# A framework for the information classification in ISO 27005 standard

Vivek Agrawal
Department of Information Security and Communication Technology
Norwegian University of Science and Technology, NTNU
Gjøvik, Norway
Email: vivek.agrawal@ntnu.no

***Abstract*—Information Security Risk Management (ISRM) process involves several activities to conduct a risk management (RM) task in an organization. ISRM activities require access to various information related to the organization. An organization often needs to share information related to an ISRM process with the stakeholders involved in the activity. Therefore, it is important to manage the information which is critical to the operations of the organization. The presence of an information classification scheme can enable the proper handling of the information involved in the RM task. We selected ISO/IEC27005:2011 risk management standard to assess various information generated during the process of applying this standard in an organization. The purpose of this study is to propose a framework to show various information objects involved in ISO27005 risk management standard and classify the information based on the guideline provided by UNINETT scheme. A case scenario of a health clinic is developed to identify ISRM related information objects using the proposed framework and classify the information using UNINETT scheme.**

***Index Terms*—information classification; information security; ISO27005; risk management**

## I. Introduction

ISO 27005 is a well-known Information Security Risk Management (ISRM) standard. The tasks in ISO27005 include the identification, assessment, and prioritization of risk. ISRM should be an endlessly recurring process consisting of phases which, when properly implemented, enable continuous improvement in decision-making and performance improvement [2]. The ISO27005 process involves various information related to the organization. An organization creates, collects, and processes a significant amount of information in multiple formats during the information security risk management activity. Sometimes, it is required to share the information of risk management tasks with other stakeholders so that they can collaborate in the risk management activities. Therefore, it is important for the organization to identify the information that should be protected, the level of protection that should be provided. An organization cannot share everything as it may include confidential information that can ruin the reputation or normal functioning if it is disclosed to the malicious entity. The organization has the responsibility to protect this information and ensure its confidentiality, integrity, and availability. Information classification plays a vital role in storing and sharing sensitive information across the organization. Information classification can help an organization to meet legal and regulatory requirements for retrieving a given information within a specific time frame [6]. The information classification activity enables classification of information on sensitivity and importance, and to define storage periods and rules for disposal. In this study, we presented a framework for ISO27005 to represent the processes in the standard using input and output of the activities involved. A case scenario of a health clinic is presented to represent a real-world scenario where ISRM task is to be performed. Later, we used the proposed framework to identify significant information that will be involved in carrying out ISRM task in the health clinic. Afterward, the identified information is classified using the UNINETT scheme [9]. We are particularly interested in answering the following research questions in this study:

*RQ1) How to identify information objects in an organization that will be required in ISRM tasks?*
*RQ2) How can the information objects ISRM be classified in an ISRM task?*

The main contributions of this study are - a) to provide a framework for ISO27005:2011 to highlight various information associated at each step of the standard; b) present a case scenario of a health clinic to establish the relevance of the proposed framework in the real-world scenarios; c) classify the information in the health clinic using the proposed framework of ISO27005 and UNINETT classification scheme.

The structure of the paper is as follows: Section II provides an overview of information classification concept and creates the foundation for this study. Section III includes a list of work that identified the necessity of information classification in ISRM standards and proposed the classification schemes. Section IV presents the proposed framework for ISO27005:2011 standard to identify various input, output in each activity of ISRM process. Section V presents an overview of UNINETT scheme. Section VI presents a fictitious scenario of a health clinic, the application of ISO27005 framework and UNINETT scheme. Section VII presents a discussion on the findings of this study. The paper ends with research limitations and future work in section VIII.

## II. Background knowledge

This section provides necessary information on information classification and motivates the purpose of carrying out this

study.

### A. What is information classification?

Information classification is the classification of information based on its level of sensitivity and the impact to the organization if the information is disclosed, altered, destroyed without authorization. The classification of information eases the task of deciding the security controls to safeguard the information. Information classification is not only just presenting information in the form of a data file or database but also includes the associated system and user documentation, operational and support procedures, training materials, and disaster recovery plans [18]. Information classification helps to establish baseline security controls to safeguard information. There are several definitions [19], [6] of information classification presented by researchers and institutes. However, we are interested in using the information classification scheme that must suggest appropriate practices related to labeling the information, storing information, transmitting information, disposing of the information, retaining the information. Therefore, UNINETT classification scheme [9] is chosen to carry out this study as this scheme covers the information classification and handling rules.

