6. Chapter 6

6.1 Synthesis of learning, conclusion and suggestion for further research

6.1.1 Introduction

This section is a synthesis of the previous three sections to arrive at the overall conclusions, findings, recommendations, implications, contributions, limitations and suggestions for future research.

This interdisciplinary study has highlighted that data has played an extremely important role through civilizations and digital data or information is expected to play an increasingly crucial role in the future of humanity. Forbes has reported the IBM CEO’s prediction that, “data will be the basis of competitive advantage going forward, calling it the “the next natural resource”” [Online articles 340 – IBM 2013]. Today the modern and globalized business and society has grown to be dependent on the global nature of cyberspace due to the dynamic and novel use of ICT. The successful innovative exploitation of cyberspace and mature use of ICT by technologically advanced Nations is helping them and their society to prosper in the digital economy also known as the knowledge economy. Nations policy makers are beginning to realize that by embracing digitization while addressing security and privacy concerns of citizens and businesses, allows for increased access, sharing and integration of information using hyperconnectivity thereby encouraging citizens and businesses towards improving economic, political and social participation which in turn accelerates the Nation’s economic growth and global integration to achieve planetary civilization where the socioeconomic path and ICT are deeply linked [World Economic Forum and INSEAD 2012; Clift and Mandeville 2012]. The remarkable increase and dependency on ICT by businesses to achieve efficiency, collaboration, improved effectiveness and competitiveness has also led to an increasing demand for software services. A new wave of globalization not previously witnessed has international trade, investments and technology connected inseparably within global supply chains [Milberg and Schöller 2008]. Trust is at the core of social order and economic prosperity as it is the basis for
economic transactions and inter-human communication [Tonkiss 2009; Reina and Reina 2007; RISEPTIS 2009].

Outsourcing customers need trust and assurance with respect to security of their information in terms of confidentiality, integrity and availability of the data from the outsourcing and offshoring service provider for continuation of outsourcing and offshoring. The outsourcing and offshoring service providers need to continue their economic growth and thereby the Nation’s economic growth by showing improved organizational performance while addressing to the satisfaction of the outsourcing customers their concerns regarding perceived risks around information security to their critical asset – data or information, so as to continue on the journey of integrating the socioeconomic path and ICT for the Type 1 civilization. India has been able to effectively trade globally, information-intensive services by breaking it down into its constituent parts and trading them in the same way as possible with goods [UNCTAD 2004], by providing a skilled workforce at lower wages.

As seen from the previous sections, in an outsourcing offshoring arrangement, the customer trusts the service provider with their data or information with respect to its confidentiality, integrity and availability. The customer expects the service provider to ensure and provide good governance of the data at its end. Using good governance practices the service provider is expected to provide superior service quality to the customer. Providing superior service quality results in improved performance for the service provider organization. Offshore outsourcing success is dependent on relationship and partnership elements such as trust [Grover et al. 1996] which is a dynamic phenomenon, [Lewicki and Bunker 1996] and a process that can be created, developed, maintained or destroyed thus making it complex and subtle [Khodyakov 2007] which can be continuously improved upon to achieve higher levels of trust competence or maturity.

This trust competence or maturity in turn increases the interdependency of the customer on the service provider thus ensuring continued offshoring and outsourcing. Thus security of customer data by the offshore outsourced service provider creates value and economic gains.
6.1.2 Summary of the research and synthesis

The overall interdisciplinary study can be viewed as a three step process as described in the section “Outline of the research” as part of Section 1, for answering the research question.

The first step primarily helps in identifying the information security practices followed by the Indian software services industry by utilizing the business model for information security and the service quality gap model, while pinpointing areas of weakness in the select dimensions of service design and service performance of the service quality gap model.

The second step uses survey methodology to gather the data to explore governance, service quality and performance from the Indian software service providers perspective. It provides an empirical analysis using Partial Least Square (PLS), a Structural Equation Modelling (SEM) technique which has been used for modeling to validate the relationship between information security governance as part of corporate governance and information security service quality and that between information security service quality and organization performance.

The third step utilizes the survey instrument and data gathered in the previous step for mapping the individual security governance and security service quality items to individual trust items and to the key trust dimensions. This step triangulates the above two steps in a qualitative and quantitative manner.

