A Stakeholder-Centric Approach for Defining Metrics for Information Security Management Systems

Anirban Sengupta[1][0000-0002-6239-256X]

[1]Centre for Distributed Computing, Jadavpur University, Kolkata 700032, India
anirban.sg@gmail.com

Abstract. An enterprise comprises of information processing systems that help realize its business processes. Automation of these systems is achieved with the help of IT assets like hardware, software and network devices. Assets and their interconnections may contain vulnerabilities, which can be exploited by threats, leading to breach of security of information and business processes. Such probable security risks are managed by implementing an Information Security Management System (ISMS). An important aspect of ISMS is the measurement of information security posture of the enterprise; this enables the comparison of information security status over time, and provides assurance to stakeholders about the *amount* of security that exists within the information processing systems. Different stakeholders have separate concerns regarding the security of an Enterprise IT System. This paper attempts to identify all such stakeholders and analyze their security concerns. A set of metrics has been defined that covers all facets of ISMS and addresses security concerns of all categories of stakeholders. This would help in the design of an effective and efficient ISMS.

Keywords: Enterprise Information Security, Enterprise Stakeholders, ISMS, Security Concern, Security Metrics, Security Risk.

1 Introduction

An enterprise comprises of information processing systems that help realize its business processes. Automation of these systems is achieved with the help of assets like hardware, software and network devices. Assets and their interconnections may contain weaknesses, or *vulnerabilities* [1, 2], which can be exploited by *threats* [1], leading to breach of security and privacy of information and business processes. Such probable *risks* need to be controlled [1] and *all* stakeholders need to be assured that information is being processed securely by the enterprise. This is usually achieved by implementing an Information Security Management System (ISMS) [3]. An important aspect of ISMS is the measurement of information security and privacy posture of the enterprise; this enables the comparison of information security and privacy status over time, and provides assurance to stakeholders about the *amount* of security and privacy that exists within the information processing systems. Standards like ISO/IEC 27004 [4] and NIST SP 800-55 [5] describe the components of an enterprise security metrics programme to comply with ISMS standards ISO/IEC 27001 [3] and NIST SP 800-53 [6], respectively. However, they do not state specific metrics that may be used to measure assurance and improvement in enterprise security and privacy posture. Implementers of enterprise security usually limit themselves to finding gross measures like count of virus outbreaks, count of security-aware personnel etc. These can, at the most, provide sketchy ideas about some aspects of security metrics programme implementation; they do not pinpoint the ground-level effectiveness of ISMS. Moreover, researchers have mostly concentrated on finding ways of measuring specific characteristics of security devices. Such values can prove the efficacy of individual devices like firewalls, IDS/IPS etc. [7, 8]; they cannot provide stakeholders with composite figures that prove the effectiveness of complete ISMS. Thus, the definition, modelling and implementation of security and privacy metrics continue to intrigue researchers and it has remained a *hard problem* in information security research [9].

From an enterprise information security perspective, the need is to develop a comprehensive set of metrics that can i) address the security and privacy concerns of *all* types of stakeholders, and ii) help in the continual improvement of enterprise ISMS [4]. This paper tries to deal with this issue by defining metrics that i) cover all facets of ISMS, and ii) address security and privacy concerns of all categories of stakeholders of enterprise information systems. The paper is organized as follows. A survey of related work is given in Section 2. Section 3 categorizes the stakeholders of an enterprise and describes their concerns. Mapping between these concerns and security / privacy parameters is given in Section 4. Section 5 presents a set of ISMS metrics, while the relation between stakeholder concerns and ISMS metrics is detailed in Section 6. Finally, Section 7 concludes the paper.

2 Related Work

There has been some significant research on specific areas, and techniques, of information security measurement. Marcus Pendleton et al. have published a detailed survey on systems security metrics [10]. The authors have investigated the relationships among *metrics of system vulnerabilities*, *metrics of defense power*, *metrics of attack or threat severity* and *metrics of situations*, using a hierarchical ontology. Tupper and Zincir-Heywood defined VEA-bility (vulnerability, exploitability, attackability) as a security metric [11]. Victor-Valeriu Patriciu et al. proposed metrics to evaluate security vulnerabilities and controls [12]. Besides, several researchers have presented research on risk assessment and risk metrics [13, 14].

As is evident, most of the published works have drawn inspiration from software quality metrics. Though this can be a good starting point, and may give some idea about security aspects of software and hardware, such metrics cannot be used to comprehend the complete security posture of an enterprise information system. Now let us discuss some studies that have been performed specifically on ISMS metrics. ISO/IEC 27004 [4] and NIST SP 800-55 [5] describe how to implement information security metrics programmes in compliance with the requirements of ISMS. Gaffri Johnson has suggested that five core processes, namely *IT and business alignment*, *information security risk management process*, *compliance process*, *awareness process* and *audit process*, should be measured in order to maintain an effective ISMS [15]. The paper provides some examples illustrating the measurement of these processes. A. P. Aldya et al. [16] proposed a methodology for identifying the objects, measurement parameters and metrics based on the provisions of ISO/IEC 27004. Veselin Monev proposed a methodology [17] for evaluating the maturity level of the security controls and clauses of ISO/IEC 27001 [3]. In his master's thesis, Matthias Mödinger has proposed a set of metrics and key performance indicators for ISMS [18]. The work is based on the principles of ISO/IEC 27004 [4] and caters specifically to the requirements of universities.

Thus, it is obvious that the published papers and reports do not state specific metrics that may be used to measure assurance and improvement in enterprise ISMS. They either suggest some gross methodologies for implementing ISMS metrics programme, or cater to the needs of specific industries / domains. This paper tries to fill this research gap by defining ISMS metrics that will help stakeholders to understand the amount of security / privacy that exists within an enterprise. The metrics are domain-independent, and have been defined keeping in mind the security and privacy concerns of different categories of stakeholders.

