On inter-organizational trust engineering in networked collaborations : modeling and management of rational trust

Msanjila, S.S.

Publication date
2009

Chapter 2

Aspects and characterization of trust

Traditionally, the concept of trust has been addressed at the individuals' level. It is also mostly assumed to be a phenomenon that naturally emerges rather than being created. At individuals' level, most research and practice have considered trust as a subjective aspect. However, today the concept of trust has become an amenable factor for smoothening inter-organizational collaboration and thus has raised the need to address trust from a new angle. Traditional approaches and mechanisms for both assessing the level of trust in individuals and applying such results for creation of trust are inadequate for analyzing inter-organizational trust. While comparing with inter-personal trust this chapter surveys existing work on inter-organizational trust addressing the complementary and contradictory concepts, as well as different practices in various disciplines. The chapter then presents a characterization of trust and trust relationships as addressed in VBEs and identifies three main challenges related to trust studies.

This chapter has been published, for the most part, as a book chapter in: Methods and Tools for Collaborative Networked Organizations [Msanjila & Afsarmanesh 2008b].

2.1 Introduction

Trust has been widely studied, most importantly as a component of relationships among individuals and organizations. In Section 2.2, we present a survey of existing and reported research work on trust among such individuals and organizations. The survey first discusses differences between aspects of inter-personal and inter-organizational trust and subsequently discusses in detail the concepts related to trust among individuals. In Section 2.3, we introduce the characterization of inter-organizational trust in VBEs. In that section, we present concepts which either complement (such as security, reputation, etc.) or contradict (e.g. risks, privacy, etc.) aspects of inter-organizational trust. In that section, we also introduce fundamental aspects of organizational trustworthiness, namely those of a technological, structural, economical, social, and managerial nature. In Section 2.4, we present fundamental aspects necessary to guide organizations for deciding on the type of trust-related data, which are needed in the VBE and shall be sufficient to enable them trust other organizations. In that section, we also address different kinds of evidence of validity for trust related data of organizations. In Section 2.5, we briefly introduce fundamental steps proposed to guide establishmet of inter-organizational trust relationships in VBEs.

2.2 Traditional practices on trust

As a subject, trust has gained increased attention and has been examined in both research and practice. The challenges related to inter-personal trust date far back and correspond with the beginnings of human life. This section first examines the differences between inter-personal and inter-organizational trust, and then focuses on inter-personal trust.

2.2.1 Inter-personal versus inter-organizational trust

Many researchers have indicated that trust is an important issue in smoothening inter-personal and inter-organizational relationships. However, research work conducted to address inter-organizational trust has focused on theoretical evaluations [Currall & Judge, 1995]. Nevertheless, in the current information society some studies have addressed trust from a practical standpoint and have produced fundamental empirical evidence on the creation of trust among actors [Smith & Barclay, 1997]. Even so, until today there is still no actual agreement on the exact nature and definition of the trust with respect to its conceptualization, perception, preference and measurement (Section 1.3). To address trust in research satisfactorily, understand the effects of trust in different types of partnerships, and enable acceptable results for all stakeholders, it requires the involvement of communities and other institutions from heterogeneous domains [Smith & Barclay, 1997].

A fundamental difference between inter-personal trust and inter-organizational trust relate to their antecedents [Msanjila & Afsarmanesh, 2007d]. Inter-personal trust is defined at the level of the individual and it represents the extent to which a person places trust in another person. It has been observed that although inter-organizational trust and inter-personal trust differ in a number of aspects, they share the aspects of time in relation to the ***temporary and dynamic nature of trust*** [Ratnasingam, 2003]. For example, ***time*** can influence the decision on the trust related data, considering aspects such as validity, sources and mechanisms applied for its collection, which are needed to create trust among actors. Thus, time is a key aspect to consider when analyzing and modeling trust relationships among organizations as addressed in Section 4.3.1. Table 2.1 presents a summary of comparisons of complexity of trust among individuals and organizations.

Table 2.1: Complexities of trust among individuals and among organizations.

Trust among individuals	**Trust among organizations in VBEs**
The creation of trust is traditional and proven	The creation of trust is emerging and unproven
Mechanisms for assessing the level of trust are known and informal	There is lack of mechanisms for assessing the level of trust and formal ones are needed
The assessment applies opinions of others	The assessment is based on rational data
The trust related data and their sources are known and are proven	The trust related data and their sources are difficult to define and need verification
Does not necessarily need tools for supporting related processes	Needs tools due to the urgency for processing a large amount of data
Trust criteria are mostly known and static	Trust criteria are not known and are dynamic
Less interferences in establishing trust relationship	Other stakeholders must be involved while establishing trust relationships

A basic or essential level of trust is required for smoothening inter-organizational cooperation. An established climate of trust that is internalized in organizational behavior and

supported by mutual belief is necessary for collaborative efforts between partner organizations [Cosimano, 2004]. Optimal gains from a network can be achieved through collaboration that is facilitated by inter-organizational trust, such as reduced costs, greater achievement speed, and an improved ability to handle complexity of different activities. Furthermore, trust influences an organization's long-term strategic plans, collaborative market performance and loyalty. Trust also broadly influences organizational relationships, commitment, cooperation, functional conflict, uncertainty, the propensity to leave, and acquiescence [Msanjila & Afsarmanesh, 2008a].

The difficulty in the conceptualization of trust among organizations is extending a phenomenon that is inherently at an individual level, to an organizational level. These difficulties can produce confusion in relation to the creation of inter-organizational trust.

2.2.2 Trust among individuals

The theory on origins of inter-personal trust [Cosimano, 2004; Lahno, 2001] has mainly proceeded along three main fronts: (1) explaining differences among the individual propensity to trust, (2) understanding diverse dimensions of trustworthy behavior, and (3) suggesting different levels of trust development.

- *Individual propensity to trust:* Trust among individuals is regarded as a generalized expectancy that assumes people may be relied on. This expectancy is a function of the degree to which trust has been honored by that individual's history of past social interactions. Recent work has suggested that both the characteristics of the trustees involved in trust relationships and their level of trust vary with time [Msanjila & Afsarmanesh, 2008a]. As further addressed in Section 5.4, the computed trust level of an organization is a relative value depending on the applied set of trust criteria, other involved organizations, and interpretation of trustworthiness scores by the trustor organization, as addressed below.
  - *Applied set of trust criteria* depends on the preference and perception of the trustor organization on trust, depending on the objective for establishing inter-organizational trust relationships. Trust objective might vary with time which means the preference and perception of trustor organizations on trust might also vary with time.
  - *Number of involved organizations* depends on the objective of the collaboration that indicates the needed collective competencies and resources owned by selected organizations. The availability of these competencies and resources might vary with time. Furthermore, if the involved organizations change then the optimal values of trust criteria that are used to compute the comparative values might also change (see Section 5.4.1). This in turn might cause changes in the levels of trust in organizations.
  - *Interpretation of trustworthiness* score depends on a number of issues such as the trust objective, risks associated with the collaboration, previous experience of the trustor, etc. which also vary with time.
  - *Applied trust related data* is based on the performance of an organization both within the VBE in collaboration with other organizations and from individual organization's projects. As organizations continue participating in different activities their performance data is collected and thus their trust related data is updated which means it changes with time. This implies that their trust level will also be continuously evolving with time.
- *Dimensions of trustworthy behavior:* Trust among individuals can be grounded into the evaluation of three main specific characteristics, namely their ability, integrity and benevolence [Cosimano, 2004]. Furthermore, the more a trustor observes and/or identifies

these three characteristics in a trustee, the more likely the trustor's level of trust in that trustee will grow [Msanjila & Afsarmanesh, 2007a], as addressed below.