### B. Why should ISRM information be classified?

There are many reasons why an organization must be concerned about information classification of various information objects related to an ISRM process [6]. The possible reasons are as follows:

**Protecting confidential information** - In an ISRM process, certain information must remain confidential. Examples of such information include the information related to potential vulnerabilities, annual provincial budget. A competitor can fetch this information in the absence of any information classification scheme and can misuse the information. Applying proper security classification and practices can safeguard against unauthorized access to confidential information.

**Contractual commitment** - Some companies also have contractual commitments to protect information according to customer or business partner specifications. There are many stakeholders (e.g. customer, owner, partner) involved in an ISRM process in an organization. A company can avoid the risk of financial penalties by complying with the regulatory and legal requirements.

**Regulatory mandates** - It is vital to meet the regulatory mandate in some countries and some sector of business. For instance, the Gramm Leach Bliley and the Health Insurance Portability and Accountability Acts mandate information protection controls for financial and medical organizations respectively. As ISRM process includes various sensitive information related to the organization and its client, it becomes eligible for the special information handling requirements.

**Competitive advantage** - An organization that follows a proper information classification scheme consistently can get an edge over companies who have not incorporated information classification as seriously.

## III. Related Work

Information classification is not a new concept for an organization dealing with sensitive information. However, many organizations still struggle to establish their information classification [8], [7], [14], [20] schemes. Park et. al [16] conducted a survey of information security management systems (ISMS) in 5 hospitals with more than 500 beds. A checklist is designed according to the international standards ISO/IEC 27001; 17799, JIS Q 15001. The checklist collects information related to the medical information security policy, asset management, human resource security, access control, etc. The outcome of the survey reveals that asset management and information classification were the most vulnerable part of the ISMS. There was little classification guidelines to establish countermeasures for information security management in hospitals. The Health Service Executive (HSE) released a document [13] in the year 2013 on information classification in Ireland. HSE created a mandatory policy for its staff, students, contractors, sub-contractors, agency personnel and third parties who have access to HSE information. According to the policy, all information owned, created, received, stored and processed by the HSE must be classified as, *Public*, *Internal*, *confidential*, *restricted*. According to Information Classification Policy of ISO/ IEC 27001: 2005, a company must ensure appropriate level of protection for information assets. Information assets can be classified according to the information classification system i.e. *unclassified public*, *Proprietary*, *Client Confidential Data*, *company confidential data*. The main objective of information classification is to ensure that business assets are properly handled [19]. An organization must identify and classify any private information that it retains. The author in [19] recommended considering the role of people who can access the information, the availability of information, the length of time the given information will be retained. Etges et al. [5] mentioned that the primary objective of information classification should be based on the business processes. It is important to understand the how much a given piece of information is critical to its business processes. An information classification exercise must start with a high-level business impact analysis (BIA). The outcome of a BIA specifies the most critical business process. Using the information gather from the outcome of BIA, the information systems and infrastructure components that support those business processes can be easily comprehended. The information identified in the above task must be processed through business and security requirements. A given information must be structured using data classes, ownership, and requirements.

## IV. ISO/IEC27005 standard

### A. Overview of ISO27005

ISO27005 was prepared by Joint Technical Committee ISO/IEC_JTC1, Information Technology, subcommittee SC 27, IT Security Techniques. ISO27005 standard provides guidelines for information security Risk Management. This standard builds on the knowledge concepts, models, processes