3 Stakeholders of an Enterprise and their Concerns

An enterprise comprises of different stakeholders who are directly, or indirectly, associated with its business processes and information assets. In fact, the existence and business of an enterprise are governed by its stakeholders. Analyses of standards like ISO/IEC 27001 [3] and ISO/IEC 27002 [19] reveal that stakeholders can be broadly categorized as Employees, Clients, Third Parties and Authorities. In this section, specific security and privacy concerns of different stakeholders are discussed; this is the outcome of interactions of the author with stakeholders during several instances of ISMS implementation. It may be noted that in case of some stakeholders, only a subset of the listed concerns (for that stakeholder category) may be applicable.

Employees - Employees are usually under the direct supervision of an enterprise. They can be further categorized as “management” or “operational” personnel. While, management establishes the objectives and business strategies of an enterprise, these are implemented and maintained by operational staff. Since, the nature of their contributions to enterprise functions are different, their concerns also vary. Specifically, managers own the business processes and critical information assets of an enterprise, and establish ISMS for protecting the same. This leads to the following security and privacy concerns: (i) Security of enterprise Business Processes and critical information assets – these are the primary assets of an enterprise, and are directly owned by senior management; (ii) Safety of client data – management of an enterprise are accountable for the protection of data of all its clients (individuals and other enterprises) with whom business relations exist; (iii) Safety of personal data – it is the concern of managers to ensure security of personal data of all employees (including their own data); (iv) Reputation of enterprise – if the reputation of an enterprise is sullied, the senior management is usually held accountable; and (v) Efficacy of the implemented ISMS – it is important to ensure that the implemented ISMS complies with the information security requirements of the enterprise, and effectively addresses the security concerns of all stakeholders; moreover, greater the efficacy of ISMS, higher is the Return on Investment (RoI) of security processes and controls.

As is obvious, management personnel have concerns pertaining to information security and privacy requirements of the entire enterprise. However, the concerns of operational staff would be more of a personal nature; they would be worried about issues that are directly related to their roles. Specifically, operational personnel are concerned about: (i) Safety of *their* personal data; and (ii) Whether they will be accountable for others' misdeeds – sometimes, owing to lack of proper audit trails and monitoring, innocent members of staff may be held accountable for misdeeds which have been actually perpetrated by others; this is a major area of concern for operational personnel.

Clients - Clients of an enterprise are bothered about the safety of their personal data or assets (e.g. money, devices etc.), and the legal protection of their consumer rights. They are usually *not* concerned about the security of the enterprise, unless it affects them directly, or indirectly.

Third Parties - Third parties refer to all such external organizations or individuals who help an enterprise to realize its business objectives. Some examples of third parties are: Internet Service Providers (ISPs), third party data centres, organizations to which software development is outsourced, materials suppliers, third party employees, and courier companies and delivery personnel. Third parties are concerned about the security and privacy of those business processes and information which may have a bearing on their own business interests. Specifically, they are interested in the following: (i) Security of third party enterprise data and Business Processes; (ii) Safety of *their* personal data; (iii) Protection of *their* reputation – third parties are usually concerned whether loss of reputation of an enterprise, with which they are doing business, will also tarnish their own image; (iv) Protection of legal and contractual obligations – this includes all statutory requirements and service-level agreements between organizations; and (v) Whether they will be accountable for others' misdeeds.

Authorities - Authorities refer to all such entities that define and enforce legal and regulatory frameworks for enterprises. It is mandatory for enterprises to conduct their businesses within the ambit of these frameworks and to comply with relevant requirements. Examples of authorities are Reserve Bank of India (for Indian banks), Office of the Comptroller of the Currency (for US banks), ARCEP (for France's Electronic Communications, Postal and Print media distribution), certifying authorities (ISO/IEC, ISACA etc.) and judiciary. Security and privacy concerns of authorities usually comprise of the following: (i) Safety of data and assets of clients of an enterprise; (ii) Safety of data and assets of third party enterprises; (iii) Security of nation – this is applicable for critical-sector enterprises like defense organizations, space research organizations, banks etc.; (iv) Reputation of nation; and (v) Compliance.

4 Security / Privacy Concerns and Parameters

The security and privacy concerns of stakeholders are addressed by implementing controls (like policies, procedures, laws, security tools etc.) within the ambit of ISMS. Controls, in essence, help to protect security and privacy parameters of enterprise assets [19]. Hence, in order to select appropriate controls, it is important to identify the parameters that relate to the existing concerns of stakeholders. Analysis of the concerns described in the previous section reveal that they can be decomposed into requirements for the protection of specific *security* and *privacy parameters* of Business Processes and information assets. The analysis is presented in this section.

The relevant parameters that have been considered are as follows [3, 20]: *confidentiality* (C); *integrity* (I); *availability* (A); *authenticity*; *non-repudiation* - ability to prove the occurrence of a claimed event or action and its originating entities; *anonymity* - inability to identify the owner of personally identifiable information; *unlinkability* - inability to establish a link between two or more pieces of data items; *undetectability* - inability to determine the existence of a data item; *accountability* - responsibility for actions; *legal & contractual requirements*; and *image / reputation*. Let us now identify the parameters corresponding to stakeholder concerns.

Security of Business Processes and information assets – Traditionally, security is interpreted as the ability to protect C, I, A of assets. Another parameter that is of significance is authenticity. It is important to ensure that a business process or information asset is authentic; that is, it is indeed that asset which it claims to be.

Safety of client data – Similar to the case for information assets, safety of client data items, which is in the possession of an enterprise, would entail the protection of their C, I and A. Additionally, safety would also require ensuring the *privacy* of those data items that comprise of personally identifiable information [19]. Privacy has been defined as the protection of anonymity, unlinkability and undetectability parameters, in addition to C, I and A [20]. Thus, this concern can be addressed by ensuring the protection of six parameters – C, I, A, anonymity, unlinkability and undetectability. It may be noted that another privacy parameter, unobservability, has not been explicitly considered in this work as it is a combination of unlinkability and undetectability.

Safety of personal data and assets – This is similar to the above case. It can be addressed by ensuring the protection of C, I, A, anonymity, unlinkability and undetectability.

Reputation of enterprise – This concern can be directly mapped to the parameter image / reputation. This is an intangible parameter and depends on the perception of customers and users.