A) The summary of the findings and discussion of the first step is as follows:

1) Based on the secondary data and field work, the equilibrium of the business model for information security comprising of the four elements and six dynamic interconnections was studied and found to be out of balance. It is observed from the secondary data that the Indian
software service providers are securing the customer data by focusing on people, technology, governing and enabling and support. There are challenges on the human factors, architecture and culture areas. From the field work it is seen that human factors, emergence and culture are areas that need focus. Hence the main areas for focus for the Indian software service providers are architecture, emergence, human factors and culture. Each of these is discussed here:

(a) Architecture: There seems to be no synchronization between the overall corporate security strategy and overall security architecture. This architecture is primarily all the connections that comprise of the organizations infrastructure such as hardware, software, people, information security process and information security policies. This means that the business goals and objectives cannot be shown linked to the security architecture or in other terms the senior management is not aware of how robust and resilient security architecture can or cannot contribute to the overall business goals and objectives. Understanding of this is critical because it is at the architecture level that one can describe how the different security controls are placed and their relation to the overall business and IT architecture which is aligned to the business goals of the enterprise. This shows a lack of understanding, appreciation and importance with respect to information security at the governance layer in the organization and hence the senior management is unable to completely adhere to and control, direct, regulate or shape the information security strategy within the organization for protection of data or information belonging to the customer. This could lead to impacting the confidentiality or integrity or availability of customer data thus leading to a loss of customer trust.

(b) Emergence: The organization infrastructure and the organization itself is a complex amalgamation of various components such as people, processes, technology, policies, customers, threats, regulatory environment and government policies. These components interact in a dynamic manner with each other within the organization resulting in cause and effect situations. These situations can create patterns over a period of time which could develop into risks for the organization and need to be managed. For example, the threats to data or information (including customer information to which the service provider has access or which resides in the service providers ICT systems) keep evolving and it is necessary for service providers to manage this evolving risk by understanding
the business impact of the threat, likelihood of the threat and efforts involved or the cost to mitigate the threats on an ongoing basis. This requires a good understanding of the information security threat scenario with respect to the customers business domain so as to judiciously distribute limited resources across the four elements and six dynamic interconnections. This too shows a lack of understanding and appreciation with respect to the depth that one needs to go to with respect to information security at the governance layer in the organization and hence the senior management is unable to prudently decide if the business impact of the threats and costs involved in their mitigation is worth focusing on and if it would cause any loss of trust between the service provider and the customer. If the emergences of such threats are not mitigated in time it could create a crisis situation leading to security breaches and thereby a loss of customer trust.

(c) Human Factors: In the service provider organization providing offshore outsourced software services it is people and technology that play a vital role. People can be productive and contribute to operational efficiencies and hereby organization performance if they use the technology in a safe and secure manner, else there could be disruptions and downtime adversely impacting productivity, efficiency and performance. The culture of the people, the culture of the organization and emergence as discussed above impact the people. Architecture discussed above impacts the technology. Since emergence and architecture have a lack of understanding at the governance layer in the organization, the senior management is unable to control, direct or shape the human resource policies in a manner that addresses the complexity of information security aspects in a digital environment which in turn can contribute towards trust within the organization and there by between the service provider and the customer.

(d) Culture: This is the expected behavior of people in an organization based on the experiences and responses that an organization may have gone through over a period of time. This is the very fabric of the organization and is driven from the top person in the organization within the organization. The findings indicate that security is not a part of the service providers culture and hence not deeply ingrained as part of the organization design and strategy making it a corporate governance issue.
These issues or gaps in architecture, emergence, human factors and culture at the Indian service providers end are contributing to service design gaps and service performance gaps.

2) The Business model for information security helps in highlighting that there are service design gaps and service performance gaps as part of the Service Quality Gaps Model thus creating a gap between expected service and perceived service or the customer gap.

3) Though the equilibrium of the Business model for information security is disturbed as per the findings, it is seen that there has not been any change in the overall Indian software exports percentage and the overall software export figures have continued to grow. This probably implies that the customers perceive their data or information is safe at the service provider’s end. This helps towards trust building between the customer and service provider.