and terminologies of ISO/IEC 27001 [11]. It assists implementation by taking a risk management approach. The first step consists of context establishment which includes determining the objectives of the organization, specifying the basic criteria (e.g. setting risk evaluation criteria, risk acceptance criteria), outlining the scope and boundaries of information security risk management, among others. The risk assessment consists of Risk Identification, Risk analysis, and risk evaluation. In the risk identification step, the assets and their owners are identified. It is followed by the identification of the threats to those identified assets, the existing and planned controls, the vulnerabilities that might be exploited and a record of incident scenarios with their impacts related to those identified assets. Risk analysis step takes either qualitative or quantitative approach to assessing the consequences and the likelihood of occurrence of relevant incidents. In the risk evaluation step, the identified risks are prioritized according to the risk evaluation criteria about the incident scenarios that lead to those risks. If the result of the risk assessment step is satisfactory, then the risk treatment options are selected. Risk treatment options are selected based on the outcome of risk assessment, the expected cost of implementing these options and the expected benefits from these options. The risks are retained when the level of risk satisfies the risk acceptance criteria. Risk communication and consultation step ensure exchange/ sharing of information between the decision-maker and other stakeholders throughout the risk management process. Similarly, risks and their factors i.e. the value of assets, impacts, threats, vulnerabilities and the likelihood of occurrence should be monitored and reviewed to identify and changes in the content of the organization at an early stage.

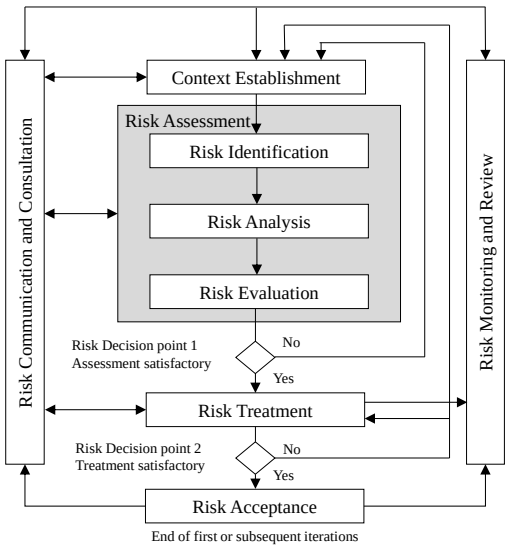


Fig. 1. Overview of ISO27005, taken from [12]

### B. Proposed Framework

The objective of this section is to answer the research RQ1. A framework is presented to show various information objects involved in ISO27005 risk management standard. The representation of ISO27005 standard using the input and output at each activity is shown in the Figure 2. The whole process in ISO27005 is presented into six essential activities (A1-A6). The activity uses some inputs I.*m.n* and produces a number of outputs O.*m.n*, where m denotes the activity no. and n denotes the step. This framework of ISO27005 helps identifying potential information (in the form of input and output) that are needed to conduct the risk management task. The first activity (A1) i.e. *Context Establishment* takes previous risk assessments report and other important information related to the organization e.g. financial, budget planning, IT goals planning, resource requirements, etc. as an input and produces Risk evaluation criteria, impact criteria, scope and boundaries, and different roles and responsibilities of the associated stakeholders in the organization. The output (O.1.1-O.1.5) of the activity (A1) is fed as the inputs (I.2.1-I.2.5) in activity A2. Similarly, A3, A4, A5, and A6 have such information that is available in the form of input and output in the figure 2 .

