Developing An Empirical Relationship
To Propose An Information Security
Assurance Model For Collaborating
Business Processes

D. Vinod\textsuperscript{1} and S. Chandrasekaran\textsuperscript{2}
\textsuperscript{1}Research Scholar,
Department of Computer Science and Engineering,
Sathyabama University,
Chennai - 600 119 Tamil Nadu, INDIA
vinoitkid2010@gmail.com
\textsuperscript{2}Professor Department of Computer Science and Engineering,
Sri Ranganathar institute of Engineering and technology,
Coimbatore Tamil Nadu, INDIA
January 4, 2018

Abstract

During the last few decades, organizations have re-engineered business processes on the back of digital data and computer networks. Recently, organizations are beginning to realize that increased accessibility, and productivity, carries a hidden cost of making the data more vulnerable in security breaches. It makes intuitive sense to incorporate information security into strategic decision-making during business process. Consequentially, companies are often enhanced sub-optimally retrofit security into their business processes in response to security breaches. The present investigation presents an information security risk analysis proactively conducted at an internationally well renowned business organization. The prime goal of the study was to
propose an information security assurance model for collaborating business processes. The business processes have to handle sensitive information either in structured or unstructured forms that may be leaked by security flaws in business transactions. An empirical model of a risk based enhanced security for business processes is proposed with suitable metrics during the integration of the structured and unstructured information for business continuity. This research also describes the dynamic activation of appropriate safeguards; prevention and recovery from risks due to both the structured and unstructured information were considered. The expected business continuity (EBC) in business importance and attack security index is proposed from the standards towards the security compliances.

**Key Words and Phrases:** Security Assurance; Business Continuity; Attack Severity; Compliance; Geni tool;

1 Introduction

Business organizations are more dependent than ever on the reliable operation of their information systems. Yet institutions worldwide face increasing security threats that can undermine the operation of these systems. Considering today’s high threat cyber environment, organizations need security assurance models to protect their valuable information [Kenneth et.al, 2009].

Forces like global market, mounting expectations and requirements of the customers and advances in enabling integration technologies [Chalmeta et.al, 2001] push enterprises to take advantage of the possibility to access information over any distance. Web technologies enable today ICT-supported business processes within global enterprises and across enterprise boundaries [Braa and Roland, 2000; Leem and Kim, 2002; Britton and Bye, 2004; Linthicum, 2004]. However, there are numerous questions to be solved before the information systems of collaborating business partners can be set up and made accessible for the exchange of information, independent of the geographic location of the sites of the partners. A core issue in building e-services partnerships are mutual trust [Heikkila et.al, 2005]. To build trust in cases where the provisioning of the service requires exchange of data between the business
information systems of the partners, one of the first thresholds to overcome is the protection or security of the information systems and data from unauthorized access. However, remote services feature a promising business opportunity.

Information security is critical to ensure the integrity and confidentiality of structured and unstructured information in business processes. A business process is a collection of related, structured activities or tasks that produce a specific service or product for a particular customer or customers. These activities are handling a huge size of unstructured and structured information where the unstructured information is a direct product of human communication. Since the unstructured information represents the largest, most current and fastest growing source of knowledge available to businesses and governments worldwide, they have to be secured.

The earlier information security model address the business outcome, importance of assets needed for the business and also the recovery time for the assets after the attacks are so as to put them into use for business days [Anita and Labuschagne, 2005]. The proposed model from the literature discussed here categorizes the assets into different types without concentrating its data types or structure. The attacks especially the insider threats are more severe and possibly in the case of unstructured information in the business communications like email or design documents. In another model, an objective analysis is performed for the probability assessment of threats to information systems through a possible reasonable approach for a risk management system to manage these threats [Fariborzet.al, 2003]. The earlier research proposes poly-instantiateion that allows the use of cover stories in databases which appear differently to users different security classes while maintaining consistency relative to any one particular user. In another approach, the potential information leakage through conciliation and a rescheduling policy for higher secrecy action is studied [Keith et.al, 2008]. The throughput, operational cost, and compliance of the information have to be analyzed towards the effects of loss of such information. The security engineers should resist the temptation to view information security requirements as a collection of technical mechanism and should focus on the business impact of security failures [Ivan Tirado, 2008].
2 Related Works

