A Reference Model of Information Assurance & Security*

Yulia Cherdantseva
School of Computer Science and Informatics
Cardiff University
Cardiff, UK
y.v.cherdantseva@cs.cardiff.ac.uk

Jeremy Hilton
Department of Informatics and Systems Engineering
Cranfield University
Cranfield, UK
j.c.hilton@cranfield.ac.uk

***Abstract*—Information Assurance & Security (IAS) is a dynamic domain which changes continuously in response to the evolution of society, business needs and technology. This paper proposes a Reference Model of Information Assurance & Security (RMIAS), which endeavours to address the recent trends in the IAS evolution, namely diversification and deperimetrisation. The model incorporates four dimensions: Information System Security Life Cycle, Information Taxonomy, Security Goals and Security Countermeasures. In addition to the descriptive knowledge, the RMIAS embeds the methodological knowledge. A case study demonstrates how the RMIAS assists with the development and revision of an Information Security Policy Document.**[1]

***Keywords*-Information Assurance, Information Security, Conceptual Model, Reference Model, Information Security Policy Development**

I. Introduction

A. Information Security and Information Assurance

Year by year the importance of Information Security (InfoSec) and Information Assurance (IA) grows. In 2012, security budgets received higher priority worldwide compared with 2011. The spending on security is expected to grow from $55 billion in 2011 to $86 billion in 2016 [1].

The terms InfoSec and IA are often interpreted differently [2]. For the sake of clarity, the definitions of InfoSec and IA accepted in this work are outlined below (throughout the text all important definitions are *italicized*). The definitions are adopted from [2] where they are elaborated on the basis of the detailed analysis of the related literature.

Information Security *is a multidisciplinary area of study and professional activity which is concerned with the development and implementation of security countermeasures of all available types (technical, organisational, human-oriented and legal) in order to keep information in all its locations (within and outside the organisation's perimeter) and, consequently, information systems, where information is created, processed, stored, transmitted and destructed, free from threats* [2].

Information Assurance *is a multidisciplinary area of study and professional activity which aims to protect business by reducing risks associated with information and information systems by means of a comprehensive and systematic management of security countermeasures, which is driven by risk analysis and cost-effectiveness* [2].

In this research, we refer to the ***Information Assurance & Security*** (IAS) knowledge area [2], which incorporates the knowledge acquired by both InfoSec and IA. In the scope of IAS this includes all actions directed at keeping information secure as well as the management of these actions. The realm of IAS is not limited to the protection of electronic information, or to the technical security countermeasures. IAS promotes an holistic approach to security where a sensible combination of security countermeasures of different types is exploited for the adequate information protection.

B. Reference Modelling

Any knowledge area has either an explicit or assumed conceptual model which describes the phenomenon being investigated, "map[s] reality, guide[s] research and systematize[s] knowledge" [3]. A conceptual model, which represents a problem at the industry level and captures the domain knowledge, is referred to as a *reference model* [4]. OASIS [5] provides the following definition of a reference model:

*A **Reference Model** (RM) is an abstract framework for understanding significant relationships among the entities of some environment. It enables the development of specific reference or concrete architectures using consistent standards or specifications supporting that environment. A reference model consists of a minimal set of unifying concepts, axioms and relationships within a particular problem domain, and is independent of specific standards, technologies, implementations, or other concrete details.*

In addition to the descriptive knowledge, an RM often incorporates the methodological knowledge. It outlines fruitful methods of research and practice [3].

An RM is usually graphically represented. The effectiveness of the visual appearance of an RM is crucial because a model should be easily understood by a wide range of stakeholders with different backgrounds. An RM does not usually use any formal modelling language, but visualises the thinking it promotes in a clear way, which is easy to grasp and remember. Since the comprehension of an RM does not require knowledge of a formal modelling language, used for its representation, an RM is more easily accessible by experts who lack this knowledge.

[1]* This is an author's preprint version of the paper to be published in IEEE proceedings of ARES 2013, SecOnt workshop (2-6 September, 2013, Regensburg, Germany). The published version will be available at IEEE Xplore after the conference.

An RM may be used in several scenarios [6], but in the majority of cases it is used in the Information System (IS) development context [4]. In this work, the following definition of an IS is adopted:

*An **Information System** is a socio-technical system, which delivers information and communication services required by an organisation in order to achieve business objectives. An IS encompasses six components: (1) information (data), (2) people, (3) business processes (procedures), and ICT, which includes (4) hardware (5) software and (6) networks.*[2]

An IS, as it is understood in this research, is not limited to either the technical or social perspective. The combination of all perspectives defines the complex socio-technical nature of an IS. No IS exists in a vacuum (every system provides information and/or services to and receives them from external parties) and, therefore, the interactions of an IS with the environment should also be taken into account.

C. Role of a Reference Model in the IAS domain

Many security issues are caused by wrong security decisions being taken on the basis of incomplete knowledge or misunderstanding of the security domain [11]. An RM helps to overcome this problem by bringing together, in a clear all-encompassing picture, the main entities of the knowledge area and the relationships between them as well as the fruitful methods of research and practice [3].

A model of the IAS domain structures the acquired knowledge, creates a common ground for professionals and serves as a conceptual framework for researchers. It fosters a profound, systematic understanding of IAS and, as a result, helps practitioners to do their job more efficiently. It allows technical and business experts to communicate more effectively [12]. The model also enables newcomers to get a faster appreciation of the domain's diverse nature.

An RM of IAS plays a crucial role in the IS context because it serves as a blueprint for the design of a *secure* IS. It provides a basis for the elicitation of security requirements and for the development of an Information Security Policy Document (ISPD). A model may be used for predicting security vulnerabilities, tracing back security incidents and security benchmarking [7].

D. Contribution and Structure of the paper

A conceptual model of a discipline often becomes debatable and requires a revision when a discipline evolves and broadens [3]. Since IAS is an intermittently dynamic domain, which changes shape following the evolution of society, business needs and technology, its conceptual model should be regularly revised to reflect the changes in the domain [13].