- *Ability* typically refers to the trustee's knowledge, skill, or competency. This dimension recognizes that establishing trust relationships depends on the trustee being capable of performing properly and meeting the expectations of the trustor.
- *Integrity* refers to the degree to which the trustee adheres to principles that are acceptable to the trustor. This dimension leads to trust, based on the consistency of past actions, communication credibility, commitment to standards of fairness, and the congruence of the trustee's word and deed.
- *Benevolence* refers to the trustor's assessment of how concerned the trustee is about the trustor's welfare, in order to either advance the trustor's interests, or at least not to impede them. Here, the trustee's intentions and motives are the most central issues. For example, honesty and open communication, the delegation of decisions, the sharing of control, and so on, all act as an indication of a person's benevolence.

- *Different stages of trust development:* Early theories on trust have described it as a uni-dimensional phenomenon that simply increases (or decreases) the magnitude and strength of a relationship [Ishaya & Mundy, 2004]. Recent approaches suggest that trust builds in continuous and sequential stages. Therefore, trust may grow with time to 'higher' levels (or diminish to lower levels); moreover, it can become stronger and more resilient. When defined by *calculus-based trust (CBT) and identification-based trust (IBT)* trust can be dynamic [Ishaya & Mundy, 2004], as is discussed below.

During the early stages of a relationship between two individuals, the level of trust is mainly *calculus-based*. In other words, the trustor (with the help of trust experts) can carefully calculate the trustee's likely level of trust in a given situation. This also depends on the environment's rewards for being trustworthy and deterrents against untrustworthy behavior, as these encourage more trustworthy behavior. Over time, *calculus-based trust (CBT)* can grow as individuals are able to improve their reputation and assure the stability of their behavior by behaving consistently, e.g. meeting deadlines, fulfilling promises, and so forth. CBT is largely a cognitively-driven trust approach, grounded in judgments about the trustee's predictability and reliability [Castelfranchi & Falcone, 2000]. However, once actors come to a deeper recognition of each other through repeated interactions, they become more aware of each others' shared values and goals. This allows their trust relationship to grow and reach a higher and more qualitative level.

When trust between the trustor and trustee evolves to its highest level, the function is called the *identification-based trust (IBT)* [Settle, 1998]. At this stage trust has grown to the point that the actors have internalized each other's desires and intentions. They understand what the other actor really cares about and, therefore, each actor is in fact able to act as an agent for the other. Trust at this advanced stage is also enhanced by a strong emotional bond between the actors, based on the sense of shared goals and values. So in contrast to the CBT, the IBT is more emotionally -driven, grounded in perceptions of inter-personal care and concern, and a mutual need [Lahno, 2001].

2.2.3 Trust in different disciplines

Trust is a key concept addressed by research in many disciplines and it is gaining importance in the emerging information society. In this sub-section we present the reported research on perceptions of trust in five different disciplines, namely sociology, economics, psychology, politics and computer science.

In sociology, trust is defined through reputation and previous interactions among individuals. Furthermore, the ways and reasons by which reputation for trustworthiness is established or destroyed are being studied in social trust relationships. Not only will the perceivers of reputation have access to information which the reputation holder does not control, but also the manner in which both types of information are interpreted is not straightforward [Good, 1988]. Therefore, individuals wish to have complete information about the people with whom they deal before dealing with them [Dasgupta, 1988].

In economics, decisions about trust are similar to decisions about taking risky choices. Individuals are assumed to be motivated to establish trust relationship with each other in order to either maximize the expected gains, or minimize the expected losses from their transactions [Josang & Lo Presti, 2004]. The critical factor with respect to trust in economic studies is the risk management related to trust relationships. Trust in psychology is related to beliefs. A trusting behaviour occurs when an individual believes that there is an ambiguous path; the result of which could be good or bad [Morgan & Hunt, 1994]. The occurrence of the good or bad result is contingent on the actions of another person. If the individual chooses to go down that path, he makes a trusting choice.

In politics and digital governments, trust is related to truth telling. It is important for digital government, to maintain high standards of truth telling and to avoid being associated with poor reputation and thus loosing the trust of the public [Sztompka, 1999]. Trust in governments and politics is essential in order for the governments and the related political parties to remain in power. However, several other factors are also identified as influential on the level of trust governments have towards their citizens, such as reputation, performance, accountability, commitment, and so on [Sztompka, 1999].

In computer science, trust has been mainly associated with security, privacy and reputation. Establishing trust among interacting systems that are developed based on the service oriented architecture depends on their compliance to the set of communication policies. These policies provide regulations that must be met by a system to be trusted [Blaze, et al., 2009]. Generally, when an environment is secure, it is easier to establish trust relationships among the systems' users, and equally if a user respects the privacy of others in relation to their personal data and sensible information he can be regarded as trustworthy [Seigneur & Jensen, 2004]. Reputation is being used for managing trust in systems that are developed using multi-agent technology; therefore, in multi-agent systems the trustworthiness of a trustee represented by an agent "*b*" is assessed by a trustor represented by an agent "*a*", using the reputations witnessed by the trustor (or trustor's friends) or certified by the trustee's friends [Huynh, et al., 2004].

None of the existing studies have adequately addressed *trust among organizations*, particularly within collaborative environments such as VBEs [Msanjila & Afsarmanesh, 2006b]. Among other reasons, this inadequacy is due to the fact that the collaborative networked organization (CNO) is itself a newly emerging scientific discipline [Camarinha-Matos & Afsarmanesh, 2005], and thus demands innovative approaches and mechanisms to support its necessary establishment and operation. Also, the collaboration for which the establishment of trust is required is not at the level of individuals since it is dealt with traditionally, but at the level of which the involved participants are only organizations, as is further discussed in Section 2.3.

VBE members may constitute organizations that operate in different domains or disciplines. The member organizations might differently perceive trust, e.g. according to their

trust objectives their perceptions might be influenced by a number of aspects related to what is believed to be important for their businesses and future goals. We address inter-organizational trust in VBEs considering a wide variety of the above aspects, taking into account how those aspects are characterized in various disciplines as some of which are briefly addressed in this section. Large volume of aspects from different disciplines is analyzed later in this thesis and classified into five "points of view" that are referred to as trust perspectives, further addressed in Section 2.3.6 and in Chapter 3. For instance, the elements of trust addressed above from the politics and digital governments discipline constitute a part of the managerial perspective of our proposed model, while the psychology and sociology aspects are related to social and managerial perspectives, and the computer science aspects are related to technological perspective, etc.

2.3 Trust among organizations in VBEs

The emerging preparatory co-working environment (or 'VBE'), as described in Chapter 1, is characterized by some features that have never been practiced before. In this section we address these emerging practices and the research results that have been achieved on trust among organizations involved in VBEs.