The attacker can then damage the asset by degrading its confidentiality, integrity, or availability thereby causing potential business losses. In case of a number of business processes that are collaborating the vulnerabilities may originate from technology, people or processes that are viewed as flaws in the implementation of software and hardware. In information security, however, verification has to be done involving more entities, such as security specification, security policy, security mechanisms etc. [Andy Juan Wang, 2005]. The internal policy is the base for regulatory compliance, practice and insider incident prevention. The policy defines and governs actions and behaviors of personnel within an organization. It is vital that an organizations information is protected not only for the business operations but for client security as well. In an earlier investigation, a responsibility driven distributed system is proposed, where exceptions needing immediate attention are conveyed to the right person in minimum possible time [Michael DCarroll, 2006]. The information security model has encompassed all security incidents that can be deliberate or accidental and can be caused both by technical and physical means to damage to the information or database assets of the organization. The internet acts as a source of potential IS incidents and events, but at the same time as a source of information for the vulnerability monitoring process. It is generally a good idea to purchase a document imaging system that offers the maximum capabilities to deal with both types of documents, rather than purchasing a system that caters only to a single document type [Bhilare, 2009]. The goal of the risk mitigation, monitoring and management plan is to identify as many potential risks as possible. When all risks have been identified, they will then be evaluated to determine their probability of occurrence, and how Game Forge will be affected if they do occur. Plans will then be made to avoid each risk, to track each risk to determine if it is more or less likely to occur, and to plan for those risks should they occur [Anna, 2004]. In the earlier information security incidents, the dynamic activation of appropriate safeguards, prevention and recovery from risks due to unstructured information were not considered. Since business processes and transactions are performed in parallel and the concurrent business principles force collaborated
to ease the collaboration through the following requirements:

- Dynamic activation of appropriate safeguards, prevention and recovery from risks due to structured and unstructured information.

- The security management team must define a set of managed processes which should be developed and maintained for business continuity throughout the organization.

- Provide secure transparency against the risks due to security breach which leads to loss of confidentiality (LOC) and loss of integrity (LOI) of the information assets needed for the business processes.

- Provide easy access to business data of the business partners if granted;

- By providing information security assurance, the process assessment and its compliance are carried to estimate the probabilities of potential risks and possible attacks based on the vulnerabilities.

- The business processes should be continued and the resulting risks are estimated to minimize the loss with the presence of explicit or implicit attacks too.

To tackle the issues collaboration in a distributed environment and dynamic data sharing and security, this paper describes the concept of security assurance and the business continuity along with the estimation of minimizing loss in the presence of explicit or implicit attacks. From the published literature, it was understood that the very few investigations has been carried out to deal with the information security management model to continue the business transactions in structured and unstructured information. Hence the present investigations focused on developing an empirical relationship to propose an integrated information security management model and its risks when a number of processes are collaborating to continue business transactions dealing structured and unstructured information. Furthermore, expected business continuity (EBC) in terms of business importance and attack security index is proposed from the standards towards the security compliances.
3 Integrated Information Governance, Risk And Compliance

The information assets are recognized as values to the organization where an asset is any tangible or intangible thing that has value to an organization. They are not easily replaceable without cost, skill, time, resources and they form a part of the organizations corporate identity, without which, the organization may be threatened. The data or asset classification would normally be proprietary, highly confidential or even top secret. The information security governance (ISG) indicates the objectives and operations about the security incidents that had happened or may happen inside or outside the organization. Information security governance can be defined as representing the framework for decision rights and accountabilities to encourage desirable behavior in the use of IT (Weill, 2004). Some respondents in similar previous studies felt that information security itself must be viewed as a governance issue stating, Information security is often treated as a technology issue, when it really should be treated as a governance issue. Some others have suggested that failing to realize that information security is a corporate governance responsibility is the number one deadly sin of information security management (Von Solms R and Von Solms B, 2004).