An analysis of the InfoSec and IA literature, summarised in [2], allowed the marking out of two major trends in the recent evolution of IAS. First, IAS has become a much-diversified field of research and practice that utilises knowledge of such disciplines as sociology, physiology, criminology, mathematics, management, marketing, law, etc. As a result of its manifold nature, IAS has been recognised as a complex managerial issue which requires a comprehensive and systematic approach. This means that experts with different backgrounds should communicate effectively with regard to security issues. In order to do this experts should be equipped with an agreed-upon high level of abstraction understanding of the IAS domain.

Second, there is a shift from closed isolated IT environments to open interconnected environments (this phenomenon is known as *de-perimeterisation*) [2], [14]. Organisations intensively collaborate (share information, and integrate ISs and business processes) in order to improve their competitiveness and effectiveness. E-commerce, outsourcing and cloud computing assume information sharing with external parties and induce a proliferation of cross-organisational dependencies. In this landscape, IAS becomes more challenging because information calls for protection, not only within the safe boundaries of an organisation, but also outside of them. In order to improve the overall protection of information in an information sharing community it becomes essential to harmonise an understanding of IAS not only within an organisation, but across an entire community of organisations collaborating in a de-perimeterised environment.

The purpose of this paper is to propose a **R**eference **M**odel of **I**nformation **A**ssurance & **S**ecurity (RMIAS), which endeavours to overcome the limitations of the existing conceptual models of InfoSec and IA, and to address the recent trends in the IAS evolution, namely diversification and de-perimeterisation. The RMIAS reflects the diverse scope of the domain and attempts to convey an understanding of IAS as a complex managerial and organisational issue that requires addressing in a comprehensive and systematic manner. It also meets the demands of the collaborative de-perimeterised environment and covers the protection of information in all its locations.

The remainder of the paper is structured as follows. In Section II, the existing models of InfoSec and IA are discussed. Section III presents the overview of the RMIAS and its four dimensions. Section IV describes the interrelationships between the dimensions and outlines the methodological knowledge embedded into the model. Section V reveals the details of a case study where the RMIAS has assisted with the review of an ISPD. Section VI contains concluding remarks.

II. Related Literature

The CIA-triad (confidentiality, integrity and availability) has for several decades been serving as a conceptual model of computer security and, later, InfoSec [10]. Its origin could be traced back to 1975, when Saltzer and Schroeder [15] stated that at that time security specialists distinguished three categories of threats to information:

[2]This definition is synthesised on the basis of the extensive analysis of the IS definitions in [9]. Six components of an IS are also listed in [10, p.17-19].

unauthorised information release (confidentiality), unauthorised information modification (integrity) and unauthorised denial of use (availability). The term CIA-triad, as we know it today, appeared only in 1986-1987. The term was coined at the Johnson Space Center, USA [17] and, for the first time, appeared in a JSC-NASA Information Security Plan, also known as "The Pink Book" in 1989. The CIA-triad rapidly gained popularity among InfoSec practitioners. Until now, a wide range of security-related material is based on the CIA-triad, despite the fact that the adequacy of the CIA-triad has been questioned [10], [13].

The first comprehensive model of InfoSec was developed by McCumber [7] in 1991 (Figure 1). The model, also known as the McCumber's Cube, is a part of the National Training Standard for Information Systems Security Professionals (CNSS 4011) [10, p.15].

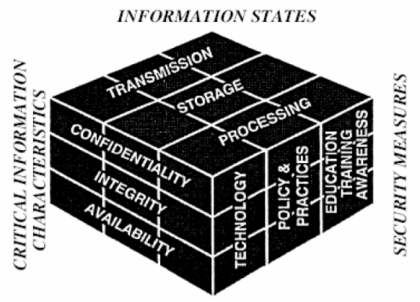

Figure 1. McCumber's Cube [7]

The McCumber's Cube consists of three building blocks: (1) information states (transmission, storage, processing), (2) critical information characteristics (confidentiality, integrity and availability), and (3) security measures (technology, policy and practices, and education, training and awareness).

Maconachy et al. [16] extend the McCumber's Cube by introducing a dimension of time and additional security services: authentication and non-repudiation.

Parker [13] suggests a new model of InfoSec which consists of six essential foundation elements: availability, utility, integrity, authenticity, confidentiality and possession. Parker claims that his model addresses the limitation of InfoSec by the CIA-triad. In [17], Parker further elaborates on his model and introduces into the model: (1) types of acts that induce risk to information; (2) types of control and practices for protection of information; and (3) objectives of InfoSec, which may serve as a kernel of the security policy of an organisation.

ISACA (a non-profit, global association which develops practices for information systems) proposes the Business Model for Information Security (BMIS) [12]. The BMIS (Figure 2) consists of four elements: (1) organisation design and strategy element, (2) people element, (3) process element and (4) technology element. The elements are linked together by six dynamic interconnections: governing, culture, enabling and support, emergence, human factors and architecture.

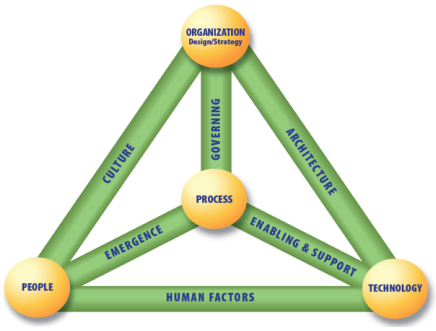

Figure 2. BMIS [12]

Jonsson [8], [18] presents a conceptual security model, where the security of a system is considered in terms of system input and output. Capturing the intertwined nature of the dependability and security concepts, Jonsson proposes an integrated model of security and reliability. The main purpose of the model in [8], [18] is to assist with reasoning about security.

