IT Risk Management: A Capability Maturity Model Perspective

Marian Carcary
Innovation Value Institute, National University of Ireland Maynooth, Maynooth, Co Kildare, Ireland
marian.carcary@nuim.ie

Abstract: Understanding the value derived from IT investments and IT enabled operational improvements is difficult, and has been a subject of research and debate among ICT practitioners and academics for many years. This is particularly so because innovative technological developments have supported transformative changes in organizational operational activities. Research continues to investigate approaches to not only understanding the value derived by IT but also to optimizing this value. One of the key aspects of optimizing IT-driven value is the requirement to effectively manage risk. The continual evolution of the IT risk landscape requires effective Risk Management (RM) practices for all IT risk areas, such as, but not limited to security, investments, service contracts, data protection and information privacy. Effectively managing these risk areas pose specific concerns from the perspective of Chief Information Officers (CIOs) and Chief Risk Officers (CROs). Hence, significant considerations should be given to not only the processes involved in assessing, prioritizing, handling and monitoring these risks but also to ensuring the development of an appropriate risk culture and the establishment of effective RM governance structures, to support effective RM.

This paper examines the maturity model/framework approach to improving an organization's IT capabilities, with specific reference to effectively managing IT-related risks, and increasing value derived over time. A new IT Risk Management maturity model is presented; this framework is part of the IT Capability Maturity Framework (IT CMF) which supports value-driven IT management practices. It was developed by the Innovation Value Institute at the National University of Ireland Maynooth, following a design science and open innovation research approach. The IT CMF, consisting of 33 Critical Capabilities, focuses on maturing key activities of the IT organization. The Risk Management Critical Capability presented in this paper enables organizations to determine their IT RM maturity and identify key recommendations in specific areas to improve maturity overtime. Thereafter the paper presents an analysis of the maturity model approach to managing risk, to improving an organization's IT capabilities, and to deriving enterprise-wide value from more mature IT practices.

Keywords: IT risks, IT risk management, maturity model, IT CMF, critical capability, RM practices, outcomes and metrics

1. Introduction

Risk is a function of the likelihood of a particular threat source exploiting an organization's vulnerability, and the impact of the adverse event on the organization (Elky, 2006). However, for many organizations the various IT risks are often under assessed (Benaroch et al, 2006; Glass, 2006). As technology continues to drive industry transformation, traditional business models are gradually being replaced by technology-enabled models (Ernst and Young, 2011), and while this may support improved operational efficiency, it also exposes an organization to increased risk likelihood and impact levels. Today, with the proliferation of mobile computing, social networking, and cloud based services, organizations face increased risk of data leakage, asset theft and reputational damage. In fact, IT risks stories are common in the recent literature. Reports of the TK Maxx security breach resulting in theft of over 45 million customer card numbers (Gaudin, 2007); Estonia's denial of service attacks, affecting government, banking and school websites (Kirk, 2007); and the recent high-profile wiki-leaks publishing global intelligence files are just a few examples.

Therefore, the ability to effectively manage the various IT risks is an important factor in organizations deriving and optimizing the value associated with their IT investments. Effective practices should consider all key IT risk areas to enable CIOs and CROs to prioritize their resources in addressing the most significant risks. This paper presents a new maturity modeling approach to identifying and developing an organization's risk management capabilities. The maturity model in Information Systems (IS) research continues to grow in popularity, and while concerns exist regarding the development process and foundations upon which some models are developed, the RM capability maturity model presented in this paper was built upon existing theories and methodologies, followed a rigorous development process based on a design science approach, and was externally validated in a number of pilot organizations.

Reference this paper as: Marian Carcary, "IT Risk Management: A Capability Maturity Model" The *Electronic Journal Information Systems Evaluation* Volume 16 Issue 1 2013, (3-13) , available online at www.ejise.com

The structure of the paper is as follows: Section 2 presents an overview of the IT risk landscape and existing approaches to RM. Section 3 introduces the concepts of maturity models in IS research and highlights the concerns that exist regarding the approach. Section 4 provides an overview of a new IT management maturity model, the IT Capability Maturity Framework (IT CMF), and an outline of how the concerns associated with maturity models were addressed in its development. It further discusses the model's RM critical capability for assessing and improving RM maturity overtime. Section 5 concludes the paper with a discussion of the value of the maturity modeling approach for optimizing IT capabilities, and specifically RM capabilities

2. Managing IT risks

Investing in IT exposes an organisation to several risk factors, including for example project, organizational and technical risks (see for example Amberg and Okujava, 2005; Brown, 2005). Undoubtedly, one of the biggest concerns from an organizations perspective is security, in terms of protecting the organizations business critical applications and confidential/sensitive data. The Frost and Sullivan (2011) study, which was conducted for the International Information Systems Security Certifications Consortium (ISC^2), reported that key risks from an organizations security perspective include application vulnerabilities, mobile devices, viruses and worm attacks, internal employees, hackers, contractors, cyber terrorism, cloud-based services and organized crime. The study further reported that the key new and emerging risks facing organizations today include mobile devices and mobility, cloud computing and social media.