4) Since the service design and service delivery in the Service Quality Gaps Model is primarily customer driven and as has been concluded in this step of the study that the equilibrium of the Business model for information security is disturbed, it can be inferred that the equilibrium of the Business model for information security at the customer end is also probably disturbed.

5) A disturbed equilibrium of the Business model for information security will not impact software exports growth adversely since it seems to qualify as an acceptable information security service quality as long as the customer gap remains within tolerance limits, as defined and perceived by the customer.

6) To improve the overall information security practices in a supply chain, the acceptable service quality as defined and perceived by the customer needs to be raised to a higher level both within their own organization and at the service provider end. The service providers in the supply chain should explore the process of self-attestation for the state of equilibrium of the Business model.
for information security at their end thereby helping create transparency with the customers and thereby enhancing trust.

7) It seems that the service providers have been able to govern the customer data adequately to provide acceptable service quality to customers and in turn continue to improve their organization and industry performance.

This leads one to explore the relationship between governance, service quality and performance further as the next step. The reason to explore this further is that though there are evident governance gaps, the service quality and organization performance seem acceptable but had there been a focus on governance to reduce the gaps or their elimination then can one predict superior service quality and improved organization performance thus contributing to enhanced trust? This is covered in the second and third step as discussed next.

B) The summary of the findings and discussion of the second step where the relationship between governance, service quality and performance is explored as follows:

1) Using the survey methodology approach to gather data for exploring the relationship between governance, service quality and performance from the Indian software service providers has been carried out in this step. Empirical analysis has been carried out using Partial Least Square (PLS), a Structural Equation Modelling (SEM) technique which has been used for modeling to validate the relationship between information security governance as part of corporate governance and information security service quality and that between information security service quality and organization performance.

In summary the empirical data validates the research model confirming that:

a) the reliability of each question modified for information security and asked in the survey instrument is acceptable and highly significant,
b) there is a positive relationship collectively between elements of Security Governance, Security Service Quality and Organization Performance, and

c) security governance as part of corporate governance has a highly significant impact on security service quality and can be predicted and quality of security services in turn has a highly significant impact on the overall corporate performance and can also be predicted.

Thus this step provides validation of the relationship between information security governance as part of corporate governance and information security service quality and that between information security service quality and organization performance.

2) This step also shows that existing dimensions and instruments for Corporate Governance, Service Quality and Organization Performance, available in literature, can be used by appropriate modification to reflect the context of information security.

3) This step demonstrates that information security governance as part of corporate governance drives information security service which in turn drives organization performance. For the Actual case, it indicates that a 100 points change in Governance will bring 59.0352 points change in Quality. Similarly a 100 points change in Quality will bring 55.9613 points change in Performance. The values are positive and are at a significance level of 1 percent which is highly significant. The effect size is large for both performance and quality implying that the estimated magnitude of information security governance on information security service quality is large and the magnitude of information security service quality on organization performance is also large in the Actual case.

For the ratio case it indicates that a 100 points change in Governance will bring 40.1858 points change in Quality. Similarly a 100 points change in Quality will bring 31.3618 points change in Performance. The values are positive and are at a significance level of 1 percent which is highly significant. The effect size is small and medium for performance and quality respectively implying that the estimated magnitude of information security governance on information security service quality is large.
security service quality is medium and the magnitude of information security service quality on organization performance is small in the Ratio case.

4) The model has predictive relevance and the values for predictive relevance fall in the medium effect category for quality and performance in the Actual case and in the small effect category for quality and performance in the Ratio case.

5) Thus it is clear that if the Indian software service providers focus on information security governance to reduce or eliminate the issues or gaps such as architecture, emergence, human factors and culture, then they can deliver superior information security service quality which can be predicted and they can thereby achieve improved organization performance which can also be predicted. The issues identified in the previous step namely architecture, emergence, human factors and culture correspond to strategic planning, information and analysis, human resource focus and leadership dimensions of information security governance.

6) As the empirical results show that Governance of security services in an outsourcing company providing software services has a highly significant impact on the quality of security services and can be predicted, and the quality of security services in turn has a highly significant impact on the overall corporate performance and can also be predicted, thus it can be assumed that probably the performance (both monetary and value dimensions) of the service providers can improve in a significant manner from the current values if they focus on the governance and service quality aspects of security services.