An IA model based on a diligence approach is presented in [19]. An InfoSec ethics education model is elaborated in [20]. A conceptual model of the Information Security Compromise Process from the viewpoint of a target organisation is outlined in [21].

Analysis of the existing models shows the lack of an agreed upon set of security goals (which are interchangeably referred to in the literature as security attributes, properties, fundamental aspects, information criteria, critical information characteristics and basic building blocks). In addition to the CIA-triad, authors include in the models such goals as non-repudiation, authentication, possession, authenticity, utility, etc. A clear high level of abstraction classification of security countermeasures, which would encompass all possible types, was not found in any of the references. Consideration of time within the models (e.g. [16]) is too generic, and does not have pragmatic value. Although protection of information outside the organisation's perimeter is mentioned in some works ([7], [12], [16]), it is not explicitly addressed.

III. The RMIAS overview

The RMIAS, depicted in Figure 3, has four dimensions:

- **Information System Security Life Cycle Dimension** illustrates the progression of IS security along the IS Development Life Cycle (ISDL);
- **Information Taxonomy Dimension** describes the nature of information being protected;
- **Security Goals Dimension** outlines a broadly applicable list of security goals. *A **Security Goal** is a desirable ability of an IS to resist a specific category of threats.*

  There are two approaches to analysing IAS issues [25]: the threat-based and goal-based approaches. The threat-based approach analyses specific threats to information in greater technical detail. The goal-based approach operates at a higher level of abstraction.

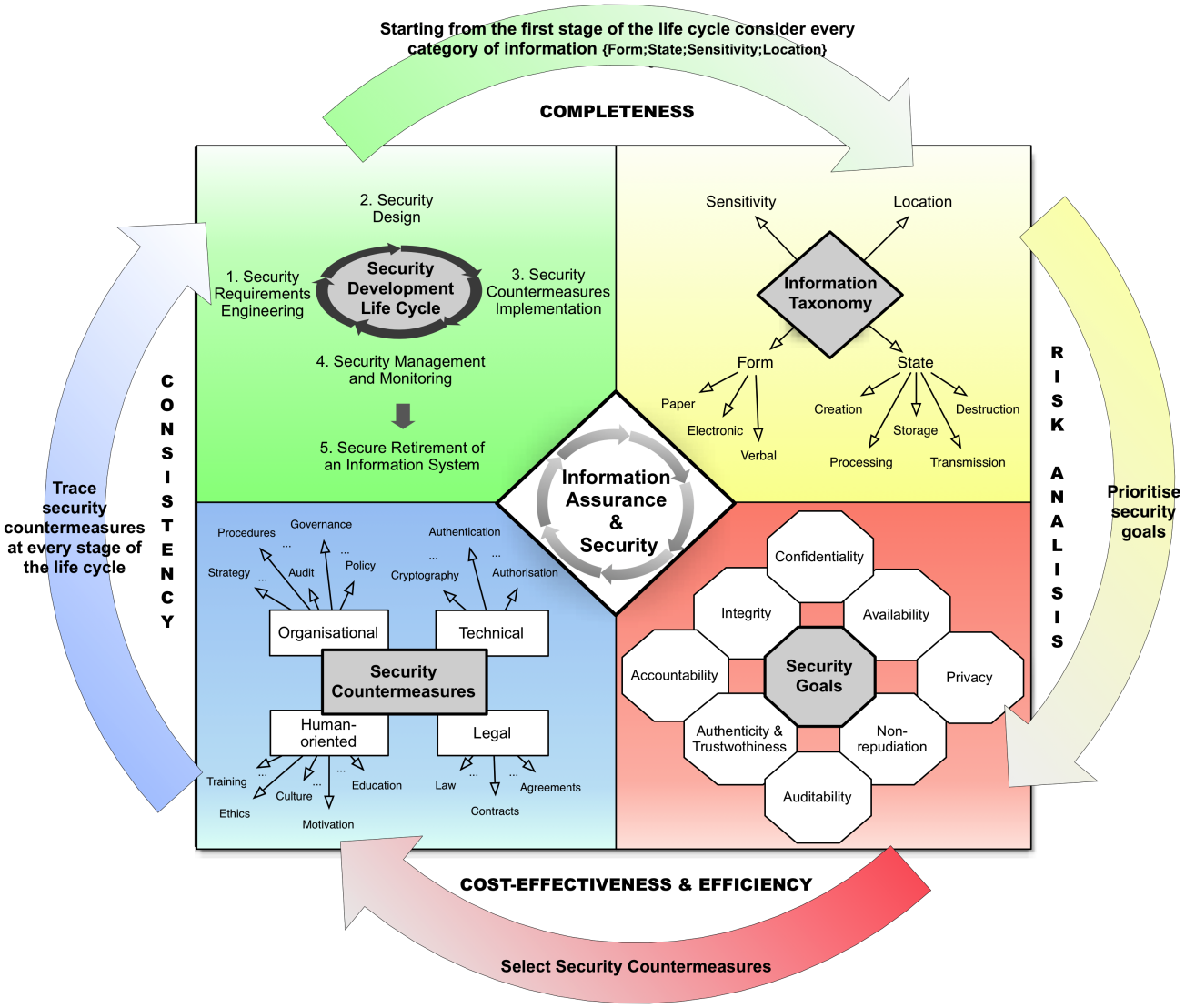

Figure 3. Reference Model of Information Assurance & Security[3]

Rather than concentrating on the details of a specific threat, a goal reflects a specific category of threats [23] (e.g. all threats that fall under the description of an *unauthorised modification* are covered under the umbrella of the security goal *integrity*). Focusing on goals allows security experts to communicate with other stakeholders using concepts that do not require technical knowledge [24]. Since the RMIAS is destined for a wide audience of non-technical and non-security experts, the preference has been given to the goal-based approach.