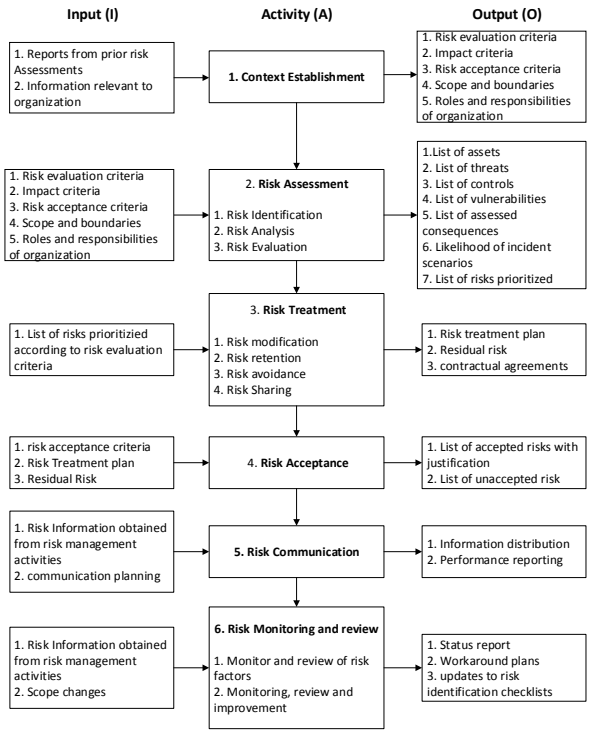


Fig. 2. Overview of ISO27005 standard based on input, output of each activity

## V. UNINETT CLASSIFICATION SCHEME

UNINETT classification scheme is proposed by UNINETT led working group on information security in 2013 [9]. The scheme is developed to identify and classify the institution's information objects. The classification is done on the basis of sensitivity and critical value of the information. The aim of this work is not to validate the UNINETT scheme, but

to establish a classification scheme that is suitable for the information objects in ISO27005 risk management related tasks. The original scheme contains thirteen classification categories where as we adopted only seven categories in this work. The seven categories of the scheme are given as follows:

**Unrestricted data**: An organization can decide to share their information with others so that it can be used to provide other better services. The shared data can be used by the research organization, industry to extract other meaningful information from it. This information can include survey data, annual business report, organizational models, output report of the previous incident handling the task. It is also important for the organization to share the data in machine-readable formats so that it can be accessible by the other agencies properly. The government of Norway has produced a guideline for disclosure of public data. The guideline describes how the published data can be legally used and how it must be published (structure, format) [15]. In this study the unrestricted data is marked with either ***OPEN*** or ***CLOSED***. ***OPEN*** signifies that the given information can be available for the public use, ***CLOSED*** signifies that the information is critical for the business and must not be made available to the public.

**Security classification**: It is the level of protection that is needed for the information object. Security classification controls should consider the organizational needs for sharing or restricting the information and the consequences that it can case if the information is not handled properly. In this study the possible controls under security classification are: a) ***OPEN*** - The information can be accessed by the internal members of the organization and external agencies without having any special access rights, b) ***INTERNAL*** - The information can be accessed by both internal members of the organization and the external agencies only in the presence of controlled access rights, c) ***CONFIDENTIAL*** - Information can only be accessed by the internal members of the organization with controlled access rights.

**Security requirement**: The requirement can be formed based on the nature and value of the information. The requirement consists of ***Confidentiality (C)*** - It refers to the ability to protect the information from those who are not authorized to access it, ***Integrity (I)*** - It refers to the ability to prevent information from being changed in an unauthorized or undesirable manner, ***Availability (A)*** - It refers to the ability to access the information when and where it is needed. The combination of C, I, and A is also known as CIA triad [3].

**Preservation value**: Preservation value signifies that information holds relative value/importance for the organization. The information can have ***LEG*** - The information that has Legal value can be used anytime to solve a legal dispute, ***ENT*** - The information that has enterprise-critical value is useful for carrying out day-to-day activities of the organization, ***HIST*** - The information with historical value usually kept for permanent or extended long-term basis.

**Personal Information**: It defines to what extent a given information can be linked to an individual. The objective of this component of the classification is to protect the privacy of the persons through the processing of personal information. There are several acts present to protect the personal information. Under EU law, one can legally collect personal information only under strict condition provided that it will be used for a legitimate purpose. The article 1 of BSI Act on the Federal Office [4] mentions that personal data can also be used beyond the specified implementation if there is any suspicion that the information could contain malicious software. The present study defines the personal information into, a) ***Personal (P)*** - It refers to the information that can be associated to an individual, b) ***Sensitive Personal (S)*** - It refers to the information related to health, religious belief, racial or ethnic region, etc [17].

**Storage period**: The information object must have a period of which it will be kept in the organization. The storage period is defined when an information object is created/ defined. The storage period is defined into, a) ***PERMANENT (PERM)*** - The information object will be stored in the database permanently, b) ***LIFETIME-RELATED (LT)*** - The information object is attached to other objects, i.e. projects, contract, c) ***NN years*** - The storage period is defined explicitly in terms of number of years.