Efficacy of implemented ISMS – This concern is not related to any parameter explicitly. However, effective and efficient ISMS would imply that *all* required security and privacy parameters have been adequately protected.

Accountability for others' misdeeds – It is important to implement controls (monitoring mechanisms, audit trails etc.) so that innocent operational personnel and third parties are not held responsible for misdeeds perpetrated by others. These controls help to protect the image / reputation of innocent personnel as miscreants are not able to repudiate, and can be held accountable for, their misdeeds. Hence, the parameters that are significant for this security concern are accountability, non-repudiation and image / reputation.

Legal protection of consumer rights – The rights of consumers should be protected as per applicable legal and contractual requirements. This ensures that the image / reputation of consumers is not sullied due to mishap at the enterprise end. This also ensures that consumers are not held accountable for misdeeds perpetrated by others. Hence, the parameters accountability, legal & contractual requirements and image / reputation of consumers are important here.

Protection of legal and contractual obligations – Third parties are concerned about the protection of legal and contractual obligations as specified in service level agreements and statutory requirements. This will ensure that their image / reputation is not sullied and they are not unnecessarily held accountable for others' misdeeds. Hence, the parameters accountability, legal & contractual requirements and image / reputation of third parties should be addressed here.

Security of nation – Authorities are concerned about the protection of national security. Security and privacy breaches in critical-sector enterprises may jeopardize the integrity and / or availability of national assets (like power grids, networks etc.). This may, in turn, cause breaches of legal and contractual obligations with other countries, organizations etc., thus making the nation accountable for the same. Hence, this security concern should be addressed to protect integrity and availability of national assets, and accountability and legal and contractual obligations of the nation.

Reputation of nation – It is essential to prevent security and privacy breaches in critical-sector enterprises so that the image / reputation of the nation is not tarnished.

Compliance – An enterprise has to comply with all relevant legal and contractual obligations. Failure to do so may lead to litigations, loss of business, blacklisting etc.

The above analyses show that each security and privacy concern pertains to the protection of a set of relevant *security* and / or *privacy parameters*. The results have been summarized in Table 1 (columns 2 and 3).

Table 1. Security and Privacy Concerns, corresponding Parameters and ISMS Metrics.

Sl. No.	Security Concern	Security / Privacy Parameter	ISMS Metric
1	Security of Business Processes and information assets	Confidentiality, Integrity, Availability, Authenticity	Risk Metric
2	Safety of client data	Confidentiality, Integrity, Availability, Anonymity, Unlinkability, Undetectability	Risk Metric, Policy Compliance Metric
3	Safety of personal data and assets	Confidentiality, Integrity, Availability, Anonymity, Unlinkability, Undetectability	Risk Metric, Policy Compliance Metric
4	Reputation of enterprise	Image / Reputation	Risk Metric, Legal / Regulatory Compliance Metric, Contractual Compliance Metric, Con-

			trolled Incident Metric, Uncontrolled Incident Metric
5	Efficacy of implemented ISMS	All parameters	Risk Mitigation Metric, Controlled Incident Metric, Uncontrolled Incident Metric, Process Effectiveness Metric, Efficiency Metric
6	Accountability for others' misdeeds	Accountability, Non-repudiation, Image / Reputation	Risk Metric, Non-Repudiation Metric, Policy Compliance Metric, Legal / Regulatory Compliance Metric, Contractual Compliance Metric, Composite Compliance Metric
7	Legal protection of consumer rights	Accountability, Legal & Contractual requirements, Image / Reputation	Legal / Regulatory Compliance Metric, Contractual Compliance Metric
8	Protection of legal and contractual obligations	Accountability, Legal & Contractual requirements, Image / Reputation	Legal / Regulatory Compliance Metric, Contractual Compliance Metric
9	Security of nation	Integrity, Availability, Accountability, Legal & Contractual requirements	Risk Metric, Legal / Regulatory Compliance Metric, Contractual Compliance Metric, Controlled Incident Metric, Uncontrolled Incident Metric
10	Reputation of nation	Image / Reputation	Risk Metric, Legal / Regulatory Compliance Metric, Contractual Compliance Metric, Controlled Incident Metric, Uncontrolled Incident Metric
11	Compliance	Legal & Contractual requirements	Policy Compliance Metric, Legal / Regulatory Compliance Metric, Contractual Compliance Metric, Composite Compliance Metric

Security / privacy requirements of an enterprise can be derived as a union of the security / privacy concerns of *all* its stakeholders, as described above. An enterprise implements ISMS, including controls and specific techniques, to address its security and privacy requirements. The next section proposes a set of metrics that can be used to comprehensively measure the effectiveness of implemented ISMS, along with the amount of security and privacy that exists in the enterprise.

5 ISMS Metrics

Establishment of ISMS requires the implementation of controls that can address stakeholder concerns. It is important for stakeholders to assess the efficacy of the ISMS in meeting their security and privacy requirements. This can be achieved by defining and generating relevant metrics that correctly convey the status of the ISMS. In this section, a set of ISMS metrics is defined. These metrics cover the ISMS processes and activities as required by ISO/IEC 27001 standard [3].

Risk Metric - Risk values are measures of insecurity in an enterprise. *Risk* is defined as the probability that threats will exploit vulnerabilities to breach security parameters and cause harm to assets [1]. Lower the risk value corresponding to a parameter, greater is the assurance that the parameter is difficult to breach. The process of computing risk values is referred to as *risk assessment*. There are several well-known risk assessment methodologies [1]; hence, this paper does not propose any new methodology or risk metric.