- **Security Countermeasures Dimension** categorises countermeasures available for information protection. *A **Security Countermeasure** is a technique or a process which helps to achieve one or more security goals and helps to mitigate risks to information and vulnerabilities in an IS.*

These four dimensions are deemed compulsory and sufficient for an understanding of the IAS domain at the chosen high level of abstraction. They do not overlap and do not duplicate each other.

The interrelationships between the dimensions, illustrated with arrows in Figure 3, are explained in Section IV. The following subsections present the detailed description of each dimension of the RMIAS.

A. SECURITY LIFE CYCLE (TIME) DIMENSION

IAS is an integral part of an IS and could not be considered separately from it. All IAS activities should be aligned with the ISDL. The ISDL consists of several stages with each having its purpose and outcome [26]. Standards (e.g. [26], [27]) do not require an organisation to follow any particular life cycle model, but require it to

[3]The Security Countermeasures dimension outlines only some countermeasures related to the specific type, but not the exhaustive lists. Within the Information Taxonomy dimension, attributes *Location* and *Sensitivity* possess values specific to an organisation (Section III-B2 and III-B3).
A coloured version is available at http://RMIAS.cardiff.ac.uk.

choose or tailor, and consistently follow a life cycle model that better suits the organisation's specifics. The security life cycle should be adjusted to the ISDL chosen by an organisation.

There is a wide range of ISDL models [27], [28], and security life cycle models [27]. The RMIAS incorporates a generic Security Development Life Cycle which has five stages as depicted in the top left quadrant of Figure 3.

Many standards (ISO/IEC 27000 series; the Federal Information Security Management Act (FISMA); Office of Management and Budget (OMB) Circular A-130, Appendix III; NIST Special Publication 800-64) require security to be addressed starting from the early stages of the ISDL. In practice, InfoSec is often treated as an afterthought and left until implementation or maintenance stages. The incorporation of the IS Security Development Life Cycle into the RMIAS highlights the need to address security consistently throughout all stages of the system life cycle and enables the establishment of a time-dependent sequence of necessary IAS activities.

B. INFORMATION TAXONOMY DIMENSION

McCumber [7] claims that in order to identify the appropriate security goals and, subsequently, the required countermeasures for a specific piece of information, it is sufficient to know the state of information.

We argue that knowing the current state of information is insufficient. The RMIAS incorporates the extended Information Taxonomy which helps to understand fully the nature of information being protected. As a result, the RMIAS provides for a better grounded choice of security countermeasures. In the RMIAS, information at any moment in time has the following attributes:

1) Form (Format),
2) Sensitivity,
3) Location, and
4) State.

Sensitivity of information may change over time and should be revised regularly. State, form and location of information change numerous times during its life cycle while information sensitivity changes less frequently.

1) Information Form: Information may be in one of three forms (formats): *paper*, *electronic*, or *verbal*.

2) Information Sensitivity: There are two reasons behind the incorporation of the information sensitivity classification into the RMIAS.

First, goals and countermeasures, are defined on the basis of information sensitivity (ISO/IEC 27002:2005, Sec. 7.2). For example, for a document restricted to internal use only, confidentiality has high priority, whereas for the publicly available document (e.g. press-release), confidentiality is not essential while integrity is. Accordingly, different security countermeasures should be applied to information of different levels of sensitivity: a normal business document may be sent by ordinary post, while a confidential one should only be sent by special delivery.

Second, the information sensitivity classification is one of the mechanisms for enhancing information protection in the collaborative de-perimeterised environment. ISO/IEC 27002:2005 requires an organisation to classify information by sensitivity, criticality and value to the organisation, and label it appropriately. An organisation develops an information classification scheme according to its business needs. This means that within an information sharing community every member often operates its own bespoke classification scheme.

In order to protect information in the de-perimeterised environment, the information classification and labeling schemes of organisations involved in information sharing should be in agreement. ISO/IEC 27010:2012, Sec. 7.2 states that "care should be taken in interpreting classification markings assigned by other members of an information sharing community". The consensus use of classification schemes is crucial, but hard to achieve because, first, information has different values for different organisations and, second, even similar classification and labeling schemes do not automatically imply a similar level of protection being applied. Consistent handling and protection of information should be negotiated in an information sharing community as part of an harmonised classification and labeling scheme.

3) Information Location: Risk to information and, consequently, the required countermeasures also depend on the current location of information. Sensitive information processed on a laptop at an internet café should be protected differently from the same information processed on a desktop in the organisation's office. This aspect acquires particular importance in the collaborative de-perimeterised environment. Within each location, it is important how much control an owner of information has over the environment and information itself.

Another aspect that the *Location* attribute brings to light is that location or physical possession does not assume information ownership. Although a software developer possesses the program code on his laptop, the ownership belongs to the employer [13]. Outsourcing is another example: a service provider (e.g. cloud provider) physically possesses information, but the ownership is retained by a customer. Clear answers to such questions as to *who owns information and where it is physically located* help to identify adequate countermeasures.

The categorisation of locations, similarly to the information sensitivity classification, is organisation-specific. As an example, the following categorisation of locations is suggested:

controlled - locations where information is under the full control of an organisation (e.g. organisation's offices);

partially controlled - locations where information is physically possessed by parties with which an organisation has contractual relationships (e.g. IT-service provider, third parties storing or processing information on behalf of the organisation, business partners and employees' homes); and

uncontrolled - locations other than those falling into the previous two categories (e.g. meeting rooms in hotels and other public buildings).

4) Information State: State of information, along with form, sensitivity and location, defines security countermeasures to be implemented. During its life cycle, at every specific moment, information may be in one of five states: creation, transmission, storage, processing or destruction. Information may change its state between transmission, processing and storage numerous times. Information reaches the states of creation and destruction only once at the beginning and at the end of its life cycle.

Not considering the creation and destruction stages of information (which is observed in [7], [16]) is erroneous. Analysis of information security policies of various organisations confirms that protection of information at the states of creation and destruction, as well as at the other three states, is important and thoroughly addressed in practice and, therefore, should be captured in the model.