**Disposal**: It is important to get rid of the information properly at the end of the storage period. The disposal rules that are applied in this study are as follows: a) ***REVIEW (REV)*** - The information is sent to the owner of the information to review at the end of the storage period, b) ***DESTROY*** - the information is erased securely at the end of storage period, c) ***DEPOSIT*** - The information is saved in the archive at the end of storage period, d) ***KEEP*** - The information which is eligible for the permanent storage.

## VI. Case scenario of a health clinic

The purpose of this section is to answer the research question RQ2. A fictitious case scenario of a health clinic [2] is presented. The information relevant to the activities A1-A3 of ISO27005 standard is identified for the health clinic. Afterward, the identified information is classified using UNINETT scheme.

The health clinic is responsible for providing healthcare services to the citizen. They host general practitioners (GP) in their clinic. The organizational structure of the health is composed of a CEO, an HR manager and an IT expert. There are 22 staff consists of 18 doctors (9 male, 9 females), 2 ladies at reception, 2 nurses work in the clinic. The task of these receptionists is to provide information related to doctors, (e.g. appointment date, details). They are also responsible to register a new patient in the health system. The clinic uses the IT services in the form of email server, file server, patient records, billing database, medical records. The printers are used to print out document related to patients treatment. It is possible to book an appointment through website and SMS. The IT strategy and information security policy is outdated. The last modification took place in 2010. An attacker can try to gain access to the healthcare system to steal personal information of a patient (patient record). Receptionist uses preferably simple

password to log into the system. The scenario of the health clinic is represented as a Data flow diagram (DFD) in the figure 3.

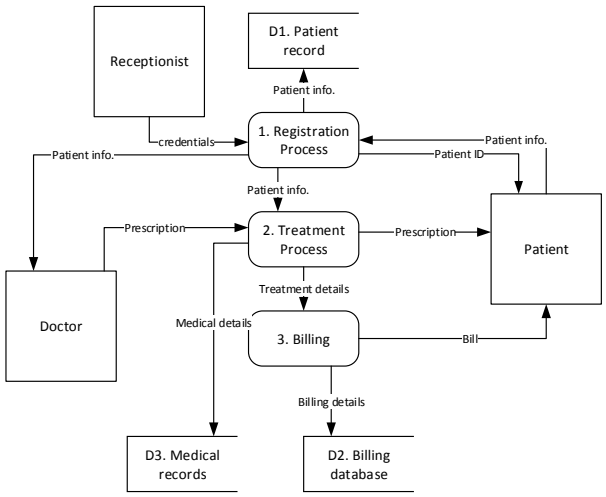


Fig. 3. Data flow diagram of the health clinic

### A. Application of ISO27005 framework

In this section, the ISO27005 framework is used to identify all the important information that will be generated in the activities A1-A3, see Table I. The details of the activities in A4-A6 are not shown in the paper due to space limitation. The information in the table I will be classified using UNINETT scheme in the next section. The information object in the table I can be identified in the figure 2 through the ***Tag*** column used in the table. The tag column also shows that if given information object is used as input or output or both.

### B. Application of UNINETT scheme

In this section, we apply UNINETT information classification scheme [9] to the various risk management information objects identified in the health clinic scenario under table I. The classification of the information objects using the UNINETT scheme is presented in Table II.

## VII. Discussion and Conclusion

The present study proposes a framework for ISO27005 in figure 2 that can be used to identify information objects involved in a risk management task in an organization. A case scenario of health clinic is mentioned to present a real-world scenario where we can use the proposed framework to discover necessary information required in the ISRM task in the table I. The information associated with the ISRM task of health clinic is further classified using the UNINETT scheme in the table II.