The focus of governance is to identify the various risks and security compliance (ISC) in different directions and dimensions so as to take decisions that defines the expectations to grant the regulatory processes. It was motivated that the acceptance and implementation of an ISG framework are an important action in securing business information through the protection of information systems, acting in accordance with legislation, as well as improving the efficiency of business operations, amongst other things [Entrust, 2004]. Thus information, security governance enables an organization to effectively full fill all the internal and external requirements in terms of protecting business information assets and, therefore, covers the full scope of risks faced by an organization in this regard. These security requirements could be viewed as information risk directives that would advise executive management on what should be done in order to govern and manage information security properly. The information security risk (ISR) analysis based on the
business processes is configured not only to regulate the processes but also report the necessary updates. Risk analysis can be done to an asset or a group of assets with two different objectives: one is for identification of all possible risks associated with the assets due to their vulnerability and another is for improving the vulnerabilities using safeguards or firewalls. Managing information security risks requires a suitable risk assessment and risk treatment method which may include an estimation of the costs and benefits, legal requirements, social, economical and environmental aspects, the concerns of stakeholders, priorities, and other inputs and variables as appropriate.

Fig. 1 Information Security Governance, Risk, Compliance relationship

The governance, risk and compliance of the information assets of a business organization can be analyzed through their relationships as shown in Figure 1. The results of the information security risk assessment will help to guide and determine the appropriate management treatment decisions for action and prioritization for managing information security risks, and for implementing relevant security controls to protect against these risks. The ISO/IEC 27005 standard provides information security risk management guidance,
including advice on risk assessment, risk treatment, risk acceptance, risk communication, risk monitoring and risk review. Risk analysis uses information to identify possible sources of risk. It uses the information to identify threats or events that could have a harmful impact. It then estimates the risk by asking: What is the probability that this event will actually occur in the future and acting according to the identification of security risk by following certain standards. The management action will proceed by processing the security incidents.

4 Business Information Structure, Security and Standards

Once a company has completed its risk analysis process it needs to design its own customized control framework (providing guidance, policies and processes) to address its risks. Once the company’s control framework has been designed and agreed upon, the company should build an internal control system (the interactive pieces that enable the operation of the framework) [Stephen and von Solms, 2009]. An information security incident is made up of one or more unwanted or unexpected information security events that could very likely compromise the security of information and weaken or impair the business processes. The failure of information security affects the strategy and objective of an organization and it stops the developmental business activities. The risk analysis can be done based on the business security policies and initiate the activities in order to minimize the information loss in an organization. The security standards must identify not only the assets targeted in the business processes but also the possibility and potential risks either due to the inside threats through information leakage or the outside adversaries. The organizational security and privacy policies are to be drawn in such a manner so as to comply with the existing regulations or they can demand revised regulations duly approved by the business communities. This is highly depended on the mission and business goal of the organization in the current competitive business world.

The importance of defining and declaring new business functions and activities through outsourcing or through virtual organi-
zational setups is based on the business model what they want to follow. The attacker and the insider threat will try to access the information assets irrespective of its structure and location. The size and the type of such assets are to be kept confidential for the successful business continuity. It is logically correct if the confidential information is vulnerable to different attackers then the risk is sure. But the security management team must define a set of managed processes which should be developed and maintained for business continuity throughout the organization. While defining a security management process, the team faces many challenges which are not primarily based on the conventional attacks and vulnerabilities but on the very structure and location of the information assets. For example, a highly confidential design data set of an automotive part may be hidden and sent as a sequence of numbers through an email or sent as an image placed in the attachment. Similarly video frames and audio segments may contain very sensitive information and are being sent through personal networks or social networks. There may be some hidden business between the information exchanges knowingly or unknowingly. The business loss and the reputation damage are very high in the case of illegal document release and untimed release of legal evidences through networking. In all these scenarios, the computational structure of the information is the most important criteria in managing the security activities. Hence the structure of information can be represented as a tuple of $\langle$ Identity of Info, Uniqueness, Location, Size $\rangle$ where the identity is a kind of token or a valid keyword pertaining to the business. For illustration, the identity can be expressed as a name or a type or an instance and as a parameter that is hidden or explicit. The uniqueness of the structure can be expressed as a member in the set of $\{$Context, Content, Pixel, Mixed$\}$. Similarly the location feature of the information asset or its cyber markup can be expressed as a member in the set of User Defined, Static, Dynamic, Random. The information size which plays a vital role in the end user transaction as the raw information which may be of types belonging to a set of elements like Computational, Application, Duration, Resolution as shown in Table 1.
example, the structuredness of a design data from a product center is very well represented by its identity name or number and its data type with all its related names or fields mentioned explicitly or implicit in the information exchange. The information assets belonging to business community have to be secured to continue the business in a satisfying manner even in the presence of security flaws. These security flaws or vulnerabilities have to be handled by both the clients and also the service providers as per the existing standards. This International Standard will provide practical implementation guidance and provide further information for establishing, implementing, operating, monitoring, reviewing, maintaining and improving Information Security Management Services (ISMS) in accordance with ISO/IEC 27001 and 27003. ISO/IEC 27002:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. A document like this would be able to suggest appropriate security controls that can successfully preserve the confidentiality, integrity and availability of business information and thus could serve to integrate information security into the daily activities and functions of an organization. Once the security measures have been implemented, business information risks, as well as the usefulness of the selected security controls, should be observed and reported to executive management [Corporate Governance Task Force, 2004]. These reports will further aid executive management in directing and controlling their organizations information security endeavours with greater precision. The objectives outlined provide general guidance on the commonly accepted goals of information security management. A quantitative approach to model and measure the action taken and also the net outcome of a security strategy is guided by the following standards like ISO/IEC 27004:2009. These provide guidance on the devel-