At creation, completeness and correctness of information must be ensured (integrity), the appropriate provenance data set (auditability and accountability), correct level of sensitivity assigned and the appropriate marking applied (confidentiality and privacy). Destruction of information should be controlled, audited and executed in a lawful way (e.g. the Data Protection and Sarbanes-Oxley Acts require confidential financial and personal information to be deleted with special care). Protection of information during transmission, processing and storage is discussed in [7].

5) Examples: Information category, which is a combination of attributes {form, state, sensitivity, location} is a basis for the specification and selection of security goals and countermeasures. This subsection outlines some examples of information categories.

Company A produces a monthly report about sales volumes for internal use only. The attributes of the report are as follows: form - *electronic*; state - *creation*; location - *controlled*; sensitivity - *restricted internal use*. There may be a situation where a document classified as "restricted internal use" escapes the safe perimeter of an organisation (e.g. an employee by mistake sends the document to an external party). The attributes of the document are as follows: form - *electronic*; state - *processed*; location - *uncontrolled*; sensitivity - *restricted internal use*. These attributes define a dangerous category and prompt the planning of security countermeasures that may be applied to prevent information falling into this category (e.g. email content control system prevents documents classified "restricted internal use" to be sent to external email addressed).

C. SECURITY GOALS DIMENSION

The inadequacy of the CIA-triad as a complete set of security goals has been shown in [10], [13]. The CIA-triad does not cover new threats that emerge in the collaborative de-perimeterised environment. In order to identify a complete, currently relevant list of security goals, an analysis of the InfoSec/IA literature and system engineering literature with regard to security goals has been conducted. This analysis is partially summarised in [2, Table 2].

The analysis shows that there is not an agreed-upon set of goals and that authors associate a wide range of goals with InfoSec/IA. The following problems have been identified through the literature analysis:

- The same goals are referred to by different names;
- The goals with the same name have conflicting definitions in different sources (various communities input some specific meaning into particular terms);
- Security countermeasures are not distinguished from goals;
- Lack of clarity as to which component of an IS a goal applies to (e.g. integrity may refer to either information or system integrity, or both.)

Since the existing literature does not provide a commonly agreed list of security goals, we attempted to identify a broadly applicable set of security goals which addresses the problems listed above and replaces the CIA-traid. This has shown to be a challenging task. In order to develop a set of goals the following route has been pursued:

1) An integrated list of goals has been produced to include all goals referenced in the analysed literature;
2) Each identified goal has been examined individually;
3) Goals with duplicated meaning have been either excluded or merged;
4) Countermeasures have been excluded from the list. (The advantage of the notion of *security goal* is that it does not imply a use of a certain measure: a goal outlines the problem to be solved and fosters consideration of all possible alternatives to achieve it [43]. This finally leads to more efficient and cost-effective security solutions.)
5) A security goal has been included in a finalised set if it met the following criteria:
   - A goal has a unique name;
   - A goal has a unique meaning which is not addressed by any other goal(s);
   - A goal is meaningful in the system engineering context.

Table I outlines the final set of security goals along with their concise definitions and shows the applicability of goals to the components of an IS. In Table I, the term "system" should not be interpreted as a "technical system", but in a broad sense according with the definition of an IS declared in Section I-B. It has been found that replacing the term "system" with the term "organisation" in the context of Table I provides clarity for a non-technical audience.

The size of the paper does not allow us to reveal in detail the consideration behind each goal incorporated in the final set, but in Table I we adduce the literature analysed in order to derive the definitions.

The set of goals, outlined in the RMIAS, as well as any other set, requires regular revision over time to incorporate goals addressing newly emerging threats. The modular structure, inspired by [42], has been adopted for

Table I
THE FINALISED LIST OF SECURITY GOALS

Security Goal	Definition	Analysed Literature	Components of an Information System: Information	People	Processes	Hardware	Software	Networks
Accountability	An ability of a system to hold users responsible for their actions (e.g. misuse of information)	[22], [31], [32]		X				
Auditability	An ability of a system to conduct persistent, non-bypassable monitoring of all actions performed by humans or machines within the system	[33], [34], [35]			X			
Authenticity/Trustworthiness	An ability of a system to verify identity and establish trust in a third party and in information it provides	[13], [22], [23], [31], [35], [36]	X	X	X	X	X	X
Availability	A system should ensure that all system's components are available and operational when they are required by authorised users	[7], [13], [16], [22], [31], [35]	X	X	X	X	X	X
Confidentiality	A system should ensure that only authorised users access information	[7], [13], [16], [31], [36]	X					
Integrity	A system should ensure completeness, accuracy and absence of unauthorised modifications in all its components	[7], [13], [16], [22], [31], [35]	X	X	X	X	X	X
Non-repudiation	An ability of a system to prove (with legal validity) occurrence/non-occurrence of an event or participation/non-participation of a party in an event	[22], [31], [35], [36]	X		X			
Privacy	A system should obey privacy legislation and it should enable individuals to control, where feasible, their personal information (user-involvement)	[32], [37], [38], [40], [39], [41]	X	X				

visualisation of goals (bottom right quadrant of Figure 3). It highlights the fact that the set of goals is not fixed. It may be revised to reflect future changes.

D. SECURITY COUNTERMEASURES DIMENSION

Multiple studies have shown that technical countermeasures alone are not capable of addressing many security-related issues and that a comprehensive approach to security is required [44]. A comprehensive approach means that countermeasures of a different nature should be exploited in order to protect information [14].

The fourth dimension of the RMIAS demarcates four types of security countermeasures:

1) Organisational,
2) Human-oriented,
3) Technical, and
4) Legal.

The RMIAS incorporates only the classification of measures at a high level of abstraction. It is clearly beyond the scope of this paper to produce the detailed taxonomies within each type. The lists of countermeasures, which are outlined in the following subsections, are by no means exhaustive.