Authenticity Metric - Authenticity metrics provide assurance that the information assets, along with related processing systems / applications, and users of assets are genuine. These metrics can be derived from data generated by mechanisms that verify the claimed identities of the source and destination of information. Thus, authenticity metric for application ap_i, $\mu_{auth}(ap_i)$, can be computed as:

$$\mu_{auth}(ap_i) = (count_{auth}(ap_i) / count(ap_i)) + (count_{auth}(inp(ap_i)) / count(inp(ap_i))) + (count_{auth}(usr(ap_i)) / count(usr(ap_i))) \qquad (1)$$

where, $count_{auth}(ap_i)$ denotes the no. of authentic instances of application ap_i that were executed in the enterprise during the period of measurement; $count(ap_i)$ is the total no. of instances (authentic and unauthentic) of application ap_i for the same period; $count_{auth}(inp(ap_i))$ denotes the no. of authentic inputs received by ap_i, while $count(inp(ap_i))$ gives the total no. of authentic and unauthentic inputs received; $count_{auth}(usr(ap_i))$ denotes the no. of authentic users and systems that have accessed application ap_i during the period of measurement; $count(usr(ap_i))$ gives the total no. of users and systems that have accessed ap_i.

Thus, it may be seen that:

i. $\mu_{auth}(ap_i) = 0$ when $count_{auth}(ap_i) = count_{auth}(inp(ap_i)) = count_{auth}(usr(ap_i)) = 0$ for a measurement period;

ii. $\mu_{auth}(ap_i) = 3$ when all instances of application api, along with its inputs and users, have been authentic during a period of measurement.

Hence, $0 \leq \mu_{auth}(ap_i) \leq 3$..

Non-repudiation Metric - This metric signifies the denial of actions of users pertaining to the access and use of an application or system and / or receipt of output from the application or system. Thus, non-repudiation metric for application ap_i, $\mu_{nrep}(ap_i)$, can be computed as:

$$\mu_{nrep}(ap_i) = (1 - count_{rep}(acc(ap_i)) / count(acc(ap_i))) + (1 - count_{rep}(out(ap_i)) / count(out(ap_i))) \qquad (2)$$

where, $count_{rep}(acc(ap_i))$ denotes the no. of instances, during the period of measurement, when users have falsely denied accessing / using application ap_i, while $count(acc(ap_i))$ gives the total no. of accesses of application ap_i by users during that measurement period; $count_{rep}(out(ap_i))$ denotes the no. of cases, during the period of measurement, when users have falsely denied receiving output from application ap_i, while $count(out(ap_i))$ gives the total no. of instances when users have received output from application ap_i during that measurement period.

Thus, it may be seen that:

i. $\mu_{nrep}(ap_i) = 0$ when $count_{rep}(acc(ap_i)) = count(acc(ap_i))$ and $count_{rep}(out(ap_i)) = count(out(ap_i))$ for a measurement period;

ii. $\mu_{auth}(ap_i) = 2$ when $count_{rep}(acc(ap_i)) = count_{rep}(out(ap_i)) = 0$.

Hence, $0 \leq \mu_{auth}(ap_i) \leq 2$.

Compliance Metrics - These metrics depict the level of compliance of implemented security processes with enterprise's objectives and policies, laws, regulations and contracts. Compliance objects (policies, laws, contracts etc.) comprise of sets of *to-do activities*. These activities can be mapped to implemented security controls, processes and techniques. Gap Analysis may be performed to identify compliance gaps. Weighted averages of gaps (with policies, laws, contracts etc.) generate different types of compliance metrics, namely Policy-compliance, Legal / Regulatory compliance and Contractual-compliance metrics.

Policy Compliance Metric - Information security policies state the objectives of an enterprise with respect to establishment of security practices and techniques. Examples of policies are Acceptable Use Policy, Access Control Policy, Anti-Virus Policy, Backup Policy, E-Mail Policy, Incident Management Policy etc. Evidence of implementation and enforcement of a policy is demonstrated with the help of records, which can be maintained either as physical documents or soft copies. Successful implementation of a security policy signifies execution of the statements specified in the policy document.

An enterprise should assign relative weights (w_i) to policy statements in [0, 1] based on their priorities ("1" signifies highest priority). Implementation scores (s_i) of policy statements can be obtained in [0, 1] by analyzing corresponding records ("1" means "completely implemented"). The policy compliance metric ${}^{comp}\mu_{py}(py_i)$ for policy py_i can be computed as follows:

$$ {}^{comp}\mu_{py}(py_i) = \Sigma\, w_i s_i \;\Big|\; 0 \le w_i,\, s_i \le 1 \text{ and } \Sigma\, w_i = 1 \qquad (3)$$

Table 2 lists some statements of Backup Policy, along with a sample assignment of relative weights. It also shows the implementation scores of policy statements for a particular measurement period. Hence, the compliance metric for backup policy is:

$$ {}^{comp}\mu_{py}(\text{Backup Policy}) = (0.30 * 1) + (0.25 * 0.8) + (0.20 * 0.5) + (0.25 * 0.9) $$
$$ = 0.825 \approx 0.8 $$

Table 2. Sample Statements of Backup Policy, their Relative Weights, Implementation Scores.

Policy Statement	Rel. Wt. (w_i)	Imp. Score (s_i)
All critical information shall be backed up periodically.	0.30	1
The backup media shall be stored with sufficient protection.	0.25	0.8
Backup copies of critical information system software shall not be stored in the same location as the operational software.	0.20	0.5
Backup information shall be tested at some specified frequency.	0.25	0.9

It may be seen that $0 \le {}^{comp}\mu_{py}(py_i) \le 1$; ${}^{comp}\mu_{py}(py_i)$ has a value 0 when *none* of the statements of policy p_i has been implemented, while it has max. value 1 when the policy has been completely implemented. Compliance metrics for individual policies can be combined to obtain the overall Policy Compliance Metric for the enterprise:

$$ {}^{comp}\mu_{py} = \Sigma\, (w_i * {}^{comp}\mu_{py}(py_i)) \;\Big|\; 0 \le w_i \le 1 \text{ and } \Sigma\, w_i = 1 \qquad (4)$$

Here, w_i denote the weights that can be assigned to individual policy compliance metrics as per their relative importance. The weights may vary depending on the specific requirements and priorities of the enterprise. ${}^{comp}\mu_{py}$ signifies the status of compliance of the entire enterprise with respect to applicable security policies.