The classification presented in the table II is specific to the case scenario presented in this study. For instance, patient database is a potential *asset* in the health clinic scenario. Typically, a patient database contains very sensitive data of the patient. It contains family history, habits, family history, details of physical examination, medical test results. The information present in the database is sufficient to uniquely identify the person. The leakage of this information to unauthorized party can reveal the most sensitive information of the patient. It is a direct breach of the privacy as well as confidentiality of the patient. North Carolina Healthcare Information and Communication Alliance defines privacy as "'An individuals right to control the acquiring, use or release of his or her personal health information"' [10]. United States law mandates that medical devices meet the privacy requirements of the 1996 Health Insurance Portability and Accountability Act, HIPAA. The *list of control* includes updated security policy, details of the encryption used in the health clinic. This information is kept OPEN so that relevant authorities can read it and improve it. Secondly, it is also important for the patient to have knowledge about the security policy of the health clinic so that they can monitor their privacy. The information under the *list of vulnerability* is critical to the business. Therefore, it must not be released outside the organization. A potential attacker can exploit this vulnerability through a sophisticated mean and implant eavesdropping, routing, spoofing attacks [1]. The contractual agreement has a legal value and must be retained in the organization. The information available in the agreement will be required to settle any financial or operational dispute.

TABLE I
Items and instances based on the case scenario of health clinic

| Tag | Object | Instances based on case study |
|---|---|---|
| I.1.1 | Reports | risk analysis report from 2016 |
| I.1.2 | Organization | profile of staff Annual expenditure, medical service method, financial details |
| O.1.1/ I.2.1 | Risk Eval. | System uptime requires 99.9% of availability |
| O.1.2/ I.2.2 | Impact | A single case of information leakage with the impact of fine more than 250k USD |
| O.1.3/ I.2.3 | Risk accep. | Any event that may result into the loss of up to 250K USD can be accepted |
| O.1.4/ I.2.4 | Scope | The Information security policy of NIST |
| O.1.5 | Roles | doctors, nurses, specialists, insurance, pharmacy, patient, lab staff |
| O.2.1 | Asset | Patient database, treatment process, doctors, medical equipment |
| O.2.2 | Threat | Brute Force, DDOS, data corruption, failure of medical equipment |
| O.2.3 | Control | updated security policy, strong encryption and hash algorithm |
| O.2.4 | Vulnerability | outdated security policy, simple password used by receptionist |
| O.2.5 | Consequence | loss of patient's data, lawsuit against organization |
| O.2.6 | Likelihood | qualitative : very low, low, medium, high, very high; quantitative: range in numbers |
| O.2.7/ I.3.1 | Risk | database corruption, denial of service |
| O.3.1/ I.4.2 | Treatment | develop and maintain a set of policies to support IT strategy |
| O.3.2/ I.4.3 | Residual | Logical attacks: unauthorized user trying to break into the systems |
| O.3.3 | Contractual | Contract with an insurance company to counter act of nature or any other physical hazards |

## VIII. Limitation and future work

The information objects that are presented in Figure 2 are collected through literature review and discussion with the information security risk practitioners. Therefore, it is possible

TABLE II
INFORMATION CLASSIFICATION OF ISO27005 USING UNINETT SCHEME

| Tag | Information | Unrestricted data | Security classification | Security requirement | Preservation value | Personal information | Storage period | Disposal |
|---|---|---|---|---|---|---|---|---|
| I.1.1 | Reports from prior risk assessments | OPEN | OPEN | I | HIST | - | PERM | KEEP |
| O.1.1/ I.2.1 | Risk evaluation criteria | CLOSED | Internal | CIA | ENT | - | LT | REV |
| O.1.2/ I.2.2 | Impact criteria | CLOSED | Internal | CIA | ENT | - | LT | REV |
| O.1.3/ I.2.3 | Risk acceptance criteria | CLOSED | Internal | CIA | ENT | - | LT | REV |
| O.1.4/ I.2.4 | Scope and boundaries | OPEN | OPEN | I | ENT | - | LT | REV |
| O.1.5 | Roles and responsibilities of organization | OPEN | OPEN | I | ENT | P | LT | REV |
| O.2.1 | List of assets | CLOSED | Confidential | CI | ENT | S | LT | REV |
| O.2.2 | List of threats | CLOSED | Confidential | CI | ENT | P | LT | DESTROY |
| O.2.3 | List of controls | OPEN | OPEN | IA | ENT | - | LT | REV |
| O.2.4 | List of vulnerabilities | CLOSED | Confidential | CI | ENT | P | LT | DESTROY |
| O.2.5 | List of assessed consequences | CLOSED | Confidential | CI | ENT, HIST | P | LT | DESTROY |
| O.2.6 | Likelihood of incident scenarios | CLOSED | Confidential | CI | ENT | - | LT | DESTROY |
| O.2.7/ I.3.1 | List of risks prioritized | CLOSED | Confidential | CI | ENT | - | LT | DESTROY |
| O.3.1/ I.4.2 | Risk treatment plan | CLOSED | Internal | CI | ENT | - | LT | DEPOSIT |
| O.3.2/ I.4.3 | Residual risk | CLOSED | Confidential | CI | ENT, HIST | - | LT | DESTROY |
| O.3.3 | Contractual agreements | OPEN | OPEN | I | LEG | - | PERM | KEEP |