2.3.1 Importance of creating trust between organizations in VBEs

VBEs are characterized as multi-actor environments, in which each actor organization is autonomous, and has interests and goals that might contradict those of others. A catalyser for the enhancement of cooperation between member organizations in VBEs is the establishment of trust relationships, which is why past research states that trust is the most salient factor for cooperation networks in achieving the network objectives [Morgan & Hunt, 1994]. Trust relationships between organizations are more important for large VBEs where direct personal contact are more difficult to achieve by all, while they shall operate under pressure from the global economy, the increasing value of information, and the mounting uncertainties surrounding their businesses [Msanjila & Afsarmanesh, 2007a]. Several advantages can be gained once trust relationships between member organizations have been properly established and managed in the VBE. Following are some example advantages gained by establishing trust relationships between organizations in VBEs:

- Facilitating the achievement of common goals through information exchange, knowledge sharing, tools sharing, and so forth, between member organizations.
- Enabling the member organizations to cope with uncertain or incomplete information.
- Easing the process of creating and launching VOs and smoothing the partner selection processes.
- Accelerating the contract negotiation process between selected VO partners.
- Encouraging the member organizations to avoid opportunistic behaviour during collaboration.
- Achieving the competitive advantage, through reduction of governance internalization (acquisitions) tasks, and thus the transaction costs, as addressed in Sections 1.2.2, 1.2.3, and 3.3.2.
- Enabling open communication and thus reducing conflicts between member organizations.

2.3.2 Antecedents of trust between organizations in VBEs

Trust antecedents are cardinal elements that may have a positive or negative impact on the effectiveness of the established trust relationships among organizations. Three trust

antecedents are identified for organizations in this thesis, namely the *shared values, the previous interactions,* and *the practiced behaviors*. Strengthening of these antecedents shall be aimed by all VBE member organizations as well as the VBE administration.

Shared values: Shared system of values occur when the trustor organization and the trustee organization have a common understanding on important issues that might influence the creation of trust towards each other, such as their missions, goals, policies and interpretations of right or wrong [Morgan & Hunt, 1994]. Shared values can range from business objectives to internal management processes and approaches. In business environments, it is more difficult to have shared values between two competing organizations than between two organizations that are complementing each other [Clay & Strauss, 2000]. Typically, when two organizations have a common understanding/perception and/or belief in a set of values they both feel secure in the knowledge that there will be no unexpected results during their cooperation/collaboration. It is therefore easier to establish a trust relationship under such conditions. As an aspect of preparedness, the VBE must ensure that member organizations establish shared values with other organizations within the VBE. In a VBE shared values among member organizations can be achieved through the following approaches among others:

- Establishing and maintaining a definition of common VBE value system
- Enhancing and maintaining transparency by the VBE administration
- Performing joint activities among member organizations within the VBE
- Establishing a common or interoperable ICT-I for all organizations in the VBE.

When member organizations achieve some level of shared values with each other then the process of establishing trust relationship between them can be easier accomplished [Msanjila & Afsarmanesh, 2007d].

Previous (fruitful) interactions: Previous (fruitful) interactions between the trustor organization and the trustee organization - either directly or indirectly (through other intermediate organizations) – may enhance the effectiveness of established trust relationships. These time-related interactions can be formal such as the formal exchange of information, knowledge or expertise. Interactions can also involve individuals who work within the two organizations either technical or social. Even though sometimes there may be no current business-oriented interactions, yet the existence of previous informal interactions may smoothen the establishment of trust relationship among organizations.

Member organizations of the VBE have the possibility and are encouraged to interact with each other. Interactions can be achieved through different approaches, among others:

- Inviting representatives of other VBE member organizations to attend organizational general meetings as observers
- Organizing workshop and inviting presenters from other VBE member organizations
- Supporting the sharing of information on public issues of the VBE member organizations through the portal which is maintained by the VBE management system (VMS).

Practiced ethical and/or moral behaviours: Practiced ethical and/or moral behaviours basically refer to the opposite of *opportunistic behaviour*. Opportunistic behaviour means taking immediate advantage - unethically - of any circumstance that may generate possible benefit. Traditionally, opportunistic behaviour in competitive markets seemed natural because the typical focus of organizations in such environments was on the acquisition of customers, without regard for long-term relationships with other organizations. In collaborative networks however, organizations must rather cooperate in order to best serve the same customers.

Opportunistic behaviour has therefore a negative impact on the effectiveness of trust relationships among organizations. It mainly derives from transaction cost literature and is defined as *seeking self-interest with guile* [Mukherjee, 2003]. Here we refer to opportunistic behaviour as an *ungentle action that might be taken by VBE member organizations for the purpose of benefiting themselves* ***unethically****, more than others (e.g. quitting the collaboration once they have made a large gain, or when they expect the risks of the collaboration to become a threat).*

2.3.3 Main related challenges in trust studies for VBEs

In relation to the analysis of trust in VBEs, we have identified three main challenges that must be well-addressed in order for trust to be realized and met by VBE member organizations, VBE administration and external stakeholders. These are as follows:

Main related challenge 1- Causality: a major challenge for the analysis of trust is its causality. The future trustworthiness of an organization is "causally" related to its role and behavior at present, and actions it has performed as well as events it has caused in the past. Therefore, a part of trust engineering in VBEs is intended to support decision-making about the present and future trustworthiness of organizations, while the information needed for this estimation can mostly be derived from the past.

Main related challenge 2- Transparency and fairness: one more challenge for the assessment of the level of trust in organizations is the transparency and fairness for all stakeholders. Each step taken for entire process of assessing the level of trust must be clear and transparent for all involved organizations. For fairness, the steps taken and approaches used for an assessment of the level of trust must be accompanied with some formal reasoning, and also the information used for the assessment must be accredited and/or certified to avoid personal (subjective) judgment and biases.

Main related challenge 3- Complexity: another challenge for trust analysis in VBEs is the way in which the complexity of the multi-objective, multi-perspective, and multi-criteria nature of inter-organizational trust is handled. As discussed in this thesis, trust is not a single concept that can be applied to all cases of trust-based decision making. Measurements of level of trust are subject to both the purpose of the trust relationships, and the specific actors involved. Every case is different and requires the employment of specific trust criteria in order to assess the level of trust.

2.3.4 Boundary characteristics of rational and subjective trust

Subjective trust is the most adopted and practiced form of trust for smoothening interactions among individuals. However, nowadays collaboration among organizations has become a fundamental approach for co-working in business, such as joining initiatives and efforts for the purpose of enhancing competitive power in the market. Applying subjective trust concept is difficult here as it lacks a reasoning approach and/or mechanism for results of the assessment of level of trust in organizations [Msanjila & Afsarmanesh, 2007a]. As a result, rational trust analysis is currently gaining in popularity [Castelfranchi & Falcone, 2000].

Subjective trust is created on the basis of qualitative data and is opinion-based. Some fundamental sources of information for creating subjective trust among parties include experience and knowledge of trustors on trustees, recommendations of third parties on trustees, previous interactions, trustees' reputations, and so forth.