1) TECHNICAL COUNTERMEASURES: refer to technical means designed to achieve security goals. For example, identification, authentication and authorisation help to achieve integrity, confidentiality and accountability. Cryptography is one of the main security technologies which protects both integrity and confidentiality. Other examples of technical countermeasures are biometrics, digital signature, firewall, intrusion detection system, antivirus, etc. One of the existing taxonomies of technical countermeasures is presented in [45].

2) ORGANISATIONAL COUNTERMEASURES: refer to administrative activities which aim to build and maintain a secure environment where selected security countermeasures may be effectively implemented and managed.

The examples of organisational measures are security strategy, security policy, procedures, governance, audit, compliance, business continuity and contingency planning, physical security, best practices, etc.

3) HUMAN-ORIENTED COUNTERMEASURES: address the impact of the human-factor on IAS. Some authors argue that people play the most essential role in achieving security [44], [46] since effectiveness of any technical or organisational security solution may be hindered if not supported by involved individuals. In the collaborative de-perimeterised environment, people who must be security-conscious include not only employees of a particular organisation, but also employees of business partners, service providers and authorities, who handle information of the organisation [14, Sec. 3.6-3.7]. Human-oriented measures strive to overcome the mechanical following of security instructions by explaining the rational behind security decisions. They also instil the understanding of security as everyone's day-to-day responsibility.

Human-oriented measures include, but are not limited to education, awareness, training, certification, ethics, culture, motivation, etc.

4) LEGAL COUNTERMEASURES: refer to the use of the legislation for the purposes of information protection. Information often escapes the safe boundaries of an organisation, whether intentionally or not (this is particularly true in the collaborative de-perimeterised environment). In

such cases neither technical nor organisational measures could help to protect information. In these situations, legal countermeasures play an important role.

Some examples of legal measures are established information ownership, legally agreed and enforced information classification and labeling schemes, service-level agreements, job contracts and employee non-disclosure agreements, law (e.g. copyright law), etc.

IV. Interrelationships between the Dimensions

In addition to the descriptive knowledge, outlined in Section III, the RMIAS also embeds the methodological knowledge. In Figure 3, arrows depict the logical dependences between the dimensions of the RMIAS and provide instructions on the use of the model.

The RMIAS, as any other model, is a generic abstraction. Before its use in the context of a specific organisation the following elements of the RMIAS should be adjusted:

1) The generic IS security life cycle should be replaced with the one specific to the organisation;

2) The model should be extended with the information sensitivity and location classifications specific to the organisation;

3) The RMIAS may be accompanied by the lists of countermeasures of each type available to the organisation and by a mapping between security goals and countermeasures. These lists make the use of the model more effective.

The description of the interrelationships between the dimensions of the RMIAS starts from the top left quadrant. An organisation defines its current stage at the security life cycle and then goes over the other three dimensions to come back to the next stage of the life cycle. At the stage of requirements engineering, an organisation inventories its information assets, establishes and prioritises security goals and selects security measures. At the stage of security design, an organisation ensures that all information assets, goals and measures, identified at the previous step, are consistently incorporated into and addressed by the system models. At the stages of implementation and management/monitoring, it must be ensured that (1) all countermeasures are implemented and function as designed and (2) the established security goals are achieved for every category of information.

The top arrow declares that starting from the first stage of the security life cycle every category of information, meaningful in the context of a specific organisation, must be identified. The use of the Information Taxonomy for cataloguing information which requires protection guarantees higher ***completeness*** of an ISPD. The ***completeness*** is further ensured by the consideration of all relevant security goals for every identified category of information.

Not all goals are equally important for every organisation, nor are they equally important for every category of information. The right arrow shows that for each category of information an organisation prioritises security goals driven by ***Risk Analysis*** (RA). The RMIAS is not an RA methodology, but it points out an important place of RA in the IAS domain and articulates the requirements towards an RA methodology which should assist with the creation of a detailed inventory of information and facilitate the prioritisation of security goals.

After information has been catalogued and security goals have been prioritised, an organisation identifies countermeasures that help to achieve established goals. The bottom arrow shows that the choice of countermeasures is driven by ***cost-effectiveness*** and ***efficiency***: an organisation does not aim to eliminate risks and protect information at any price, but only in the most cost-effective way ensuring that the chosen countermeasures do not hinder each others efficiency. The consideration of the full spectrum of security goals supported by RA enables the development of an optimum (cost-effective and efficient) combination of security countermeasures.

The left arrow illustrates that the identified countermeasures should be traced with ***consistency*** throughout all stages of the security life cycle. The circle created by the arrows shows that the model should be used in iterations at every stage of the life cycle.

For example, if at the stage of requirements engineering it is identified that the personnel should use the information classification scheme, then at the design stage (1) the provision of training on the classification scheme should be embedded into the business process models to guarantee that the required time and resources are allocated and (2) the training materials should be developed. At the implementation stage the actual training should take place and its effectiveness should be checked by knowledge tests. At the stage of management/monitoring the correct use of the classification scheme should be monitored, it should be updated when necessary to reflect changing business circumstances and the staff should be retrained if required.

If any change in either dimension should occur, the RMIAS should be updated accordingly and all steps should be repeated. E.g. if an organisation plans to allow employees to work from home, in the Information Taxonomy a new possible value "*employees' homes*" should be added to the attribute *Location*, and for the new categories of information goals should be prioritised and appropriate countermeasures selected.

V. A Case Study

The RMIAS has several important applications (Section I-C). This section explains how the model may be used for the development and revision of an ISPD. For the purpose of this example, we use the data of a real-life case study to which the RMIAS is applied as a part of the model evaluation process.

Our UK-based industry partner, whose name we may not reveal due to the non-disclosure agreement, provided us with a set of its security policy documents. The organisation recently undertook major changes to its business. The RMIAS is used to help the organisation to revise the ISPD to reflect the new circumstances.