to have some information objects in ISO27005 which are missing in this study. However, the study can serve as a good starting point for the people who are engaged in the ISRM activity and decision-making in the organization. The future work will involve the security risk practitioners in the health department in Norway to participate in the classification activity. They will be given the ISO27005 framework to identify the information objects in their organization. We will propose the classification of the information objects based on the UNINETT scheme.

## IX. ACKNOWLEDGMENT

This study is a part of UnRizkNow project, which is partially funded by CCIS. The author would like to thank Prof. Einar Arthur Snekkenes for his suggestions and mentoring on creating the framework of ISO27005 risk management standard to identify different information objects.

## REFERENCES

[1] Vivek Agrawal. *Security and Privacy Issues in Wireless Sensor Networks for Healthcare*, pages 223–228. Springer International Publishing, Cham, 2015.

[2] Vivek Agrawal. Towards the Ontology of ISO/IEC 27005:2011 Risk Management Standard. In *Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance*, HAISA'16, pages 101–111, Frankfurt, Germany, 2016. Plymouth University.

[3] Jason Andress. *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*. Syngress Publishing, 2nd edition, 2014.

[4] BSI. Act on the federal office for information security (bsi-gesetz - bsig) of 14 august 2009, 2009.

[5] Rafael Etges and Karen McNeil. Understanding data classification based on business and security requirements, 2006.

[6] Susan Fowler. Information classification –who, why and how. 2003.

[7] S. Ghernaouti-Helie, D. Simms, and I. Tashi. Protecting information in a connected world: A question of security and of confidence in security. In *Network-Based Information Systems (NBiS), 2011 14th International Conference on*, pages 208–212, Sept 2011.

[8] Sean Glynn. Getting to grips with data classification. *Database & Network Journal*, 41(1):8–10, 2011.

[9] Øivind Høiem. Guidelines for classification of information. 2013.

[10] North Carolina Healthcare Information and Inc. Communication Alliance. Glossary of top 45 security & privacy terms, June 2014.

[11] ISO. Information technology–security techniques–information security management systems–requirements. 2005.

[12] Information technology –security techniques –information security risk management. Iso, 2011.

[13] Information Security Project Board (ISPB). Hse information classification & handling policy, 2013.

[14] Greg Kane and Lorna Koppel. Chapter 1 - information protection function one: Governance. In *Information Security*, pages 1 – 11. Elsevier, Boston, 2013.

[15] Ann Kristin Lindaas and Kjersti Bjørgo. Retningslinjer ved tilgjengeliggjring av offentlige data, 2017.

[16] Woo-Sung Park, Sun-Won Seo, Seung-Sik Son, Mee-Jeong Lee, Shin-Hyo Kim, Eun-Mi Choi, Ji-Eon Bang, Yea-Eun Kim, and Ok-Nam Kim. Analysis of information security management systems at 5 domestic hospitals with more than 500 beds. *Healthc Inform Res*, pages 89–99, Jun 2010.

[17] Norwegian Parliament. Act of 14, april 2000 no. 31 relating to the processing of personal data (personal data act), 2000.

[18] Jody R. Westby. *International Guide to Cyber Security*. ABA Publishing, 2004.

[19] Carol Woodbury. The importance of data classification and ownership, 2007.

[20] H. Yin, K. Gai, and Z. Wang. A classification algorithm based on ensemble feature selections for imbalanced-class dataset. In *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity)*, pages 245–249, April 2016.