] KVKK (2018). Kişisel Verileri Koruma Uzmanlığı Yönetmeliği, Resmi Gazete, Resmi Gazete (30327).
[64] Marija, M., Ivan, B., Dusan, R. (2015). Supply Chain Risk Management Using Software Tool, Acta Polytechnica Hungarica (12), 167-182.
[65] Pan, L., Tomlinson, A. (2016). A Systematic Review of Information Security Risk Assessment, International Journal of Safety and Security Engineering (6), 270-281. DOI: 10.2495/SAFE-V6-N2-270-281.
[66] Sadok, M., Katos, V., Bednar, P.M. (2014). Developing Contextual Understanding of Information Security Risk, Proceedings of the Eighth International Symposium on Human Aspects of Information Security & Assurance (HAISA).
[67] TBMM (2016). 6988 Sayılı Kişisel Verilerin Korunması Kanunu, Resmi Gazete (29677).