<table>
<thead>
<tr>
<th>Structure</th>
<th>Body</th>
<th>Uniqueness</th>
<th>Location</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity</td>
<td>None</td>
<td>Type</td>
<td>Instance</td>
<td>Hidden</td>
</tr>
<tr>
<td>Uniqueness</td>
<td>Contact</td>
<td>Contact</td>
<td>Full</td>
<td>Hidden</td>
</tr>
<tr>
<td>Location</td>
<td>Definitive</td>
<td>Static</td>
<td>Dynamic</td>
<td>Reactive</td>
</tr>
<tr>
<td>Key</td>
<td>Computational</td>
<td>Application</td>
<td>Duration</td>
<td>Reaction</td>
</tr>
</tbody>
</table>
opment and use of measures and measurement in order to assess the effectiveness of an implemented information security management system (ISMS) and controls or groups of controls, as specified in ISO/IEC 27001. The failure of such security techniques in terms of the risk in the business processes and the product is also addressed in ISO/IEC 27005. The management aspect of security and risk management are specified in a set of standards called ISO/IEC 27005:2008 that provides guidelines for information security risk management. The ISO/IEC 27010 will provide guidance for information security interworking and communications between industries in the same sectors, in different industry sectors and with governments, either in times of crisis and to protect critical infrastructure or for mutual recognition under normal business circumstances to meet legal, regulatory and contractual obligations.