Rational trust (objective trust) is created on the basis of quantitative data and is fact-based. The main source of trust related data is the organizational performance which is accumulated in the past from different activities in which it participated, both in collaboration with other partners, and as an individual organization. Rational approaches for assessing the level of trust in organizations employ formal mechanisms, such as mathematical equations, which in turn provide some formal reasoning of the resulting level of trust [Msanjila & Afsarmanesh, 2007a].

Subjective trust and rational trust also differ with respect to the "*boundaries"* that are applied. The real challenge here relates to a definition of where these boundaries start and end for daily interactions among actors, for both subjective trust and rational trust.

Boundaries for subjective trust: Boundaries for subjective trust can be discussed in relation to the transitive and propagatory nature of trust among involved actors. Subjectively, trust transitivity means, for example, that if "Alice" trusts "Bob" and "Bob" trusts "Eric", then "Alice" trusts "Eric". This assumes that Bob actually tells Alice that he trusts Eric, which is called a *recommendation*. In social and individual interactions, in which subjective trust is mostly practiced, trust can be assumed to be transitive. This is because trust among individuals participating in these interactions is mostly created on the basis of other people's opinions. The opinions of these people, who trust a specific individual, are used to create trust with a new trustor. Thus, subjective trust is transitive.

It is common to collect advices from several sources in order to be better informed when making decisions. In other words, it is also common to collect several recommendations in order to convince a trustor, such as for job application, of the trustworthiness of a trustee. When the trustor has different sources of recommendations from which he or she can create trust for the certain trustee, a specific characteristic of trust transitivity emerges, namely *parallelism*.

Since subjective trust is transitive, the most complex issue concerns the point at which the propagation starts to diminish and lastly stops. This point defines the trust boundary, yet it is not clear which factors may indicate it. As such, even the trust boundary itself from one trustor to another is subjective.

Boundaries for rational trust: It can be shown that trust is not transitive for "objective-specific" collaborations and transactions, for which the rational trust is mostly needed to be practiced. For example, the fact that Alice trusts Bob to look after her child, and that Bob trusts Eric to fix his car, does not imply that Alice trusts Eric to look after her child, or to fix her television. This is because "trust objectives" in these two cases differ. Rational trust is created on the basis of facts and the application of formal mechanisms, in which different cases will have different preferences. As such, the value of the level of trust in this case is not absolute and cannot be transferred to different cases, which is why rational trust is more suitable than subjective trust for smoothening organizations' specific objective collaborations. Therefore, rational trust is not transitive.

Rationally, a trust boundary does not exist, since trust is created on the basis of preferred perspectives. Different trustors may prefer different perspectives in order to trust the same trustee. In other words if the same set of trust criteria is preferred for all trustors, the same level of trust shall be achieved, regardless of the trustor. Therefore, rational trust does not propagate among involved actors and thus all trustors shall trust their respective trustees on the basis of their own preferred perspective.

2.3.5 Main concepts related to inter-organizational trust

Trust is related to different concepts and these relations either complement (such as trust and security, reputation, co-working) or contradict (such as trust versus risks, privacy, and so on.) its perceptions among actors. This section discusses trust in relation to five concepts, namely: (a) trust versus risks, (b) trust and security, (c) trust versus privacy, (d) trust and reputation, and (e) trust and organizational virtual co-working.

a) Trust versus risks

Risk is a concept that denotes a potential negative impact to an asset or some characteristics of a value that may arise from present processes or future events. In everyday usage, "risk" is often used synonymously with the probability of a known loss. Many definitions of risk depend on a specific application and situational contexts. Frequently, risk is considered as an indicator of threat. It can be assessed qualitatively or quantitatively. Qualitatively, risk is considered proportional to the expected losses which can be caused by an event and to the probability of the same event. The harsher the loss and the more likely the event, the greater the overall risk. Measuring risk is often difficult; the probability is assessed by the frequency of past similar events, which in fact is difficult to link to the future. Trust and risk are negatively related. When there is a high chance that certain risks may arise in a certain environment it is very difficult for an organization to trust other organizations in that specific environment. Moreover, when organizations trust each other they tend to relax and rely on one another based on the assumption that risks may not arise. However, this attitude may in time increase the chance of risks arising due to new changes inside each organization.

Different types of risks may arise while organizations are collaborating in order to achieve their common goals. Below are six example types of risks related to organizations that shall be considered when aiming to reduce the severity of their impact on inter-organizational trust relationships in the VBE.

- ***Strategic risks:*** Several different strategic risks may be associated with operating in various types of business or industry domains. These include risks arising from acquiring business opportunities, changing customers, changes in customers' demands, changes in operating environments, and emerging innovative results from research and development. Organizational strategies must be flexible enough to accommodate such changes. Rigid strategies can result in risks, such as the failure of an organization to properly integrate and collaborate with other organizations in VOs as a result of unacceptable or outdated strategies.
- ***Operational risks:*** Operational risks may exist as a result of direct or indirect loss that has been caused by for example inadequate or failed internal processes, employees' behaviour that might compromise security of information management system, etc. An organization's failure to achieve the agreed results due to internal problems endangers the success of the entire consortium to achieve its common goals. Therefore, operational risks that may arise for both the organizations and the consortium must be properly addressed.
- ***Legal and cross-border risks:*** These are risks that may exist due to changes of rules, regulations and laws imposed by governments or local authorities. Usually business organizations have limited influence on the make-up of regulations and rules, for instance, only through lobbing but not direct involvement in the process. The organizations involved in a VBE might in addition be subjected to different regulations, e.g. for different sectors or in different countries. Changes in regulations in a country where one

of the member organizations is located might for example create risks for their cooperation with other organizations located in different countries. This is especially an issue when laws and regulations in the two countries contradict.

- ***Financial risks:*** VBEs have to deal with financial risks to sustain the collaboration among member organisations. There are various types of financial risks, among others, they include: credit, liquidity, transactions, interest rate and currency exchange rates.
- ***Reputation risks:*** Reputation risks are related to an organization's image and instability as a result of negative opinions, either from other member organizations in the VBE, or from the public. Poor reputation affects an organization's ability to establish new trust relationships with other organizations, or to continue with existing trust relationships. Reputation risk exposure must be properly dealt within an organization and may require exercising caution in dealing with customers and the community.
- ***Technology related risks:*** Current risks surrounding ICTs, such as network failures, lack of qualified human resources and insufficient skills, lack of network security, hacking, viruses, etc., have the potential of a greater negative impact on an organization than ever before, since collaboration and cooperation are both facilitated by computer networks. Additional risks posed by technologies might include lack of privacy, unauthorized information access, increased complexity of applied technologies and so on.

In traditional business investments, greater risks are associated with higher expected returns. In organizations, tradeoffs in relation to risks are about the returns on investment that will be obtained once a specific risk has been accepted and the outcome of taking this risk has been favorable. However, cooperation between organizations in the VBE may not provide an immediate return. The economical benefits of cooperation between member organizations include an increase in their chances of acquiring better and more opportunities as well as involvement in VOs responding to opportunities brokered with other organizations.

In practice, trust and risks are inversely related - when one increases there is a high chance that the other will decrease. Therefore, if risks existing in a certain VBE environment increase then organizations operating in this environment will feel at risk and will hardly establish trust in other organizations. Similarly, if organizations trust each other to a great degree then they will feel that risks are unlikely to arise during the course of collaboration (e.g. minimal possibility of occurring an opportunity behavior) and thus do not pay attention to the need for preparing themselves against risks.