Legal / Regulatory Compliance Metric - Laws and Regulations that are applicable to an enterprise need to be identified and implemented. Examples include IT Act, Privacy Laws, Cryptographic Laws, Reserve Bank of India (RBI) regulations for Indian banks and financial institutions etc. Like policy statements, applicable provisions and sections of laws and regulations should be listed, and relative weights (w_i) should be assigned as per their priorities. Records of implementation should be maintained as evidence of legal and regulatory compliance. There is a difference between implementation of policies and laws / regulations; the latter are either implemented in totality, or not implemented at all. Partial implementation of laws and regulations is not acceptable to authorities. Hence, in case of legal / regulatory compliance metrics, implementation scores (s_i) assume binary values. If a section or provision has been implemented completely, the value of s_i is 1; else it is 0.

Legal / regulatory compliance metric ${}^{comp}\mu_{lg}(lg_i)$ for law / regulation lr_i can be computed as follows:

$$ {}^{comp}\mu_{lr}(lr_i) = \Sigma\, w_i s_i \;\big|\; 0 \leq w_i \leq 1,\, \Sigma\, w_i = 1,\, s_i\, \varepsilon\, \{0, 1\} \qquad (5)$$

Like policy compliance metric, $0 \leq {}^{comp}\mu_{lr}(lr_i) \leq 1$.

Compliance metrics for individual laws and regulations can be combined to derive the overall Legal / Regulatory Compliance Metric for the enterprise as follows:

$$ {}^{lr}\mu_{comp} = \Sigma\, (w_i * {}^{comp}\mu_{lr}(lr_i)) \;\big|\; 0 \leq w_i \leq 1,\, \Sigma\, w_i = 1 \qquad (6)$$

Here, w_i denote the weights that can be assigned to individual legal / regulatory compliance metrics as per their significance. ${}^{comp}\mu_{lr}$ gives the status of compliance of the entire enterprise with respect to applicable laws and regulations.

Contractual Compliance Metric - An enterprise may enter into contracts with third parties for supply of goods, software, services, personnel etc. Such contracts define terms and conditions to be followed by the participating enterprises, including service levels. It is important to periodically check for compliance with the terms of contracts so that deviations can be detected and corrected early.

The executable items of a contract need to be identified and prioritized by an enterprise. Based on the priorities, relative weights have to be assigned to each item. As in case of legal and regulatory compliance, partial fulfillment of a feature, or contract item, does not hold any significance. A feature is either implemented fully, or not implemented at all. Hence, using notations similar to the ones for legal / regulatory compliance metric, contractual compliance metric ${}^{comp}\mu_{ct}(ct_i)$ for contract ct_i is given by:

$$ {}^{comp}\mu_{ct}(ct_i) = \Sigma\, w_i s_i \;\big|\; 0 \leq w_i \leq 1,\, \Sigma\, w_i = 1,\, s_i\, \varepsilon\, \{0, 1\} \qquad (7)$$

As is obvious, $0 \leq {}^{comp}\mu_{ct}(ct_i) \leq 1$. The composite Contractual Compliance Metric for all applicable contracts of an enterprise is obtained as:

$$ {}^{comp}\mu_{ct} = \Sigma\, (w_i * {}^{comp}\mu_{ct}(ct_i)) \;\big|\; 0 \leq w_i \leq 1,\, \Sigma\, w_i = 1 \qquad (8)$$

Here, w_i denote the relative weights of individual contractual compliance metrics.

Composite Compliance Metric - It may be important for senior management of an enterprise to obtain an overall idea about the status of compliance of its business and management functions with applicable policies, laws, regulations and contracts. The composite compliance metric would serve this purpose and is computed by combining the values of individual compliance metrics in a specified proportion. Thus,

$$ {}^{comp}\mu = (w_1 * {}^{comp}\mu_{py}) + (w_2 * {}^{comp}\mu_{lr}) + (w_3 * {}^{comp}\mu_{ct}) \;\big|\; 0 \leq w_i \leq 1,\, \Sigma\, w_i = 1 \quad (9)$$

Here, w_1, w_2 and w_3 represent relative weights of individual compliance metrics. It is obvious from Equations (4), (6) and (8) that $0 \leq {}^{comp}\mu \leq 1$. Legal / regulatory compliance of an enterprise is more critical than others; also, compliance to policies may be, in general, least significant in the overall compliance wheel. Hence, the following values of relative weights are suggested for computing ${}^{comp}\mu$: $w_2 = 0.5$, $w_3 = 0.3$, $w_1 = 0.2$. Thus, following this scheme,

$$ {}^{comp}\mu = (0.2 * {}^{comp}\mu_{py}) + (0.4 * {}^{comp}\mu_{lr}) + (0.3 * {}^{comp}\mu_{rg}) + (0.1 * {}^{comp}\mu_{ct}) \qquad (10)$$

However, an enterprise may choose the values of relative weights based on its specific requirements.

Effectiveness Metrics - These metrics measure the effectiveness of implemented ISMS processes and controls; this includes all security management activities like business continuity management, threat management, incident management, asset management, awareness, education and training programmes etc. As stated above, ISMS processes and controls address stakeholder concerns, enterprise objectives, risks, and legal / regulatory issues. It is important to check the effectiveness and performance of the processes and controls vis-à-vis the security needs.

While *compliance metrics* help measure the conformance of implemented processes to various compliance objects, *effectiveness metrics* produce measures that indicate whether the processes have been actually successful in securing the enterprise. There are different ways in which such effectiveness can be measured.

Risk Mitigation Metric - The amount of risk that is mitigated by implementation of a process produces risk mitigation metric. This can be measured at an asset-, business process-, or enterprise-level, whose criticality is considered while computing the metric. A process that is able to reduce risk to a critical asset (or business process, or enterprise) is considered to be more effective than one that reduces risk to a non-critical asset. Also, this metric can assume different values at different points of time. For example, it may be the case that a control (say, a firewall) is able to mitigate risk (say, unauthorized access to a bank's online portal) at a particular time of day (when network traffic is low), but it is not able to do so during other times (when network traffic is high).