5 Attacks And Threats In Business Processes

Many large businesses have been aware of and dealing directly with security issues for some time. Viruses, distributed denial of service attacks and the potential, both external and internal, for system and network compromise have been topics of concern for businesses with IT departments for several years. The importance and wide awareness of security have greatly increased since the terrorist attacks of September 11, 2001. There is a heightened level of security at airports, borders and elsewhere. However, the increased level of security awareness and concern at a broader societal level is only beginning to manifest itself in relation to the Internet. The main public concerns regarding the Internet remain centred around the privacy and security of personal information. There is insufficient awareness about the broad range of risks that systems and networks may be subject to, or about potential cyber attacks that can be generated from failure to properly secure computers. There is even less awareness of protective steps, both proactive and reactive, that can be taken to minimize these risks. The various attacks on business assets are as shown in Figure 2.
It describes about the possible internal and external attacks through which the internal attacker has grabbed all the privileges to access the authenticated records without proper permission. With this illegal permission the sensitive records may be destroyed whereas the external attacks may be due to viruses, Trojans or hacker which may not be granted permission to access those records. In some cases, the hacker may bypass the firewall and attack passively through which he/she not only views but also modifies the confidential records. The viruses may go through the firewall where the firewall cannot identify this type of hidden attacks and so it may be done actively. When using the methodology, one should not forget the following: security of an E-business system is not a state, but a process that has to be incorporated into the system from scratch, and not treated as an afterthought [Denis Trek, 2003]. There are a number of processes that are collaborating together to get the expected business output through successful transactions during a particular scenario. There may be other processes running parallel but without interacting with the remaining processes. In a business environment, there may be many processes like P1, P2 and so on which are safe guarded by security functions sg1, sg2 and so on as shown in Fig. 3.
Let the number of processes be $N_p$ and the collaborating processes are $N_c$ in any point of time of observation. The number of other processes will be $(N_p-N_c)$. Let the probability of accessing the structured information asset $s_i$ by a process $p_i$ may be represented as $p_i . \text{prob}(s_i)$. Similarly the probability of accessing the unstructured information $u_i$ by a process $p_i$ may be represented as $p_i . \text{prob}(u_i)$ and knowing that $\text{prob}(s_i) + \text{prob}(u_i) = 1$. Let the probability of an attack using any strategy on the asset which may be either structured or unstructured information be $\text{prob}(a_j)$ with number of safe guards for the structured type be $n_{sg}$ whereas for unstructured being equal to $n_{ug}$. The attacks can be quantitatively modeled based on the type of the attack and also on the duration with which they persist for example in the case of denial of service attacks. The severity of an attack is dependent on the number of security safeguarding mechanisms adopted and the storage pattern of the information assets. If the information is a structured one, then the attacker may know the location or the buffer in which it is stored using intrusion techniques. Otherwise if the information asset is an unstructured one, then the location or the indexing pattern may not be known to the attacker. Hence the attack severity index (ASI) may be evaluated as per Eqn. 1.
Attack Severity Index for attack \( k \) (ASI\(_k\)) =

\[
\text{probability of attack} \times \text{duration} \times \text{no. of vulnerabilities} \\
\times \text{type of attack} \\
\text{no. of safe guard} \times \text{weightage for indexing}
\]

The situation may be explained with the help of a process flow diagram shown in Fig 4. The business process first decides whether the customer request comes through the proper interface or is it a valid request. This is done through the first process called E-Compare. The input is verified with the security function to determine its validity. In the case of invalid input, the business security process will identify the incident as an attack through structured query injection or cross site scripting attack by html injection. These business security functional implications can be represented as follows:

E. Compare (input) → valid | invalid
Invalid input → attack.sql injection | attack.html Injection

Fig. 4 Attack to Risk Processes flow
Because of the attacks mentioned above, the risks due to security breach leads to loss of confidentiality (LOC) and loss of integrity (LOI) of the information assets needed for the business processes. The credentials of the business process or the system may be affected due to the loss of the above two attributes of information security in a business environment. The situation can be corrected by protecting the firewall itself which can be represented logically as,

- Exploit (Database) → Database revealed ⇒ LOC ∧ LOI
- Exploit (Server) → Credentials stolen ⇒ LOI
- E-Compare (firewall) → protected / unprotected

If the firewall is being unprotected, then the chances of active attacks due to viruses or Trojans are also high thereby disturbing the availability of the system resources or control elements leading to total application seizure. This may result a partial or erroneous execution due to the presence of bugs in the system key logs that can be formally specified as,

- Unprotected firewall → attack (virus) | attack (Trojan)
- Attack (virus) → Affect (System Resource) ∧ Control (System) ⇒ LOI ∧ LOA ∧ LOC
- Attack (Trojan) → Affect (application) ∧ Execute (Key log) ⇒ LOC

As per the process flow across a sample of business transactions, the time needed to complete the security actions and the associated costs are simulated as per the implications or rules mentioned above and tabulated in Table 2 and shown in Fig. 5 for a single server based processes.