The organisation uses the UK government classification and marking scheme: Top Secret, Secret, Confidential,

Table II
THE STRUCTURING OF AN INFORMATION SECURITY POLICY DOCUMENT USING THE RMIAS METHOD (EXCERPT)

	1. Form	2. Sensitivity	3. Location	4. State	5. Security Goal	6. Security Countermeasure Type: Description
1	Paper	Secret	Controlled	Creation	Confidentiality	Organisational: *Apply Protective Marking (Avoid over or under marking).*
2	Any	Any	Controlled	Destruction	Availability	Organisational: *No information, held on any media, can be destroyed unless it has been reviewed.*
3	Paper	Confidential	Partially Controlled	Transmission	Accountability, Confidentiality	Organisational: *Documents marked CONFIDENTIAL may be taken home only with a written approval of a designated person. All actions with documents marked CONFIDENTIAL to be logged.*
4	Electronic	Protect	Uncontrolled	Storage, Processing	Confidentiality, Integrity	Technical: *Any data marked PROTECT must be encrypted when taken outside the office.*

Restricted, Protect and Unclassified [30]. The locations are categorised as suggested in Section III-B3: *controlled*, *partially controlled* and *uncontrolled*. All security policy documents are analysed and structured using the RMIAS method. The excerpt from the final table is shown in Table II.

First, all information categories valid within the organisation are catalogued using the Information Taxonomy. Each row in Table II refers to a certain category of information (information attributes are outlined in columns 1-4). Thus, row 1 refers to paper documents which are created in the organisation's office and classified as "Secret". Row 2 refers to documents in any form and of any sensitivity which are destroyed in the office.

Column 5 lists goals identified for each specific category of information. Row 3 refers to paper documents marked "Confidential" taken home by employees. For this category of information the organisation pursues accountability for information use/misuse and confidentiality of information. The goals are extracted from the existing ISPDs and confirmed during the workshop with the representatives of the organisation.

Columns 6 outlines the type and the detailed description of the specific countermeasure. To achieve accountability and confidentiality for information in row 3 an organisational countermeasure is applied: *information may only be taken home with a written approval of a designated person*. Row 4 refers to electronic information taken outside the office. This information must be encrypted in order to achieve confidentiality and integrity.

The case study confirms that the RMIAS (1) helps to organise, in a manageable form, security policies spread over multiple documents, (2) permits tracing of the contradictory security policy statements, and, most importantly, (3) facilitates the identification of omissions in security policies. The Information Taxonomy and Security Goals dimensions of the RMIAS provide a solid basis for a good coverage of all potential situations (misuse cases) in which information needs protection and, hence, with higher degree guarantee completeness of an ISPD. The proposed security countermeasures classification promotes consideration of countermeasures of different types for achieving the same goals and, consequently, contributes to more cost-effective and efficient security solutions.

VI. CONCLUDING REMARKS AND FUTURE WORK

In this project, an ambitious endeavour to structure the ample knowledge of the IAS domain in an all-encompassing model has been pursued. As any other abstraction, the RMIAS sacrifices some details in order to show the full breadth of the domain. An attempt to cover the entire knowledge area forces decisions to be taken that may launch a polemic. From our side, we attempted to make the decisions transparent, supported by the argument. One such decision is the use of the informal visual representation (in a form of an RM) for organising the domain knowledge. This decision is stipulated by the fact that the RMIAS is destined for a wide audience, including non-technical stakeholders, for the understanding and communication enhancing purposes. The representation via an RM is considered to be more accessible to the target audience and more suitable for the outlined purposes. In the future work, we plan to formalise the RMIAS using one of the ontology languages to assist with the development of machine-readable security policies.

IAS means different things to different experts depending on their education and experience. The RMIAS illustrates one of the possible views on the IAS domain. The RMIAS (the descriptive knowledge) is pre-validated, at least to a certain degree, since it has been developed as a synthesis of the existing models of InfoSec/IA, and the existing knowledge of the IAS domain. The novelty of the RMIAS is in (1) the combination of the discrete knowledge with the purpose to draw an holistic picture of the IAS domain and (2) the suggested security policy development method. The pragmatic value (utility) of the model has been validated via the presented case study. For further evaluation of the RMIAS a multiphase approach is exploited, which in addition to the case study includes (1) analytical evaluation based on the criteria proposed in [3], (2) interviews with academic and industry experts, and (3) workshops with MSc students to test the explanatory power and validity of the RMIAS. The detailed discussion of the evaluation method and the reporting of the evaluation results are out of the scope of this paper and will be presented elsewhere.

REFERENCES

[1] Gartner, Inc. Forecast Overview: Security Infrastructure, Worldwide, 2010-2016, 2Q12 Update. 2012.

[2] Y. Cherdantseva, and J. Hilton, "Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals," in: F. Almeida, and I. Portela (eds.), *Organizational, Legal, and Technological Dimensions of IS Administrator*. IGI Global Publishing, September, 2013.

[3] K. Järvelin, and T.D. Wilson, "On conceptual models for information seeking and retrieval research," *Information Research*, 9(1), p.163, 2003.

[4] D. Moody, "Theoretical and practical issues in evaluating the quality of conceptual models: Current state and future directions," *Data Knowl. Eng.*, 55(3), pp. 243-276, 2005.

[5] OASIS, "Reference Model for Service Oriented Architecture," OASIS Standard. Version. 1.0, 2006.

[6] P. Fettke, and P. Loos, "Perspectives on Reference Modeling," in: P. Fettke, and P. Loos (eds.) *Reference Modeling for Business Systems Analysis*, Idea Group, pp. 1-20, 2007.

[7] J. McCumber, "Information Systems Security: A Comprehensive Model," in: Proceeding of the 14th National Computer Security Conference, NIST, Baltimore, MD, 1991.