The question that remains to be explored is that does this relationship between governance, service quality and performance contribute towards enhancing trust? This is discussed as part of the third step, next.
C) The summary of the findings and discussion of the third step where trust is explored is as follows:

1) This step uses the survey instrument, used in the previous step for security governance and security service quality, as its basis for data analysis. As seen in the previous step the following are already established – the reliability and validity of each item; the positive relationship collectively between elements of Security Governance, Security Service Quality and Organization Performance; and the predictiveness. This step goes on to show that the individual items / questions administered in the survey instrument, in the previous step, for information security governance and information security service quality to the respondents, with the help of existing literature, can be mapped to a primary trust perception item, which in turn can then be mapped to one of the key trust dimensions.

2) This step demonstrates that existing dimensions and instruments for Governance, Service Quality and Organisation Performance, available in literature, can be used by appropriate modification to not only reflect the context of information security but also that of trust.

3) This step illustrates how categorization of organizations on the basis of trust level maturity on the lines of capability maturity model can be carried out.

4) Further, this step proposes five different levels of trust maturity, six key process areas (competence, culture, communication, people, process and technology) and some key practices which can be implemented by organizations and continuously improved upon to achieve higher levels of trust competence or maturity.

5) This step delivers an integrated trust maturity framework where trust as understood in the industrial economy and as required in the digital or knowledge economy is converged and the
processes are repeatable, adaptive and intelligent so as to address the complexities of security and trust.

6) Using qualitative and quantitative methods it is concluded that the governance of security services can predict the quality of security service which is the essential determinant of client satisfaction and client satisfaction is the basis of continued trust in a service organization. Trust leads to corporate sustainability and growth and can be depicted in the form of a maturity framework.

6.1.3 Key learnings from the study

There are key takeaways from each of the three steps of this study. The key learnings from each of the steps in this interdisciplinary study can be summarized as follows:

1) The Business model for information security helps in identifying, including visually, areas of weakness or gaps present in service design and service performance as part of the Service Quality Gaps Model thus contributing to the gap between expected service and perceived service or the customer gap. The weaknesses, evident as governance gaps, in the business model for information security have an impact on the equilibrium of the model. Though the equilibrium of the Business model for information security is disturbed as per the findings, it is seen that the overall software export figures for the Indian software services industry have continued to grow. This probably implies that the customers perceive their data or information is safe at the service provider’s end and they do not perceive any governance gaps. Since the service design and service delivery in the Service Quality Gaps Model is primarily customer driven it can be inferred that the equilibrium of the Business model for information security at the customer end is also probably disturbed. Hence a disturbed equilibrium of the Business model for information security at the Indian software service providers end will not impact software exports growth adversely since it seems to qualify as an acceptable information security service quality as long
as the customer gap remains within tolerance limits, which are as defined and perceived by the customer.

2) The empirical results show that Governance of security services in an outsourcing company providing software services has a highly significant impact on the quality of security services and can be predicted, and the quality of security services in turn has a highly significant impact on the overall corporate performance and can also be predicted.

3) It is seen that information security governance and information security service quality dimensions can be mapped to trust dimensions which in turn using qualitative and quantitative methods helps in arriving at an integrated trust maturity framework where trust as understood in the industrial economy and as required in the digital or knowledge economy is converged and the processes are repeatable, adaptive and intelligent so as to address the complexities of security and trust. Quality of security service is an essential determinant of client satisfaction and client satisfaction is the basis of continued trust in a service organization. Trust leads to corporate sustainability and growth.

4) From an overall perspective of the study one can conclude that the different dimensions of security governance, security service quality and organization performance can be studied, understood and measured subjectively and objectively in terms of soft and hard data. Trust is the “soft” catalyst for “hard” wealth creation in inter-organizational asymmetric partnership for service organizations in the digital or knowledge based economy as a step towards better globalization.

5) Thus this overall study possibly makes a convincing case for information security is free, implying that the returns on security investment are far greater than the cost that is incurred for information security by the Indian software service providers.
6.1.4 Revisiting the research question and research objectives

It is prudent to revisit the research question and research objectives to understand if these have been addressed in the study.

The problem statement or research question was: “Can governance of security services in an outsourcing company providing software services predict the quality of security services, and can quality of security services in turn predict overall corporate performance?”