Table 2 Work time and Cost for Security Actions

<table>
<thead>
<tr>
<th>Attack to Risk Flow</th>
<th>Work time</th>
<th>Cost</th>
<th>Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-Compare</td>
<td>15.90</td>
<td>37.01</td>
<td>Loss availability</td>
</tr>
<tr>
<td>E-Compare</td>
<td>11.83</td>
<td>26.82</td>
<td>Loss of confidentiality</td>
</tr>
<tr>
<td>E-Compare</td>
<td>24.85</td>
<td>37.91</td>
<td>Loss of integrity</td>
</tr>
</tbody>
</table>
It is found that a lot of work time is needed to maintain the confidentiality of the structured information when compared with the time needed to make that information available to the customers. But at the same time, the cost associated with the integrity assurance is more than that assuring the availability of the business information. It is found out that the integrity assurance is costlier than the confident assurance when a number of business processes are collaborating with each other assuming zero waiting time for all the processes. If the waiting time is included, then the scenario will be dependent on the individual waiting times for each and every business token collected over a specific period of working time. When multiple clients and servers were involved in the business processes, then the case results are based on the number of busy servers and aborted or terminated transactions which are tabulated in Table 3 and shown in Fig. 6.
Table 3 Multiple servers business Security Assurance

<table>
<thead>
<tr>
<th>Instance</th>
<th>Cycle time</th>
<th>Work time</th>
<th>Cost</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>21.5</td>
<td>29.42</td>
<td>81.05</td>
<td>Loss of availability</td>
</tr>
<tr>
<td>2</td>
<td>18.68</td>
<td>18.88</td>
<td>44.35</td>
<td>Loss of confidentiality</td>
</tr>
<tr>
<td>3</td>
<td>40.23</td>
<td>61.65</td>
<td>143.44</td>
<td>Loss of integrity</td>
</tr>
<tr>
<td>4</td>
<td>22.37</td>
<td>30.09</td>
<td>83.21</td>
<td>Loss of availability</td>
</tr>
<tr>
<td>5</td>
<td>24.13</td>
<td>24.13</td>
<td>62.05</td>
<td>Loss of integrity</td>
</tr>
<tr>
<td>6</td>
<td>30.35</td>
<td>30.35</td>
<td>91.3</td>
<td>Loss of integrity</td>
</tr>
<tr>
<td>7</td>
<td>23.21</td>
<td>23.21</td>
<td>61.37</td>
<td>Loss of integrity</td>
</tr>
<tr>
<td>8</td>
<td>22.34</td>
<td>27.63</td>
<td>66.71</td>
<td>Loss of confidentiality</td>
</tr>
<tr>
<td>9</td>
<td>22.55</td>
<td>41.95</td>
<td>92.45</td>
<td>Loss of availability</td>
</tr>
<tr>
<td>10</td>
<td>24.86</td>
<td>37.13</td>
<td>82.14</td>
<td>Loss of confidentiality</td>
</tr>
</tbody>
</table>

Fig. 6 Work time and Cost for multiple servers
6 Security Assurance And Business Continuity

Business Information Assurance is part of corporate governance in which the top level management provides accurate and correct information to the stakeholders about the efficiency and effectiveness of their security policy and operations. If any of the critical information assets is accessed frequently then the business index can be determined from the knowledge of the frequency of an access and the number of such collaborating processes which needs that information at that point of time. The number of security operations performed on the asset over a session is also a factor to determine the business continuity. Business continuity planning (BCP) is a very important issue and it has to be covered carefully [Devargas, 1999].

One aspect of incident handling and response should be business continuity. Business continuity implies the existence of work around mechanisms that allow a company to continue to operate in the event of a non-catastrophic failure. A decision to employ business continuity or full disaster recovery will depend on the nature of the business and its own business risk assessment. After a serious disaster many businesses recover with difficulty, e.g. in the case of a major fire in the UK, over 80% of businesses never recover, despite insurance arrangements, which effectively cover 30-50% of losses. Thus, continuity planning should be an integral part of security policy. BCP starts with threat identification, asset valuation and determination of likelihood of incidence. Afterwards, business impact analysis has to be done to identify critical business functions. This analysis should identify the effects of disaster and requirements for a recovery, including all resources. Afterwards, critical business functions need to be prioritised, depending on their impact. This impact forms the basis for financial justification of related investments for equipment, procedures and training to enable recovery in the necessary time frame. BCP requires inclusion of internal and external effects, which includes business interruptions of partners processes, loss of credibility and image. The proposed metric, called as Expected Business Continuity (EBC) may be considered as a factor that depends not only on the number of such assets in the business transaction during that session but also on the rel-
ative business importance of the information assets. The assets being secured with safeguards, the EBC factor can be expressed as the ratio of number of assets, their relative importance and the weight age factor of security in terms of safeguards to ASI of all types of attacks over a period [Devargas, 1999]. The security assurance for the information needed to continue the on-going business processes is a complex technique in which each and every stage, the underlying information system needs to ensure the confidentiality, integrity, availability and accountability of information. There are application program interfaces (API) shown as T1, C1, B1 and P1 through which the behavioral changes are reflected in to the nearby sub systems. For example, the APIs in the threat side of the Fig 7 say, T1 or T2 senses any possible threat and activated by the attack sub module and signaled to legislation and specification modules. Similarly the APIs in the content side say C1 or C2 sensed the variation in the information content will be communicated to the risk and policy sub modules to adapt to the incoming attack due to the existing vulnerabilities. The legislation and the business policies are interacting with the guidelines and the specifications of the business transaction requirements as shown in Fig 6