Advancements from PDAs to multi-functional and ubiquitous smartphones and tablets have resulted in a proliferation of mobile devices. However, ability to access business applications, corporate sensitive data and confidential personal data “anytime, anywhere” poses risks regarding data leaks or loss/theft of mobile devices. For example, smartphones were growing at the rate of 21% in North America, and tablets and e-readers were expected to reach sales levels of 22 million units in North America by 2016. This concept of the “borderless environment” poses specific concerns from a data security and control perspective (Frost and Sullivan, 2011; Ernst and Young, 2011).

Cloud computing, regarded as an enabler of scalable, flexible and powerful computing, poses specific concerns in terms of confidential information exposure to unauthorized sources; loss or leakage of confidential data; weak systems or application controls; susceptibility to cyber-attacks; disruptions in the continuous operations of the data centre; and inability to support compliance audits, among others (Frost and Sullivan, 2011). Similar cloud based challenges and a number of additional ones were highlighted in Ernst and Young's (2011) Global Information Security survey and include legal compliance and privacy; information security and data integrity; contractual and legal risks; governance and risk management assurance; reliability and continuity of operations; and integration and interoperability. From the Information System's Audit and Control Association's (ISACA) (2010) survey, 45% of US IT professionals believed that the risks of cloud adoption outweighed any associated benefits; only 10% surveyed would consider migrating mission critical applications to the cloud. However, 61% of Ernst and Young's (2011) respondents were currently using, evaluating or planning adoption of cloud computing-based services.

Further, the growth in use of social media tools means that social media applications are now being used, not just for personal uses but also business purposes, in connecting with customers, tracking customer comments about their products and services, developing brand loyalty etc. Approximately 15% of the world's population are registered users of popular social and business networking sites. For example, Facebook had 687.1 million users in June, 2011, while LinkedIn had 79.2 million unique visitors worldwide in March 2011. IT risks associated with their use for business purposes include exposure to malicious software within social networks; hacked accounts; and exposure of confidential data or sensitive company information (Ernst and Young, 2011).

The above key emerging technological trends pose a significant concern regarding IT-security related risks. This is supported by a recent IBM commissioned survey by Forrester, who interviewed over 2000 industry experts across Europe and America. 72% of the respondents reported that security threats were escalating and constituted a major concern. This increase in threats has led to severe shortages in trained security staff. According to the 2010 Centre for Strategic & International Studies (CSIS) report called “A Human Capital Crisis in Cybersecurity” there is a need for 30,000 cybersecurity specialists in the US alone, with only 1000 positions currently filled.

News reports also provide us with some evidence of the impacts from poor Information Security. Information Security has three primary tenets: Confidentiality, Integrity and Availability of information must be preserved. Recently, the Ulster Bank has had to pay compensation to many of its customers following a failure in their systems in June 2012 (King, 2012). In this case, availability was violated, with many customers unable to access their accounts. Another prime example is the SONY password leak, which impacted 100 million customers (Goodin, 2011) - here the confidentiality tenet was violated. Once someone gains access to information, it is relatively easy to compromise its integrity – this was evidenced by Hershey when hackers breached their site and changed one of their recipes (Goodin, 2011b). This is a relatively minor change but the potential is there for far more serious changes to be made. For example, in July 2012, it was reported that a mother hacked into her son's school system and changed his grades (Grossmann, 2012). Imagine if someone could hack into a University's systems to create a fictitious degree for themselves – the possibilities are endless for the integrity of critical data to be compromised.