The short answer to the research question is yes. As can be seen in Section 4 of this study, empirical analysis has been carried out using Partial Least Square (PLS), a Structural Equation Modelling (SEM) technique which has been used for modeling to validate the relationship between information security governance as part of corporate governance and information security service quality and that between information security service quality and organization performance. The empirical results show that Governance of security services in an outsourcing company providing software services has a highly significant impact on the quality of security services and can be predicted, and the quality of security services in turn has a highly significant impact on the overall corporate performance and can also be predicted.

The following objectives relating to the research question were to be studied from the Indian software services perspective:

1. To examine information security practices followed in the Indian software services industry using a holistic, scalable, theory based, business oriented model for information security

Based on the literature survey in Section 2, the business model for information security was identified which was grounded in theory on the academic side as well as practical for usage by industry. Based on this the model was used in Section 3 of this study to arrive at an understanding of the information security practices followed in the Indian software services industry. This is also covered in a paper that was published [Bahl et al. 2011].
2. To examine select dimensions of service quality to understand if it leads to any perceived service quality gap in the security services from the Indian software services providers’ perspective within the Indian software companies?

The service quality gaps model as covered in the literature review in Section 2 was used in Section 3 along with the business model for information security in the select dimensions of service design and service performance. This helped in identifying, including visually, areas of weakness or gaps relating to architecture, emergence, human factors and culture which primarily stem from governance weaknesses. This weakness disturbs the equilibrium of the Business model for information security leading to service design gaps and service performance gaps as part of the Service Quality Gaps Model thus contributing towards a gap between expected service and perceived service or the customer gap. This is also covered in a paper that was published [Bahl et al. 2011].

3. To identify how governance dimensions relate to security service quality dimensions within the Indian software companies?

The Section 4 of the study carries out an empirical analysis to show that Governance of security services in an outsourcing company providing software services has a highly significant impact on the quality of security services and can be predicted. This is also covered in a paper that has been accepted for publishing [Bahl and Wali coming 2014].

4. To identify how perceived quality of security services relates to perceived overall organizational performance?

The Section 4 of the study carries out an empirical analysis to show that the quality of security services in an outsourcing company providing software services has an impact on the overall corporate performance and can be predicted. This is also covered in a paper that was published [Bahl and Wali 2013].
5. To draw conclusions for proposing trust governance framework that could help in sustained trust.

As seen in Section 5 that with the help of existing literature in Section 2, items administered in the survey instrument for information security governance and information security service quality to the respondents in the study in Section 4, can be mapped to a primary trust perception item, which in turn can then be mapped to one of the key trust dimensions. This study also helps towards understanding of the trust management processes as part of governance with intermediate outcomes in service quality so as to arrive at better understanding of performance. Trust leads to corporate sustainability and growth and can be depicted in the form of a proposed maturity competency framework. Thus organization can be categorized on the basis of trust level maturity. This study proposes five different levels of trust maturity, six key process areas (competence, culture, communication, people, process and technology) and some key practices which can be implemented by organizations and continuously improved upon to achieve higher levels of trust competence or maturity and thereby sustained trust.

6.1.5 Major insights gained from the study

The adoption and innovation of natural resources facilitated the evolution of the industrial revolution and now it is data which is fuelling the current information revolution towards the future planetary civilization progression. Increasingly data or information is handled, processed, transported or stored in digital systems thus making it a pervasive critical asset for human civilization and its survival. Hence this critical asset, which is data or information, needs to be safeguarded and protected.

In an outsourcing offshoring asymmetric relationship the customer trusts the service provider with their data or information with respect to its reliability in terms of confidentiality, integrity and availability. This study has attempted to deliver an integrated trust maturity framework where trust as understood in the industrial economy and as required in the digital or knowledge economy is converged. In the digital or knowledge economy where asymmetric partnerships are
established (such as between the offshore outsourcing service provider and customer), trust is about the reliability of data and can help establish long-term strategic partners.

This interdisciplinary study shows that different dimensions of security governance, security service quality and organization performance can be studied, understood and measured subjectively and objectively in terms of soft and hard data. Trust is the “soft” catalyst for “hard” wealth creation in inter-organizational asymmetric partnership for service organizations in the digital or knowledge based economy as a step towards better globalization.