Considering the style of virtual co-working in VBEs, organizations may interact with others without ever meeting face-to-face, thus enhancing fears about some potential risks, such as those discussed above. One strategy that organizations can assume as a means to avoid risks associated with collaboration is being reluctant in engaging in such trust relationships with other organizations. However, such a strategy can cause problems with respect to sharing resources, knowledge, competency, and information which are necessary for facilitating collaborations in VBEs. Cooperation in the VBE and collaboration in VOs are the only potential styles of co-working that have demonstrated to be suitable for member organizations in these environments. Establishing trust relationships between participating organizations has proven to be an amenable facilitator that eases cooperation between organizations in the VBE as well as their collaboration in configured VOs. However, a challenging issue for VBE administrators is how to convince organizations to establish and commit to their established trust relationships despite the existing risks. In the VBE, member organizations are encouraged to trust others in order to smoothen their collaboration through the following strategies:

- Enhancing the sense of togetherness and safe feelings among organizations in the VBE by promoting the culture of sharing day to day information, useful knowledge, etc., through the common storage and retrieve portal called "*bag of assets*" [Afsarmanesh, et al., 2008].
- Defining and applying a comprehensive set of "*working and sharing*" principles that can also provides guidelines on how to share any kind of loss caused by collaborative business among organizations due to emerged risks during the collaboration [Romaro, et al., 2008].
- Defining and encouraging use of proper *value systems* in the VBE that will also provide a set of performance indicators for measuring performance of organizations, which in turn provide data to be used as input to the computation of the trust level of organizations.
- Define *rewarding strategies and build reward mechanisms* to encourage good behavior and high achievements for organizations in collaborative activities.

b) Trust and security

Inter-play between trust and security can be examined from different aspects. The two most popular aspects that are also discussed here are: in respect to management systems and in respect to technologies owned by and available to organizations.

Trust and security for management systems

Until a few years ago, enhancing the security of systems that are used for the management of information, resources, stored knowledge, available skills, and so forth, was the fundamental approach used to enhance trust among collaborating organizations. Since this time and even currently, the situation has changed dramatically. New security regulations, significant security, privacy incidents, and so on, are no longer enough to guarantee smooth operations for business organizations on markets that currently present continuously increasing turbulent conditions [Grandson & Sloman, 2000]. Consequently, it is now fundamental that the search for solutions and a balance between trust and security in relation to the ICT systems and the facilitated businesses now involves both business organizations and ICT industries.

From a business perspective, security mainly concerns the management of risks and, in this case, with respect to ICT-facilitating tools. Current markets are characterized by turbulent conditions, including scarce resources, lack of knowledge and skills, volatile business opportunities, changing and emerging unique customer requirements. Therefore, enhancing the security of the ICT systems and managing the related risks do not fully guarantee the success and survival of an organization in the current market.

An ICT system can provide the right level of security whether or not it keeps the risks for business at an acceptable level. Potential losses due to malicious acts by disgruntled employees, hackers, unauthorized users, and so on, are central to each risk. Whether a risk is acceptable or not is a business decision and is not only influenced by the state of the ICT system, but also by many more different factors relating to the system, such as the behavior of other partners, changes in business requirements, and so on [Msanjila & Afsarmanesh, 2007c]. The description of a security level and the demonstration that an ICT system meets this level are fundamental challenges in computer science, and specifically in relation to the newly emerging needs of management to build inter-organizational trust. It is more challenging in the current climate as organizations have to collaborate together in order to acquire and respond to opportunities. This collaboration needs geographically distributed support from ICT systems. The level of security that is enough to support the creation of inter-organizational trust in such an environment is still unclear and it is difficult to define.

The security of an ICT system alone is not sufficient for smoothing cooperation and collaboration among organizations, and thus guaranteeing the necessary success and survival. As a result, security boundaries among organizations are fast becoming increasingly less stringent. Therefore, trust propagation that is based on the security of an ICT system is decreasing and becoming rationally specific. Applications that used to run on dedicated servers now are running on virtual environments, sharing infrastructure with others, and using widely-distributed physical resources [Rabelo, et al., 2006]. This makes the process of creating inter-organizational trust with the application of system security even more difficult.

As a result of amplification of problems related to the security of ICT systems, risks associated with businesses supported with ICT systems, market turbulences, and so forth, certain other approaches for smoothing co-working environments - such as VBEs - are needed and must be considered. Managing trust among organizations, by applying rational mechanisms for assessing level of trust and creating trust, has emerged as a promising approach for achievement of the required smoothening [Msanjila & Afsarmanesh, 2007a]. In our approach, systems (Trust Management systems) are suggested as a means to support organizations in the performance of tasks related to creating trust of their organization in others. A number of processes also need to be supported with tools in order to provide the required services for the management of trust among organizations, as discussed in Chapter 6.

c) Trust and security in relation to owned and experienced technologies

There has been a misconception about trust and security, and roles that technology plays in this binomial for setting/facilitating collaboration. Most people tend to believe that trust is merely the result of security - when security exists, actors can trust each other - but researchers have observed that this notion does not represent the entire picture [Rousseau, et al., 1998]. Trust is a wider concept and its link with security is not linear [Msanjila & Afsarmanesh, 2007c]. Technology can effectively provide security; for example, every step of an online transaction has one or more procedures for transmitting users' data safely, such as using cryptography and protocols technologies. However, this does not represent trust. Security-driven approaches for creating trust among organizations have led to a bias entitled "*the double illusion of 100% safe*" [Weth & Bohm, 2006].

It is said that technology is always deceptive: it is safe until it is violated. Every secure environment will soon become insecure, because technical innovation occurs in both the positive area of security protocols and the negative area of hacking processes. Organizations that use security of environments that are enhanced by technology as the only means of trusting others might face difficultly when unexpected problems occur, such as the hacking of software [Grandison & Sloman, 2000]. This is the first illusion.

Imagine for a moment that a secure environment has been obtained. Organizations are able to act freely and confidently because they are protected by technology. However, this is not a trust-building atmosphere because the importance of trust increases when there is a chance that certain risks may increase [Rousseau, et al., 1998]. An environment depicted with hard technology protection deteriorates trust building: organizations feel the security but not necessarily trust. This is the second illusion.

d) Trust versus privacy

At the individual level, privacy can be seen as a fundamental human right. Similarly, organizations are now facing problems related to privacy and, more specifically, with respect to confidential data and strategies. Different legislative and technological mechanisms have

been proposed to enhance the privacy of organizational data in the world of computers. Protection depends on whether privacy is seen as a right, which should be protected by laws; or a need, which should be supported by devices [Msanjila & Afsarmanesh, 2007c]. From the point of view of privacy and considering the co-working among organizations, there is an inherent conflict between trust and privacy: the more knowledge a first entity gains about a second entity, the more accurate the results will be of the level of trust assessment. Nevertheless, the more knowledge is gained about the second entity, the less privacy is left to this entity [Seigneur & Jensen, 2004]. The contradiction of enhancing level of trust in organizations, while at the same time enhancing their privacy, is a challenge for further research.