However, IT risks span a broader spectrum than security, and include a wide range of risks that may affect or result from IT operations, for example risks associated with compliance with regulatory changes; compliance with ethics policies; IT investments; IT project lifecycles; service continuity due to security breaches, system failure or natural disasters; internal process changes impacting on product or service quality; supplier contracts; and reputation. Hence, an effective approach to managing these and other IT risks is required to enable organizations to reduce their exposure and their potential impact on the organization's operations and in essence to protect the organization's assets and mission (Elky, 2006). Some of the various IT risks may be intractable, in that they resist mitigating actions, or unforeseen/ not apparent at the time of project planning (Taylor, 2006). Hence, a proactive approach to identifying and scoring IT risks including new and emerging risks, to prioritizing identified risks according to determined risk likelihood and impact scores, to identifying and implementing appropriate risk handling strategies, and to monitoring effectiveness of the implemented risk controls overtime is required.

Management of risk is well discussed in the literature (for example Casey, 2007; Da Veiga and Eloff, 2007; Rosenquist, 2007; Westerman and Hunter, 2007), and several IT management frameworks address the issue of RM in varying degrees of depth (for example, CMMI, Management of Risk (MoR), ISO 27001, ISO 27002, IT Risk Framework, Open Group's Information Security Management Maturity Model (O-ISM3), and COBIT). "*Risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions*" (Stoneburner et al, 2002). Ability to understand IT risks on the horizon and the likelihood and magnitude of these risks enables stakeholders to prioritize scare resources and take steps to protect the IT assets proportionate to their value to the organization. A systematic approach should be established to estimating the magnitude of risk based upon which risks should be prioritized for risk treatment. According to Sumner (2009), a risk preparedness strategy should be developed for high-impact, high-probability risks. An inventory of risks, their attributes and current control activities should be established and maintained. Such control activities or risk handling strategies are defined to support reduction of risk to an acceptable level, and may be outlined in a detailed information security risk treatment plan. Such treatment approaches may include risk acceptance, avoidance, transference and mitigation. Residual risks, acceptable risk levels, and RM processes goals and metrics should be monitored over time taking into account changes in the internal and external environment, and deviations or problems identified, tracked and reported (e.g. National Institute of Standards and Technology methodology, OCTAVE, COBRA etc.); this closes the loop on RM processes, enabling continual monitoring of the effectiveness of RM approaches (Elky, 2006). However, effective RM approaches alone is not sufficient. Management and stakeholder support and buy-in, development and enforcement of policies that deal with new and emerging risks, and development of a risk culture that involves training and communication of RM activities are also essential (Da Veiga and Eloff, 2007). Further, IT RM should not exist in a silo; many authors highlight the importance of integrating IT RM approaches into the overall Enterprise Risk Management (ERM) framework - an approach that involves holistically managing the enterprises entire risk portfolio (Fraser and Simkins, 2010; Kouns and Minoli, 2010). As RM seeks to protect the organizations assets and mission, it needs to be regarded as a management function as opposed to merely a technical activity (Elky, 2006). Integrating IT risk with ERM practices promotes a greater understanding by IT of the business priorities and protection of critical business services, and enables more effective risk mitigation, avoidance of risk oversights and better return on IT investments (Silicon Republic, 2010).

The following sections of this paper considers the maturity modeling approach to improving risk management capabilities, by enabling organizations to understand their current RM capabilities and identify practices to improve their capability maturity overtime. The maturity modeling approach has been well adopted in IS research. Section 3 provides a brief overview of maturity models prior to introducing a new capability maturity framework that addresses organizations RM capability maturity.

3. Maturity models in IS research

There are several IT risk management approaches, models and frameworks reported in the literature, an examination of which reveals some evolution in thought processes regarding the most effective risk management methods. In 2002, Siponen used the term "software maturity criteria", suggesting that maturity standards represented the way forward in terms of managing information security in organisations. Maturity models are "conceptual models that outline anticipated, typical, logical and desired evolution paths towards maturity" (Becker et al, 2010), where maturity is "a measure to evaluate the capabilities of an organization in regards to a certain discipline" (Rosemann and de Bruin, 2005). Maturity can also be regarded as "an evolutionary progress in the demonstration of a specific ability or in the accomplishment of a target from an initial to a desired or normally occurring end stage" (Mettler, 2009). Maturity models outline characteristics associated with various levels of maturity, thereby serving as the basis for an organization's capability maturity assessment. In essence, they serve to help organizations to understand their "as is" situation and enable them to transition to the desired "to be" maturity, through deriving and implementing specific practices or improvement roadmaps. These improvement maps support a stepped progression with respect to organizations capabilities, enabling them to fulfill the characteristics required to meet specific maturity levels.