Considering the above factors, the value of risk mitigation metric, ${}^{rmit}\mu_{tc}(pr_j)$, at time t_c, for a process (or control) pr_j, can be computed as follows:

$$ {}^{rmit}\mu_{tc}(pr_j) = (\Sigma\, cr(a_i) * rf_r(a_i)) / n$$

$$\text{where, } rf_r(a_i) = \begin{cases} (rf_o(a_i) - rf_c(a_i)) / rf_o(a_i), \text{ if } rf_o(a_i) \geq rf_c(a_i) \\ (rf_o(a_i) - rf_c(a_i)) / rf_c(a_i), \text{ if } rf_o(a_i) < rf_c(a_i) \end{cases} \qquad (11)$$

Here, $a_1, \ldots, a_n$ denote the assets whose risks are supposed to be addressed by pr_j; $cr(a_i)\ \varepsilon\ \{1, 2, 3\}$ represents criticality of asset a_i (or business process, or enterprise); $rf_o(a_i)$ denotes original risk factor (that is, before implementation of process or control) of asset a_i (or business process, or enterprise); and $rf_c(a_i)$ denotes current risk factor (at time t_c) of asset a_i (or business process, or enterprise). Values of criticality are assigned as follows: $cr(a_i) = 1$ if loss of asset a_i has limited adverse impact on the business of an enterprise; $cr(a_i) = 2$ if loss of a_i has serious adverse impact on enterprise business; and $cr(a_i) = 3$ if loss of a_i causes severe or catastrophic adverse impact on the business of an enterprise. The value of ${}^{rmit}\mu_{tc}(pr_j)$ for a process (or control) pr_j is computed by considering all assets (or business processes, or the entire enterprise) whose risks are supposed to be addressed by pr_j; this is obvious from the summation (Σ) used in Equation (11).

It may be observed that the value of $rf_r(a_i)$ can be positive or negative depending on the relative values of $rf_o(a_i)$ and $rf_c(a_i)$. $rf_o(a_i)$ will be greater than $rf_c(a_i)$ if the implemented process (or control) is successful in mitigating the risk, leading to $rf_r(a_i)$ having positive value. $rf_r(a_i)$ will be zero if the process has failed to mitigate the corresponding risk. On the other hand, negative value of $rf_r(a_i)$ indicates that the implemented process (or control) has actually *increased* the risk; this is a cause for serious concern and should be corrected without delay.

Since, $cr(a_i) \varepsilon \{1, 2, 3\}$ and $-1 \leq rf_r(a_i) \leq 1$, the value of each product $cr(a_i) * rf_r(a_i)$ belongs to [-3, 3]. Hence, $-3 \leq {}^{rmit}\mu_{tc}(pr_j) \leq 3$.

Incident Metric - This measures the incidents that occur despite implementation of security processes. The reason could be either, a) improper / incomplete implementation, or b) non-implementation of relevant processes owing to lack of correct identification of security needs. Hence, these metrics can be classified as i) *Controlled* incident metrics, and ii) *Uncontrolled* incident metrics. An incident may cause breach of security and / or privacy parameters, physical loss of IT assets, financial loss, loss of image or reputation, or destruction of lives. Examples include buffer overflows, malware attacks, theft of assets etc. An incident may be classified as low-impact (causing limited adverse effect on enterprise business), medium-impact (serious adverse effect), or high-impact (severe or catastrophic adverse effect) [6]. Different enterprises may perceive criticality of impacts differently, depending on the significance of those impacts on their business processes. For example, while defense-sector organizations may consider loss of confidentiality to be of serious concern, the entire business of an e-commerce organization may revolve around maximizing information dissemination. In case of the latter, loss of availability of product information may have serious consequences.

Controlled Incident Metric - An enterprise should detect and record all information security-related incidents and quantify their impacts to business processes. All such incidents, which have occurred during a period of measurement, are grouped according to the corresponding security processes or controls (that had been implemented to prevent these incidents). The value of controlled incident metric, ${}^{cinc}\mu_{tp}(pr_j)$, for period of measurement t_p, for a process (or control) pr_j, can be computed as follows:

$$ {}^{cinc}\mu_{tp}(pr_j) = \begin{cases} 3 - (\Sigma \, Imp(In_i) \, / \, n), \text{ if } n > 0 \\ 3, \text{ otherwise} \end{cases} $$

$$ \text{where, } Imp(In_i) \text{ denotes the impact of incident } In_i \qquad (12) $$

Here, $In_1, \ldots, In_n$ denote the relevant incidents that have occurred during measurement period t_p.

Values of impact of incidents are assigned as follows: $Imp(In_i) = 1$ for low-impact incidents; $Imp(In_i) = 2$ for medium-impact incidents; and $Imp(In_i) = 3$ if impact is high. Since, $Imp(In_i) \varepsilon \{1, 2, 3\}$, $0 \leq {}^{cinc}\mu_{tp}(pr_j) \leq 3$. It may be noted from Equation (12) that the value of the metric is obtained after subtracting it from 3. This has been done in order to maintain uniformity in interpretation of metrics; higher value of a metric indicates positive result, that is proper ISMS implementation, while lower value means the security processes and controls have not been implemented correctly.

Uncontrolled Incident Metric - This metric provides the impact value of all information security-related incidents for which no relevant processes or controls have been implemented. The value of uncontrolled incident metric, ${}^{uinc}\mu_{tp}$, for period of measurement t_p can be computed as follows:

$$
{}^{uinc}\mu_{tp} = \begin{cases} \Sigma\ \mathrm{Imp}(\mathrm{In}_i) / n, \text{ if } n > 0 \\ 0, \text{ otherwise} \end{cases}
$$

where, Imp(In$_i$) denotes the impact of incident In$_i$ (13)

Here, In$_1$, …, In$_n$ denote the *uncontrolled* incidents that have occurred during measurement period t$_p$. As in the case of controlled incident metric, $0 \leq {}^{uinc}\mu_{tp} \leq 3$.