[8] E. Jonsson, "Towards an integrated conceptual model of security and dependability," Availability, Reliability and Security, The First International Conference on. IEEE, 2006.

[9] S. Alter, "Defining information systems as work systems: implications for the IS field," *European Journal of Information Systems*, 17(5), pp. 448-469, 2008.

[10] M. Whitman, and H. Mattord, "*Principles of Information Security*", 4th ed., Cengage Learning, 2012.

[11] A. Ekelhart, S. Fenz, M. Klemen, and E. Weippl, "Security Ontology: Simulating Threats to Corporate Assets," in: Bagchi and V. Atluri, (eds.) Information Systems Security, v. 4332. Springer, pp. 249-259, 2006.

[12] ISACA, "An Introduction to the Business Model for Information Security," 2009.

[13] D. Parker, "*Fighting Computer Crime*", NY: J. Wiley and Sons, 1998.

[14] Y. Cherdantseva, O. Rana, and J. Hilton, "Security Architecture in a Collaborative De-Perimeterised Environment: Factors of Success", in: *ISSE Securing Electronic Business Processes*, pp. 201-213, 2011.

[15] J. Saltzer, and M. Schroeder, "The protection of information in computer systems", Proceedings of the IEEE 63(9), pp. 1278-1308, 1975.

[16] W. Maconachy, C. Schou, D. Ragsdale, and D. Welch, "A Model for Information Assurance: An Integrated Approach," in: Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, U.S. Military Academy, NY, 2001.

[17] D. Parker, "Our Excessively Simplistic Information Security Model and How to Fix It", *ISSA Journal*, pp.12-21, July, 2010.

[18] E. Jonsson, "An integrated framework for security and dependability," in: Workshop on New security paradigms, pp. 22-29, ACM, 1998.

[19] W. Al-Hamdani, "Non-risk assessment information security assurance model," in: InfoSecCD Information Security Curriculum Development Conference, Kennesaw, USA, 2009.

[20] M. Dark, N. Harter, L. Morales, and M. Garcia, "An information security ethics education model," *Journal of Computing Sciences in Colleges*, 23(6), pp. 82-88, 2008.

[21] S. Ransbotham, and S. Mitra, "Choice and Chance: A Conceptual Model of Paths to Information Security Compromise," *Information Systems Research*, 20(1), pp.121-139, 2009.

[22] Committee on National Security Systems: National Information Assurance (IA) Glossary, CNSS Instruction No. 4009, 26 April 2010.

[23] Foreword by W. Ware in C. Pfleeger and S. Pfleeger, "*Security in Computing*", 4th ed. Prentice Hall, 2006.

[24] A. Antòn, J. Earp, and A. Reese, "Analyzing website privacy requirements using a privacy goal taxonomy." Requirements Engineering, IEEE Joint International Conference on. IEEE, pp.23-31, 2002.

[25] S. Rőhrig, *Using Process Models to Analyse Security Requirements*, Phd. Thesis, University of Zurich, 2003.

[26] ISO/IEC 12207:2008(E) IEEE Std 12207-2008 *Systems and software engineering Software life cycle processes*.

[27] NIST, Information Security Handbook: A Guide for Managers, NIST Special Publication 800-100. October, 2006.

[28] PD ISO/IEC TR 24748-1:2010 *Systems and software engineering Life cycle management. Part 1: Guide for life cycle management*.

[29] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, Wiley Publishing, 2001.

[30] HMG Security policy framework. 1 May 2010.

[31] ISO/IEC 27000:2009 (E) *Information technology - Security techniques - Information security management systems - Overview and vocabulary*.

[32] D. Weitzner, H. Abelson, T. Berners-Lee, J. Feigenbaum, J. Hendler, and G. Sussman, "Information accountability," *Communications of the ACM*, 51(6), pp. 82-87, 2008.

[33] Financial Reporting Council (FRC), Internal Control: Revised Guidance for Directors on the Combined Code, 2005.

[34] Sarbanes-Oxley Act of 2002. Pub. L.107-204. 116 Stat.745.

[35] P. Neumann, "*Computer-Related Risks*," ACM Press, 1995.

[36] R. Anderson, "*Security Engineering: A Guide to Building Dependable Distributed Systems*," Wiley Publishing, 2001.

[37] R.Smith, and J. Shao, "Privacy and e-commerce: a consumer-centric perspective," *Electronic Commerce Research*, 7(2), p.89-116, June, 2007.

[38] Report of the Secretary's Advisory Committee on Automated Personal Data Systems, "*Records, Computers and the Rights of Citizens*," July, 1973.

[39] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980.

[40] U.S. Privacy Protection Study Commission, Personal Privacy in an Information Society July, 1977.

[41] H. Almagwashi, and A. Gray, "Preserving Privacy in E-government: A System Approach," in: Proceedings of IFIP EGOV2012, Kristiansand, Norway, 2012.

[42] D. Moody, "The "Physics" of notations: Toward a scientific basis for constructing visual notations in software engineering," *Software Engineering*, IEEE Transactions on, 35(6), pp. 756-779, 2009.

[43] H. Mouratidis, P. Giorgini, and G. Manson, "Integrating security and systems engineering: Towards the modelling of secure information systems," *Advanced Information Systems Engineering*, pp. 10-31, Springer, 2003.

[44] I. Winkler, and B. Dealy, "Information security technology?... Don't rely on it. A case study in social engineering." in: Proceedings 5th usenix Unix Security Symposium, 1995.

[45] H. Venter, and J. Eloff, "A taxonomy for information security technologies," *Computers & Security*, 22 (4). pp.299-307, 2003.

[46] D. Lacey, "*Managing the Human factor in information security*," J. Wiley and Sons Ltd., 2009.

A Corresponding Author, Yulia Cherdantseva, may be contacted by email: Y.V.Cherdantseva@cs.cardiff.ac.uk.