![Fig. 7 Business Continuity and Assurance](image)

The various services like asset assessment service, compliance services are to be checked as per Assessment and Compliance Services like NIST 800-30, 800-18 and 800-53 against all possible attacks on various assets involved in the business stages. That is the system should be certain to do something and make that thing cer-
tain to happen. It is integrated policy framework in which multiple components are interacting concurrently like a biological signaling pathway so as to minimize future losses to manage possible risk which may or may not take place. In the case of business information processing, the care should have been taken in reimbursing or protecting a process or an asset from a variety of contingent risk of losses through financial means. The assurance can be calculated based on the assessment of the compliance, correctness and certainty of the information handled by each and every process or component during a particular period of time. The various interactions and their translations discussed are represented as a pathway for information assurance as shown in Fig. 8

![Information Security Assurance pathway](image)

Fig. 8 Information Security Assurance pathway

By providing information security assurance, all the parameters for the process assessment and its compliance are carried to estimate the probabilities of potential risks and possible attacks based on the vulnerabilities. The legislations and policy along with the behavior of the persons involved are modified so as to secure the business content which is the valuable asset when multiple customer services are collaborating. The minimization business risk is done by securely storing and transmitting the business information at all times and the data and processes should be used only for that purpose exclusively in a virtual environment. After determining the significant probability of potential risks, the final relationship to estimate The business continuity can be estimated based on the number of assets involved in business transactions and the security guards for the processes needed for continuation The business continuity can be estimated based on the number of assets involved
in business transactions and the security guards for the processes needed for continuation. If an attack on the asset happens, then based on the index of information being structured, the resulting risk factor can be represented in first order logic as given by the equation where $BI$ represents the business information whether structure or unstructured and $sg$ represents the number of security guards or functions for the processes involved. The business will be extended and continued (EBC) if the process $Pi$ is governed as long as the security function $Sg$ for that particular succeeds is represented by the second line below.

$$BI(asset)_i * sg(asset)_i$$

$$Pi.BI(asset)_i = sg(asset)_i \quad > \quad EBC$$

The final empirical relationship for the total amount of risks including process, product and business risks can be estimated by the above procedure by considering the attack severity index and index factor of the structured information of the business assets when number of security functions are activated and summed up as given by the Eqns. (2) and (3) shown below;

$$Index = \text{location complexity} * \text{size of information}$$

$$Factor_k = \text{Level of asset}_k * asset_k$$

$$Risk = \frac{\sum_{i=1}^{n} BI(asset)_i * sg(asset)_i}{\sum_{k=1}^{f} IndexFactor * \sum_{j=1}^{m} ASI(attack)_j}$$

The total number of assets is being $n$ and the index factors for the number of structuredness is being $f$ against the number of attacks is being $m$.

### 7 Conclusions

The information security assurance model is important in the case of business services deployed in the grid or in a cloud environment. The security model is based on the design heuristics that relates the structure of the information assets that are represented as a tuple with uniqueness, identity, location and size of the information. The empirical relationship model provides secured transparency against
the risks due to security breach which leads to loss of confidentiality (LOC) and loss of integrity (LOI) of the information assets needed for the business processes. The continuity in business is achieved continued and the resulting risks are predicted with minimized loss in the presence of explicit or implicit attacks. The information security assurance pathway is brought out to quantitatively model and estimate the total risks covered when a number of services are interacting if the attack and asset may become noncompliant entities.

References