Process Effectiveness Metric - Risk mitigation metric and controlled incident metric can be combined to derive the effectiveness metric for an ISMS process or security control. For a measurement period t$_p$, the value of process effectiveness metric, ${}^{efct}\mu_{tp}(pr_j)$, for a process or control, pr$_j$, can be obtained as follows:

$$
{}^{efct}\mu_{tp}(pr_j) = \mathit{floor}(({}^{rmit}\mu_{tc}(pr_j) + {}^{cinc}\mu_{tp}(pr_j)) / 2) \quad (14)
$$

The *floor* function has been used in order to derive a conservative estimate of process effectiveness in case of floating point values. An enterprise should always strive to achieve greater security by continually improving its ISMS implementation. Hence, a conservative estimate will help to put things in perspective and spur the enterprise towards better security implementation.

From Equations (11), (12), and (14), it may be seen that ${}^{efct}\mu_{tp}(pr_j)\ \varepsilon\ \{-2, -1, 0, 1, 2, 3\}$.

Efficiency Metrics - This measures the ability of implemented security processes and controls to address security concerns efficiently. Each security concern can be assigned a weight based on its priority. Priority of a concern usually considers business objectives of an enterprise, along with security issues. A process or control is judged for efficiency based on the *amount* of security concerns it addresses. *Amount* means no. of security needs along with their relative weights. *Time* and *cost* are also factored in to consider the amount of time and resources (money, manpower and infrastructure) needed to address the corresponding concern, and implement the process or control, respectively. The value of efficiency metric, ${}^{effy}\mu_{tc}(pr_j)$, at time t$_c$, for a process (or control) pr$_j$, can be computed as follows:

$$
{}^{effy}\mu_{tc}(pr_j) = \mathit{floor}((\Sigma\ p(a_i) / (t_i(pr_j) * c_i(pr_j))) / n) \quad (15)
$$

Here, p(a$_i$) = priority of the security concern of asset a$_i$ being addressed by pr$_j$; t$_i$(pr$_j$) = time needed by pr$_j$ to address the security concern of asset a$_i$; c$_i$(pr$_j$) = cost of implementation of pr$_j$; and a$_1$, …, a$_n$ denote the assets whose security concerns are supposed to be addressed by pr$_j$.

Priority of a concern p(a$_i$) can be assigned on a 3-point scale {1, 2, 3} based on its relative importance, with 3 signifying highest priority. In order to estimate cost of implementation and time elapsed to address the concern, thresholds can be defined. For example, an enterprise may define a time threshold and a cost threshold, t$_o$ and c$_o$, for each security concern. t$_i$(pr$_j$) can be determined as follows: t$_i$(pr$_j$) = 3 if the time that was needed to address the concern was greater than the threshold ($t_i(pr_j) > t_o$); t$_i$(pr$_j$) = 2 if the time needed was equal to or just less than the threshold ($t_i(pr_j) \leq t_o$); and t$_i$(pr$_j$) = 1 if the time needed to address the concern was very less as compared to the threshold ($t_i(pr_j) \ll t_o$). It may be noted that at any point in time only those cases are considered in computing ${}^{effy}\mu_{tc}(pr_j)$ where either the security concern has been addressed, or the threshold t$_o$ has already been exceeded. The value of c$_i$(pr$_j$) can be assigned similarly on a 3-point scale.

From the above discussion, it can be seen that ${}^{effy}\mu_{tc}(pr_j)\ \varepsilon\ \{0, 1, 2, 3\}$.

6 Mapping ISMS Metrics to Stakeholder Concerns

In this section, the proposed ISMS metrics are mapped to the security and privacy concerns of stakeholders.

Security of Business Processes and information assets – Since risk is the measure of insecurity with respect to the security and privacy parameters of assets, the value of *risk metric* can be used to provide appropriate information regarding this concern.

Safety of client data – Since this concern is addressed by ensuring the protection of C, I, A, anonymity, unlinkability and undetectability, the value of *risk metric* can provide proper idea regarding the safety of client data. Besides, enterprise policies ensure protection of assets. Hence, *policy compliance metric* will serve to provide assurance regarding relevant policies for the protection of client data.

Safety of personal data and assets – This is similar to the previous case. Here, too, *risk metric* and *policy compliance metric* provide appropriate information.

Reputation of enterprise – Since this is related to the image / reputation of an enterprise, the values of compliance metrics can be used to judge the same. Specifically, *legal / regulatory compliance metric* and *contractual compliance metric* will reflect on the reputation of the enterprise. The enterprise will also be judged on the presence / absence of incidents. Hence, *controlled incident metric* and *uncontrolled incident metric* are also important for this concern. Finally, the absence of risk within enterprise assets can serve to enhance its reputation; thus, *risk metric* is also significant here.

Efficacy of the implemented ISMS – The efficacy of implemented ISMS can be understood by computing its efficiency and ascertaining the amount of risk that has been mitigated, and the reduction in the number of security / privacy incidents. Hence, the metrics that are important are *risk mitigation metric*, *controlled incident metric*, *uncontrolled incident metric*, *process effectiveness metric*, and *efficiency metric*. Uncontrolled incident metric has been considered here as absence of controls, either deliberately or due to oversight, is an inherent feature of the implemented ISMS.

Accountability for others' misdeeds – This pertains to operational personnel and third parties and concerns the parameters accountability, non-repudiation and image / reputation. Hence, the metrics that can provide useful insight are *risk metric* (to understand the protection mechanisms implemented), *non-repudiation metric*, *policy compliance metric* (to understand relevant enterprise policies), *legal / regulatory compliance metric* (to understand the legal protection angle for this concern), *contractual compliance metric* (in case of third parties) and *composite compliance metric*.

Legal protection of consumer rights – Since this concerns legal protection, *legal / regulatory compliance metric* and *contractual compliance metric* are relevant here.

Protection of legal and contractual obligations – Since these concern the legal and contractual obligations pertaining to third parties, *legal / regulatory compliance metric* and *contractual compliance metric* are relevant here.

Security of nation – As discussed earlier, this addresses the protection of integrity and availability of national assets, and accountability and legal and contractual obligations of the nation. Hence, the metrics that can shed light here are *risk metric* (to know the status of integrity and availability of national assets); *controlled incident* *metric* and *uncontrolled incident metric* (to know whether incidents pertaining to national security have occurred); *legal / regulatory compliance metric* and *contractual compliance metric*.