e) Trust and reputation

Reputation concerns general opinions (more technically, a social evaluation) of the public toward a person, a group of people, or an organization. It is an important factor in many domains, such as business, online communities or social status. Reputation is known to be a ubiquitous, spontaneous and highly efficient mechanism of social control in natural societies. It is a subject which is being studied in disciplines such as social, management and technological sciences. Furthermore, reputation acts on different levels of agency, namely individual and supra-individual. At the supra-individual level, it focuses on groups, communities, collectives and abstract social entities (such as firms, corporations, organizations, countries, cultures and even civilizations) and it affects phenomena at different scales, from everyday life to relationships between nations. There are two kinds of reputation: *witnessed reputation* and *certified reputation.*

Witnessed reputation [Huynh, et al., 2004] refers to the reputation-related information that is collected by the trustor, or the trustor's associated organizations (friends). In this case, the trustor organization or its associated organizations observe characters of the trustee organization to decide its trust level. In VBEs, where organizations collaborate virtually, the adaptation of this approach is hardly feasible.

Certified reputation [Huynh, et al., 2004] refers to the reputation-related information that is collected by the trustee organizations and made available to the trustor organization. The trustee organization can provide information such as a detailed organization profile, recommendation letters, accreditation documents, auditing results, etc., to the trustor organization in order to enhance its trust level. The trustee organization can also request its friend/authorized organizations to provide positive information (e.g. accreditation document) to the trustor organization in order to enhance its trust level. The main problem of this approach is that there is high risk of user-biased information, which endangers the success of the resulting trust relationships. The validation of such information is also difficult since, in practice, bad reputations are usually hidden.

The management of an individual's reputation involves recording a person's actions and the opinions of others about those actions. These records can then be made available in order to allow other people (or agents) to make informed decisions on trusting that person. A reputation management system, particularly as applied in multi-agent technologies, which use pre-programmed criteria for reputation management, facilitates the process of supporting cooperative behaviour over selfish behaviour. Reputation has been applied in different disciplines to study relations between entities and their trustworthiness.

f) Trust and virtual co-working among organizations

The emerging economy is knowledge-based and without borders, and competition exists among both local and national organizations on how to learn faster and organize more flexibly so as to take advantage of the "technology-enabled" market. Within this new economy, ICTs are ubiquitous. They have transformed geographically separated locales into a "global village" for information sharing, organizational interactions, and an exchange of economical value. Technology, and in particular ever-expanding digital bandwidth, has resulted in the creation of new economy forms of intangible, knowledge-based capital, the value of which now exceeds that of the physical capital that once dominated old economies (Afsarmanesh & Camarinha-Matos, 2005). Whereas business models for the old economy emphasized tasks and roles organizationally, business models for the new economy focus on self-organizing: teams, companies, industry-based clusters, or CNOs. Organizations have realized that by virtually co-working, such as in CNOs, they can enhance their chance of jointly meeting the opportunities presented by the continuously changing requirements of "innovation-demanding" opportunities more effectively (Camarinha-Matos & Afsarmanesh, 2006). There are three questions that need to be addressed when considering technology in relation to virtual co-working (Msanjila & Afsarmanesh, 2007c):

i) What are the distinguishing factors that separate ICT-enabled collaboration in physical setting from virtual setting?
ii) Can previous findings on physical collaboration help us to understand the characteristics of emerging virtual collaborations?
iii) How does the creation of trust differ for physical collaborations and for virtual collaborations?

Innovative organizations that employ technology to facilitate collaborative projects are the hallmark of the new economy (Camarinha-Matos & Afsarmanesh, 2006). Such collaborations can range from arms-length information sharing to highly inter-dependent and geographical dispersed joint projects. In large VBEs, organizations cooperate/collaborate with others that sometimes are physically unknown to them. These organizations must trust each other in order to work together effectively. Basically, in the current innovative-based economy, trustees must possess technologies which can facilitate virtual co-working.

Moreover, the current economy demands the ability to acquire and possess competitive information and knowledge. Technologies are playing a great role in efficiently achieving such organizations' goals. The number of domains where technical artifacts are filtering into communications and relationships is increasingly growing, and now include computer supported interactions, computer supported co-work, e-commerce, etc. These are a few examples of this trend. In relation to technology, the importance of trust is twofold: (1) it can be seen as trust towards technical systems (i.e. with electronic payments), and (2) trust in technologies as mediators of interactions between organizations. Thus, when setting up technologically-related collaboration, organizations that possess the required technologies are judged to be technologically trustworthy.

2.3.6 Different aspects of trust in organizations - applied to the proposed approach

Most reported research results have addressed trust among organizations with a consideration of only a few aspects and in most cases with the application of only a single point of view, e.g. financial aspects. In our research we have identified five independent trust perspectives that comprehensively cover fundamental aspects which can be considered by trustor organizations,

namely, technological, structural, economical, social, and managerial as further discussed in Chapter 3. It should be noted that for different trust establishment objectives, only some of these perspectives may be relevant as exemplified in Chapter 1. This section briefly describes these five perspectives, and a discussion of their related aspects follows in the Section 3.3.

i) Technological aspect of inter-organizational trust

The current new economy is a knowledge-based economy without borders, where competition now lies not only in acquiring business, but also in acquiring and owning technology for the purposes of communication and the delivery of products/services. Technology can play two roles: (1) facilitating collaborations among organizations in a collaborative consortium, acting as a communication infrastructure; and (2) applying in production for use as resources (e.g. machines, computers, etc.). Thus organizations possessing technologies, which thoroughly address these two technological roles, will be judged to be trustworthy. A number of technologically-related aspects of inter-organizational trust have already been described in the previous section (Section 2.3.3) of this chapter, namely in relation to security, privacy, risks, and so forth. Aspects of technological perspective are discussed in Section 3.3.

ii) Structural aspect of inter-organizational trust

As an organization grows in size, geographical scope (coverage), and capabilities (competences and expertise), etc. its structural performance improves. It enhances thus its capability to transform, collaborate and cooperate, its structural trustworthiness. This perspective is further discussed in Chapter 3 in an elaboration of the approach used to analyze inter-organizational trust.

iii) Economical aspect of inter-organizational trust

Today's technologies and volatility of opportunities have encouraged organizations to start investigating and deploying values of trust that can be achieved through economical successes. Globalization has changed the old rules of competition and continuous innovation has become a strategic priority [Blomqvist, 2005]. With current advances of information and communication technologies (ICTs), it is difficult for organizations to keep information about their business strategies and investment plans confidential. At the same time, government policies aim to encourage collaboration between organizations [Assimakopoulos & Macdonald, 2002], which in turn requires extensive sharing of economical data. While organizations are not willing to let their competitors access their potential business data and thus are only looking for advanced mechanisms to enhance their privacy, new forms of collaborative networks, such as VBEs and VOs, encourage openness and sharing. Challenging issues here relate to selecting trustworthy partners with which to share such strategic economical information. The challenge remains of which information to make accessible and of finding a level of accessibility that is acceptable for all stakeholders. Below are the key economical elements for the creation of trust among organizations in VBEs [Msanjila & Afsarmanesh, 2006a]: (1) Collaborative ***economical success and survival*** of organizations in a VBE depends on the amount of trust between them, (2) the possibility of finding ***scarce resources and lacking knowledge*** owned by other partners depends on the intensity of trust among involved organizations, (3) trust among organizations reduces the frequency of the occurrence of ***financial risks*** such as by discouraging opportunistic behavior, and (4) trust among organizations enhances the ***interoperability*** between business processes at different organizations. Based on an economical perspective, trustors need to access economical data for assessing level of trust that will persuade them to create trust for trustees. Aspects related to this perspective are discussed in Section 3.3.