A recent literature review of maturity models in IS research has highlighted a growing interest in this area (Becker et al, 2010; Mettler, 2009), in order to inform organizational continuous improvements and support either self or third party maturity assessments. While the Software Engineering Institute's (SEI) Capability Maturity Model (CMM) for software development and the successor Capability Maturity Model Integration (CMMI) are most prevalent in studies of maturity (Becker et al, 2010), nonetheless, several new maturity models have been developed in recent years. These focus on improving maturity in, for example, IT/business alignment (Luftman, 2003; Khaiata and Zualkernan, 2009); business process management (Rosemann and de Bruin, 2005); business intelligence (Hewlett Packard, 2007); project management (Crawford, 2006); information lifecycle management (Sun, 2005); digital government (Gottschalk, 2009); inter-organizational systems adoption (Ali et al, 2011) and enterprise resource planning systems use (Holland and Light, 2001).

Despite the growing interest in this area, according to Becker et al (2010), IS research has "rarely endeavored into reflecting and developing theoretically sound maturity models" and as such there is a lack of evidence of scientifically rigorous methods in their development processes, with some models based on poor theoretical foundations (Mettler, 2009). Methods, such as Design Science (DS) (Hevner et al, 2004) are proposed as a useful means to develop new maturity models in a rigorous manner, using both prior studies and empirical evidence as the basis for the model's content development and stages of maturity. Further, Becker et al (2010) suggests that there is a lack of evidence of validity testing of newly developed models; however to ensure their relevance for practitioners, the proposed models need to be piloted and "applicability checks" conducted with practitioners. Closing the gap between current and desired maturity is also problematic, with Mettler (2009) suggesting that many models do not describe how to carry out improvements actions.

In line with the categorization of maturity models adopted by Becker et al (2010) (prescriptive, descriptive, descriptive/prescriptive, descriptive/reflective, and reflective), this paper reflects a prescriptive contribution (i.e. a specification of how capability improvements could take place) through the presentation of a new maturity model. The model presented addresses the concerns outlined above through following a rigorous development process based on design science and open innovation principles; empirical piloting, testing and validation of the model; and development of a series of improvement practices, outcomes and metrics to drive maturity level progression.

4. Presenting a new maturity model - the IT capability maturity framework (IT CMF)

The IT CMF (Figure 1) is a capability maturity model developed at the Innovation Value Institute (IVI), National University of Ireland Maynooth. It represents a systematic framework to enable CIO's/CEO's to understand and improve their organization's maturity in order to derive business value from IT investments (Curley, 2004; 2007). The framework represents an emerging blueprint of IT capabilities and serves as an assessment tool which enables organizations to understand and improve over time their IT capability across five levels of maturity – initial, basic, intermediate, advanced and optimizing Table 1). The meta-elements of the IT-CMF can be depicted in three interlinked layers, namely strategy, macro and micro layers.

[1] The strategy layer underpins the primary elements of the IT-CMF that support an approach to strategic thinking comprising business context driven by the organisation's vision of its future; business strategy; IT capability; business operations; and, business value (Curley, 2004).
[2] The Macro layer consists of both the content and context of application of the IT-CMF. The content segments the activities of an organisation's IT function into four macro-capabilities (MCs) namely: Managing IT like a business, Managing the IT budget, Managing the IT capability and Managing IT for business value. These four integrated IT management strategies underpin value oriented IT management.
[3] The Micro-layer comprises 33 critical capabilities (CCs) assigned to the four individual macro capabilities. These represent key activities of the IT organisation in delivering IT solutions and optimising the associated business value generated. Each CC encompasses a number of categories and capability building blocks (CBBs), which reflect the CCs content and assumptions associated with each of the five maturity levels (Curley 2004). Understanding an organisation's current and desired maturity levels helps set improvement initiatives that drive value delivery. Improving maturity across these CCs reflects organisational progress over time.