Reputation of nation – This concern needs metrics like in the previous case, that is *risk metric, controlled incident metric, uncontrolled incident metric, legal / regulatory compliance metric* and *contractual compliance metric*.

Compliance – All compliance metrics are relevant for this security concern, that is *policy compliance metric, legal / regulatory compliance metric, contractual compliance metric* and *composite compliance metric*.

Thus, the proposed metrics have been mapped to the identified security and privacy concerns of stakeholders. This is summarized in Table 1 (columns 2 and 4). This will provide assurance to the stakeholders of an enterprise regarding their specific concerns, and allow them to make informed decisions pertaining to their future course of actions.

7 Conclusion and Future Work

In this paper, the different categories of stakeholders of an enterprise have been identified. It has been shown that the stakeholders have separate security and privacy concerns as their job functions, responsibilities and expectations are different. The concerns, in essence, translate to requirements for the protection of specific security and privacy parameters of assets. These requirements are addressed by establishing ISMS within the enterprise. The paper has described how the identified concerns can be translated to such protection requirements; this will help an enterprise to design and implement an ISMS that caters to the requirements of all its stakeholders.

In order to assure stakeholders regarding the efficacy of the established ISMS, and status of protection of the security and privacy of their assets, it is essential to continually generate and convey relevant metrics. The paper has defined a set of comprehensive metrics for ISMS that address the requirements of ISO/IEC 27001 standard [3]. The metrics have been designed so that they correspond to the concerns of stakeholders and they can obtain assurance regarding their protection needs.

Future work is geared towards the design of algorithms corresponding to the metrics defined in this paper. A tool can be developed that generates attacks (for example, using attack graph methodology) and utilizes these algorithms to generate corresponding metrics for an enterprise ISMS.

References

1. The International Organization for Standardization, The International Electrotechnical Commission: ISO/IEC 27005, Information technology – Security techniques – Information security risk management. 3rd edn. ISO/IEC, Switzerland (2018).
2. Santos, J. C. S., Tarrit, K., Mirakhorli, M.: A Catalog of Security Architecture Weaknesses. In: Proceedings of 2017 IEEE International Conference on Software Architecture Workshops (ICSAW), pp. 220 – 223. IEEE, Sweden (2017).

3. The International Organization for Standardization, The International Electrotechnical Commission: ISO/IEC 27001, Information technology – Security techniques – Information security management systems - Requirements. 2nd edn. ISO/IEC, Switzerland (2013).
4. The International Organization for Standardization, The International Electrotechnical Commission: ISO/IEC 27004, Information technology – Security techniques - Information security management - Monitoring, measurement, analysis and evaluation. 2nd edn. ISO/IEC, Switzerland (2016).
5. National Institute of Standards and Technology: NIST SP 800-55, Performance Measurement Guide for Information Security. 1st rev. NIST, USA (2008).
6. National Institute of Standards and Technology: NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations. 4th rev. NIST, USA (2013).
7. Chen, H., Cho, J-H., Xu, S.: Quantifying the Security Effectiveness of Firewalls and DMZs. In: Proceedings of Fifth Annual Symposium and Bootcamp on Hot Topics in the Science of Security (HoTSoS), pp. 1 – 11. ACM, USA (2018).
8. Ulvila, J. W., Gaffney, J. E. Jr: Evaluation of Intrusion Detection Systems. Journal of Research of the National Institute of Standards and Technology 108(6), 453–473 (2003).
9. Scala, N., Reilly, A., Goethals, P., Cukier, M.: Risk and the Five Hard Problems of Cybersecurity. Risk Analysis 39(10), 2119-2126 (2019).
10. Pendleton, M., Garcia-Lebron, R., Cho, J-H., Xu, S.: A Survey on Systems Security Metrics. ACM Computing Surveys 49(4), 62:1-35 (2017).
11. Tupper, M., Zincir-Heywood, A. N.: VEA-bility Security Metric: A Network Security Analysis Tool. In: Proceedings of Third International Conference on Availability, Reliability and Security (ARES 2008), pp. 950-957. IEEE, Spain (2008).
12. Patriciu, V-V., Priescu, I., Nicolaescu, S.: Security Metrics for Enterprise Information Systems. Journal of Applied Quantitative Methods 1(2), 151-159 (2006).
13. Foroughi, F.: Information Security Risk Assessment by Using Bayesian Learning Technique. Lecture Notes in Engineering and Computer Science 2170(1), 91-95 (2008).
14. Gao, G., Li, X-Y., Zhang, B-J., Xiao, W.: Information Security Risk Assessment Based on Information Measure and Fuzzy Clustering. Journal of Software 6(11), 2159-2166 (2011).
15. Johnson, G.: Measuring ISO 27001 ISMS Processes. Neupart Information Security Management (2014), https://cdn2.hubspot.net/hubfs/163742/pdf_files/iso27001isms-kpi.pdf?t=1438891985360, last accessed 2021/06/12.
16. Aldya, A. P., Sutikno, S., Rosmansyah, Y.: Measuring effectiveness of control of information security management system based on SNI ISO/IEC 27004: 2013 standard. IOP Conference Series: Materials Science and Engineering 550, 1-11 (2019).
17. Monev, V.: Organisational Information Security Maturity Assessment Based on ISO 27001 and ISO 27002. In: Proceedings of 2020 International Conference on Information Technologies (InfoTech), pp. 1-5. IEEE, Bulgaria (2020).
18. Mödinger, M.: Metrics and Key Performance Indicators for Information Security Reports of Universities. Master’s Thesis. Hochschule Augsburg University of Applied Sciences, Welden (2019).
19. The International Organization for Standardization, The International Electrotechnical Commission: ISO/IEC 27002:2013, Information technology – Security techniques - Code of practice for information security controls. 2nd edn. ISO/IEC, Switzerland (2013).
20. Pfitzmann, A., Hansen, M.: A Terminology for Talking about Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management (2010), https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf, last accessed 2021/10/10.