iv) Social aspect of inter-organizational trust

An accurate definition of social trust is difficult to establish. However, it has been encapsulated as an ongoing motivation of social relations that form the basis for interactions. At the individual level, social trust can entail perceived honesty, objectivity, consistency, competency, and fairness; all of which foster relationships among individuals that must be maintained by the sustained fulfillment of these elements [Boslego, 2005]. A decision to trust on the basis of a social perspective has been described by several trust experts as a "risk judgment", which is a form of cooperation that has no immediate payoff or benefit, and one which involves a gamble that trusted parties will act as expected [Good, 1988]. Aspects of social trust are not universal, but vary across cultures, contexts, countries, and so on.

While people may trust their relatives, co-workers, classmates, friends, and even their friends' friends, the puzzle of social trust is the idea of trusting strangers. The difficulty a person encounters in trusting a stranger is similar to that which an organization faces when it needs to trust another completely unknown organization with which it has previously interacted. The only basis on which social trust other organizations can be judged is that organization's social performance and status, which may be influenced by their ethnic or cultural group, the characteristics and values of the society in which they were registered and are currently operating, their past experiences and interactions, and - more broadly - the historical tradition of their society [Msanjila & Afsarmanesh, 2006a].

The practical challenge concerns the actions to be taken once social trust has been broken. Should organizations with many racial, religious, and ethnic problems resign themselves to low levels of trust, or can trust be somehow re-engineered? Social trust is a good public phenomenon that should be maximized, and is thus non-excludable, non-rivalrous, and does not result in direct profit, but benefits organizations and society indirectly. Consequently, it must be re-engineered whenever is needed.

In VBEs, organizations must enhance their trust from the society in which they are operating. Social trust for an organization is very important as a way to maintain moral acceptance from the society in which it is operating its business. For social trust, internal achievements of the organization receive little attention in comparison with its external social achievements. Aspects of social perspective are discussed in Section 3.3.

v) Managerial aspect of inter-organizational trust

The need for flexible and responsive organizations has been widely publicized in today's technologically-enabled and competitive market. In order to support this flexibility, a shift has taken place to new organizational structures and processes. Organizations in this century cannot remain static. They must constantly respond to dynamic environments. What is more, they must also learn to take a proactive stance, even creating changes. To be in a static mode may mean that organizations will be left eating the dust of their competitors when markets and technologies advance [Msanjila & Afsarmanesh, 2007c].

The changes, uncertainties, and complexities that characterize today's greatest challenges in business and in particular in those performed in virtual world, also present challenges to managers at all levels. Responding to changes in external environments requires ever-vigilant managers. Managers must be flexible in order to effectively promote flexibility in their organizations. The necessary flexibilities include the flexibility to manage and compete for VBE rewards, the ability to flexibly and collaboratively plan, flexibility in collaborative problem solving, technological flexibility, and flexibility in addressing VBE politics [Msanjila & Afsarmanesh, 2006a].

Although the palpability of trust is known to organizations in VBEs, it still proves difficult to create. VBE administration cannot be successful without acquiring trust within those organizations that the administration is managing, whether at the level of the organization or at the level of the VBE. There are two possibilities from which a trustor can create trust to a trustee, based on managerial aspects:

- Trustors can trust trustees only focusing on current tasks or roles and specifically on aspects of managerial *competency* to fulfill those particular roles or tasks. This kind of trust is referred to as *situational-based rather than relational-based.* For example, business organizations trust credit card companies to handle the financial transactions that taking place all over the world using their cards. However, these business organizations can hardly trust credit card companies to train their employees on financial management. This *competence-based trust* is rationally developed and needs certified evidences. It can emerge quickly and it does not require previous interactions.
- Trustors can also trust trustees by assessing and evaluating their *motivations.* This kind of trust takes much longer to develop because both actors must be able to *understand and experience each other's intentions.* The difficulty here is that managers might have self-interests that may lower the trust of their organizations. This kind of trust needs rational data that is based on the previous performance of managers.

For some purposes, trustors may consider the managerial history of trustees as the primary element when assessing their level of trust. In this manner, trust assessment is based on how well trustees have behaved professionally and how well power has been used in management positions in past networks, such as in VOs. Aspects of managerial perspective are discussed in Section 3.3.

2.4 Characterization of trust related data for organizations in VBEs

In addition to achieving high performance in order to enhance their trustworthiness, organizations in VBEs must be able to provide evidence of validity for their trust related data (performance data expressed in terms of trust criteria as addressed in Chapter 3). In this section we address the classification of trust related data needed to support creation of trust among organizations and we also propose some sources of evidence of validity for this kind of data.

2.4.1 Classification of data for creation of trust among organizations

Organizations' perceptions of trust correspond with both the nature of the purpose of its application as well as with the actors involved. For each specific practice in which a particular group of organizations is involved, trust is interpreted and perceived differently. Organizations therefore may need different kind of information – here referred to as trust-related-data – to trust others depending on the following aspects:

- ***Who:*** Collaborations among organizations in VBEs are characterized as goal-oriented. Inter-organizational trust relationships provide a fruitful basis for achieving common or compatible goals in such collaborations. Organizations will trust other actors on the basis of the role these actors will play in helping to achieve the common goals. For example, in virtual organizations the roles that can be assumed are that of coordinator or partner. Each role might need different kinds of information to enable a certain organization to trust the organization that is seeking trust. Thus the term "who" as applied here is related to the specific role an organization will play within a collaborative consortium.

- ***When:*** In this thesis, the proposed approach for assessing level of trust requires the application of an organization's past performance data as the fundamental input data. The word "past" here is of subjective nature: it is not clear how long into the past the performance data needs to be covered to be sufficient for the organizations that give trust. The preferred time of the collection and provision of information will differ between the organizations that give trust (trustor) and organizations that seek trust (trustee). Consequently, the information that needs to be provided to organizations may vary and differ with time.
- ***What:*** This refers to the information that will be provided to each organization that is participating in the concerned relationship of trust. It is not easy to define in advance the specific type of information that each organization might need in every trust relationship due to the variation of organizations' perceptions in the specific context and preferences on what they think is important to give their trust.
- ***How:*** The validity of the information is influenced by the authenticity of both its sources and the applied mechanisms/tools for data collection and provision. It can be argued that in circumstances in which information sources and data collection mechanisms are highly trustworthy the information provided has high validity.
- ***Why:*** The information that is provided to a specific organization will also depend on the reason why it is requested. Here, this refers to the main trust objective and related sub-objectives for establishing the trust relationship between organizations.