6.1.6 Recommendations from the study

To create sustained trust organizations need to make information security governance an integral part of corporate governance. This will help reduce the service gap between customer perception and expectation which can be achieved by managing and developing behavior trust and sociological and psychological trust which in turn helps build up economic trust.

Trust in terms of data reliability helps offshore outsourcing service providers improve their economic health by providing scalable, predictable and effective information security services to their customers, improve their return on information security investment and achieve operational excellence.

This overall interdisciplinary study possibly makes a convincing case for information security is free, implying that the returns on security investment are far greater than the cost that is incurred for information security by the Indian software service providers.

6.1.7 Implications of the study

The implications of this study can be categorized into two parts namely for practice and for research respectively. Both these are discussed here – first for practice and then for research.
The study provides exploratory evidence that the senior management of the Indian software service organizations have not understood the importance, complexity and depth of information security in the organization and hence have a challenge to provide assurance to stakeholders that the security is aligned to business, is an integral part of the business and not bolted upon. The challenge for the senior management arises as there have not been many service provider side empirical evidence or specific ways to measure defined benefits of information security or how it could add value to the enterprise and the customer.

This study provides empirical evidence that governance of security services in an outsourcing company providing software services has a highly significant impact on the quality of security services and can be predicted, and the quality of security services in turn has a highly significant impact on the overall corporate performance and can also be predicted. The study shows in a qualitative and quantitative manner that a multi-dimensional, complex and subtle subject as trust is the “soft” catalyst for “hard” wealth creation in inter-organizational asymmetric partnership for service organizations in the digital or knowledge based economy.

If the goal of the offshore outsourcing service provider organization is to achieve a competitive edge, provide client satisfaction and create sustained trust then as a strategy they need to make information security governance an integral part of corporate governance and adopt the trust maturity framework as proposed in this study. This will help them manage information security risks by:

1) understanding customer expectations and keeping their commitment to meet the customer expectation thereby promoting and creating goodwill trust and sociological and psychological trust,

2) providing reliable service quality meeting the expectations of their customers thereby amplifying and maintaining competence trust and economic trust, and
3) reducing the service gap between customer perception and expectation thereby managing and developing behavior trust and sociological and psychological trust which in turn helps cement economic trust.

Indian software service providers should focus on, amplify and commit to information security governance and information security service quality at strategic, tactical, and operational levels by following the proposed trust maturity framework to achieve revenue expansion, completely satisfied customers and create sustained trust. This will not only help them create value for the customer and economic gains for themselves but also provide growth opportunities, boost internal efficiencies or operational excellence, deliver cost effective service delivery, help form strategic partnerships by being a preferred partner for customers in their quest for a superior supply chain and provides an opportunity for the country to be further elevated as a visionary and thereby take a strategic leadership role.

Trust in the digital or knowledge economy is an extremely complex phenomenon, it is multi-dimensional, dynamic in nature and plays a critical role in the success of information systems outsourcing. There is a need to maintain a fine balance between trust and security controls for the protection of information and information assets to mitigate the security risks while achieving collaboration, innovation, continuous improvement and learning. It is for this reason that Currall and Epstein [2003] mention that “successful companies build, treasure, preserve, and nurture trust”.

In the digital or knowledge economy where asymmetric partnerships are established (such as between the offshore outsourcing service provider and customer), trust is about the reliability of data or information in terms of its confidentiality, integrity and availability. The proposed trust framework provides repeatable, adaptive and intelligent processes to address the complexities of trust in a digital or knowledge economy.

As the returns on security investment are far greater than the cost that is incurred for information security, these measures in turn will help the service providers in addressing the impacts which were identified in Section 1:
(a) mitigating objections to outsourcing as a high security risk;

(b) inculcate acceptable security and privacy business practices;

(c) create trust by improving service quality and thereby customer relationship;

(d) improve the performance of organizations and thereby of the Indian IT Industry;

(e) help towards improving FDI;

(f) help in creating a trusted destination reputation for the country and contribute towards GDP growth.