2.4.2 Types of validity evidence for trust related data

Information made available to a VBE by an organization in order to assess its level of trust must be supported by satisfactory evidence of validity. This section proposes two types of evidence that can be used by organizations to examine and assure the validity of their trust related data, namely: ***certified evidence and witnessed evidence***.

i) **Certified evidence**

The validity of information in this category is based on well-defined and agreed standards that the information must meet. The validation is usually performed by authorized organizations. In light of the need illustrated in this thesis for the validation of the trust related data of organizations, we suggest the following five sources of certified evidence:

(a) *Accreditation:* Accreditation is defined as an independent act of granting recognition to an organization as proof that the respective organization meets and maintains the specified standards. In the health sector, for example, accreditation is an independent external review process that assesses the quality of healthcare services in order to encourage better performance and assure the public of the quality of the services provided by the organizations [Lichiello & Turnock, 2002]. Accreditation standards are traditionally set at what are considered to be the minimum achievable and allowed levels. Accreditation is traditionally practiced to assess the *quality and cost of business processes and their related products/services*.

(b) *Financial rating:* Financial rating (credit rate) is a published ranking that is based on a detailed financial analysis. As a rule, credit bureaus perform the financial analysis, which is based in general on the financial history of an organization and in particular on its ability to meet payment obligations. VBE member organizations must validate their financial record and have it approved by authorized organizations that are legalized to

perform the financial related analysis. Approval is thus sought for aspects including *credit score, solvency, profitability ratios, bankruptcy prediction, etc.*

(c) *Patent:* A patent is a set of exclusive rights granted by an authorized party to an organization for a fixed period of time in exchange for the regulated or public disclosure of a certain device, method, or process which is new, inventive, and industrially applicable. Patents granted to organizations could be used as evidence of performance data.

(d) *License:* License is an official or legal permission to do or own a specific item. A license can be a document, plate, or tag that is issued as proof of official or legal permission to own something or carry out an activity (e.g. a business license). The issue of a license with intellectual property rights, such as a copyright or trademark is a proof of permission to use, reproduce, or create an instance of the licensed work. Therefore, licenses can also be used to attest the information provided by an organization.

(e) *Certificate and awards:* A certificate is an official document that proves the accomplishment of a certain achievement. For example, a business registration certificate warrants the formal existence of an organization. In computing and in particular computer security and cryptography, the word certificate generally refers to a digital identity certificate, also known as a public key certificate. An award is something given to a person or organization to recognize excellence in a certain field. Such proof can also be used as a means to validate the information provided by an organization.

ii) **Witnessed evidence**

This type of evidence constitutes a certain form of documentation that is generated by third parties and that is subjective by nature. So although this type of evidence provides some proof of accuracy it can be argued that the degree of validity is less than certified evidence. Such witnessed evidence may include information obtained from: (1) Public channels, (e.g. magazines, newspapers) and (2) Private channels, (e.g. recommendations).

Although these types of evidence are not as strong as certified evidence, when certified evidence is lacking they can provide some degree of validity of the provided information. Clearly, the validity level increases if the channels used (the news sources or the person providing the recommendation) are publicly recognized. For example, reputable news media put extra effort into discovering the truth about the story they report, although their report can only focus on certain aspects of the story and they do not guarantee the provision of comprehensive coverage. Similarly, a letter of recommendation from party A about party B only shows a limited number of party B's qualifications as party A only knows party B to a certain extent.

2.5 Characterization of trust relationships among organizations in VBEs

One important strategy that is necessary for VBEs is to focus on organizational preparedness to enhance their chances of participating in VOs. Organizational strategies must therefore properly address the notion of collaboration with other business partners. As addressed in Chapter 1, in addition to acquiring resources, knowledge and competencies, a crucial aspect of the preparation process involves establishing trust relationships with potential business partners in order to smoothen possible collaboration. There are two kinds of trust relationships between organizations that can be established in VBEs, namely:

- *Short-term trust relationships:* established to facilitate co-working between organizations that will exist for a relatively short period of time, e.g. collaborations in VOs.
- *Long-term trust relationships*: established to facilitate co-working between organizations that will exist for a relatively long period of time, e.g. cooperation in VBEs.

Consideration of a large number of specific fundamental aspects is necessary when addressing trust between organizations in VBEs. As described in Chapters 3, 4, 5, and 6, inter-organizational trust is characterized as a multi-objective, multi-perspective, and multi-criteria subject. It is a challenging task to comprehensively cover all these specific fundamental aspects of inter-organizational trust and thus use them to facilitate the establishment of trust relationships between organizations. A single specialized approach, such as based on reputation of organizations, security of systems, etc., cannot adequately cover all fundamental aspects of trust that need to be considered while establishing trust relationships between organizations in VBEs. Accordingly, a generic but comprehensive and structured approach must be designed that will support the realization of inter-organizational trust relationships in VBEs.

A number of specific steps must be taken into account in order to characterize the planned relationships and prepare the involved organizations on a number of essential aspects in establishing their goal-oriented trust relationships. In order to effectively establish trust relationships between organizations in VBEs applicable to different domains, we propose the following four steps, each addressed further in next chapters. The first three steps focus on guiding involved organizations to prepare themselves in relation to trusting one another for the purpose of facilitating the intended collaboration. The following are the four proposed steps:

Step 1: Assessment of level of trust in organizations as further addressed in Chapter 5 and Chapter 6,

Step 2: Validation of trust level results based on the analysis of evidence of validity of the trust related data for organizations as further addressed in Section 2.4,

Step 3: Presentation of levels of trust in organizations and related trust concepts as easy and understandable as possible to involved organizations as further addressed in Chapters 3, 4, 5 and 6.

Step 4: Creation of trust between organizations to support the launching of the intended trust relationships by providing sufficient information based on a number of trust aspects as addressed in Section 2.4, and Chapters 3 and 6.

2.6 Chapter discussion and conclusion

This chapter has presented a survey on existing practices and reported research results on trust. It has surveyed inter-personal trust and has used results as a means of comparison with the basic concepts of inter-organizational trust. In addition, it has presented perceptions of trust experienced and applied in different disciplines and domains.

The chapter has also introduced the characterization of inter-organizational trust in VBEs and it has presented fundamental concepts which either complement (such as security, reputation, etc.) or contradict (e.g. risks, privacy, etc.) inter-organizational trust. It also introduces primary aspects of organizational trustworthiness, namely those of a technological, structural, economical, social, and managerial nature. The chapter ends by presenting the characterization of trust related data and inter-organizational trust relationships in VBEs.

A key contribution of this chapter in this thesis is the characterization of the main challenges related to trust studies, namely: (i) the causality relations between trust and a wide variety of related aspects (see further details addressed in Chapters 3 and 5), (ii) the need to enhance transparency and fairness in relation to the analysis of inter-organizational trust and measurement of performance of organizations which in turn provides fundamental input data to the evaluation of trustworthiness of the organization (see further details in Section 3.3.3), and (iii) characterization of a large set of trust elements that must be considered in building models and mechanisms for assessing the level of trust in organizations (see Sections 2.3.5 and 2.3.6, and Chapters 3, 4 and 5).

The next chapter (Chapter 3) further extends the concepts presented in Section 2.3.6 by presenting an approach which is applied for identifying and characterizing trust elements for organizations.