From a research perspective this study concurs with Busi and McIvor [2008] that it is crucial to develop a theory based approach which can be practically implemented even if it is a combination of the existing theories. Various existing theories have been combined and used in this study with appropriate modifications to reflect information security aspects and then linking them to trust after testing for their reliability and validity, for arriving at a practical trust competence framework which is implementable and useful for practice.

6.1.8 Major research contributions

There have been very few rigorous studies linking information security governance with other business critical objectives (such as total quality management, quality of service and performance), so this research is possibly a useful contribution to this area in literature.

By trying to bridge identified gaps in literature as in section 2, this interdisciplinary study contributes back by:
• being in the service industry area
• investigating outsourcing issues from the vendor's perspective impacting inter-organizational relationship
• addressing the issue of information security management, risk management and trust management
• leveraging prior disjointed research in the areas of information security, trust, governance, service quality and performance and bringing them together
• making use of empirical work in terms of Partial Least Square modeling and using prior established research methods of measurement for governance, service quality and performance namely measures of construct for survey methodology based on Likert scale by modifying them and constructing some measures to reflect the context of information security and trust by ensuring the construct validity, testing of individual items and structural model testing
• linking information security and trust management processes as part of governance with intermediate outcomes in service quality to arrive at better understanding of performance
• arriving at implications for business leaders and managers based on empirical outcomes; providing a coherent linkage between theoretical approach, the framework conceptualization and practical implementation by utilizing a combination of existing theories.

Finally this study provides a trust maturity framework which can be used by organizations to continuously improve and go higher in the trust maturity levels. This study has attempted to provide an integrated trust maturity framework where trust as understood in the industrial economy and as required the digital or knowledge economy is converged. In the digital or knowledge economy where asymmetric partnerships are established (such as between the offshore outsourcing service provider and customer), trust is about the reliability of data or information in terms of its confidentiality, integrity and availability. The proposed trust framework provides repeatable, adaptive and intelligent processes to address the complexities of trust in a digital or knowledge economy. The proposed trust maturity framework hopefully is a small contribution towards the future planetary civilization progression.
6.1.9 Limitations of the study

This interdisciplinary study has provided some interesting insights, recommendations and implications while contributing to the body of knowledge but it also has some limitations. The limitations have been brought out in each of the steps of the study in their respective sections. The synthesis of the limitations of this study is discussed here.

The limitation of this study is that it has looked at the Indian software outsourcing service providers in the Tier 1 level (companies having over 50,000 employees or associates and a revenue of over USD 1 billion) providing services to customers.

The study has identified key processes and practices for the trust framework. However the proposed trust competence framework has not been validated by means of its implementation in the field to receive feedback for refinement, if any.

Addressing these limitations would help validate and generalize the proposed trust competence framework so that it can be applied across any of the service organizations.

6.1.10 Suggestions for future research

This study while addressing various gaps in extant literature throws up a range of areas for future research thereby implying that this area needs more exhaustive study. Some of the areas of focus for future work are to:

- develop a comprehensive measurement method for the business model for information security covering the elements and dynamic interconnections
- arrive at a comparison between the business models for information security at the vendor and customer side to study the degree of alliance and divergence that may emerge so as to shed light on the governance and service delivery of the service provider and in turn on the performance of the service provider organization
• collect and analyze larger survey data from across countries and also cover survey data from other service industries from multiple countries since the survey data in this study covered software service industry from India, to explore the pervasive applicability of this framework across service industries

• collect and analyze survey data from customers of the service providers to establish if the perceptions of the employees of outsourced service companies translate into service improvements and external trust as perceived by the customer

• compare customer perceptions of outsourcers in which information security governance is internally perceived as strong (and contributing to total service quality) and those where it is perceived as weaker

• compare perceptions of outsourcers in which information security service quality is internally perceived as strong (and contributing to organization performance) and those where it is perceived as weaker

• arrive at a comprehensive list of key practices for the identified key processes along with their detailed activities, measurement, analysis and verification of implementation for the trust capability maturity framework

• validate the trust capability maturity framework by practical implementation in a service organization to further fine tune it and generalize it.

Given the growing importance, distillation and explosion of the volume, variety and velocity of data or information in the digital or knowledge economy and as we move towards the future planetary civilization progression, future researchers are urged to build upon the gaps in this work so as to enrich the literature and understanding in this field.