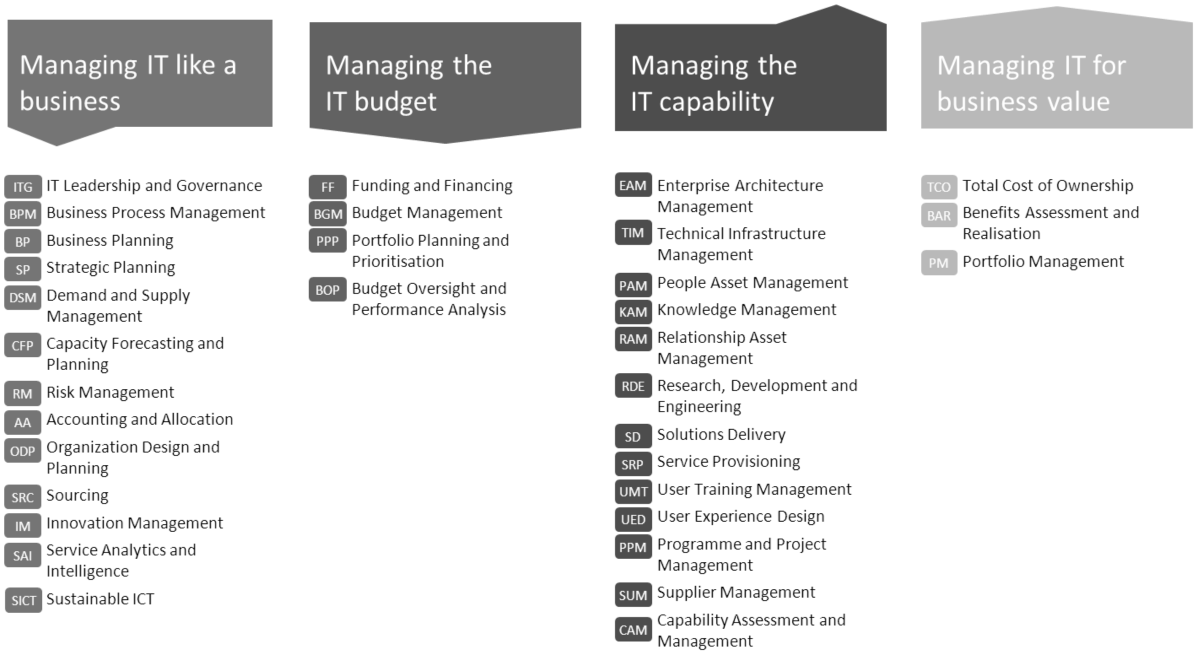
Managing IT like a business
ITG IT Leadership and Governance
BPM Business Process Management
BP Business Planning
SP Strategic Planning
DSM Demand and Supply Management
CFP Capacity Forecasting and Planning
RM Risk Management
AA Accounting and Allocation
ODP Organization Design and Planning
SRC Sourcing
IM Innovation Management
SAI Service Analytics and Intelligence
SICT Sustainable ICT
Managing the IT budget
FF Funding and Financing
BGM Budget Management
PPP Portfolio Planning and Prioritisation
BOP Budget Oversight and Performance Analysis
Managing the IT capability
EAM Enterprise Architecture Management
TIM Technical Infrastructure Management
PAM People Asset Management
KAM Knowledge Management
RAM Relationship Asset Management
RDE Research, Development and Engineering
SD Solutions Delivery
SRP Service Provisioning
UMT User Training Management
UED User Experience Design
PPM Programme and Project Management
SUM Supplier Management
CAM Capability Assessment and Management
Managing IT for business value
TCO Total Cost of Ownership
BAR Benefits Assessment and Realisation
PM Portfolio Management

Figure 1: IT CMF (source: Innovation Value Institute)

Maturity Level	Maturity Level Details
5- Optimising	• Value centric IT management • State of the art practices and outcomes
4- Advanced	• Benefits from IT investments quantified and communicated • Practices and outcomes well above industry average
3- Intermediate	• IT/business interaction formalised for all critical capabilities • Transparent investment decisions
2- Basic	• Delivering basic IT services • Some IT/business interactions formalised
1- Initial	• No formal processes • Ad hoc management of IT

Table 1: IT CMF generic maturity levels (source: Innovation Value Institute)

Content development for the IT CMF is undertaken by the IVI consortium. The consortium is made up of over 80 industry partners linked to IVI through a common desire to develop and enhance their organization's understanding of improved business value through IT capability management. The consortium members are invited and encouraged to participate in the research and development activities of the IVI through workgroup contribution. A work group exists for each of the 33 CCs, which include a mix of Subject Matters Experts (SMEs) and Key Opinion Leaders (KOLs), including academic researchers, industry-based practitioners, and consultants. Work group development output evolves through a series of four stages and is reviewed at the end of each stage by a technical committee (TC). As development work progresses through the various stages, more in-depth content is required and the CC material is subject to more rigorous reviews and validation processes.

This content development across the four stages follows the Design Science (DS) research approach. This approach is increasingly recognised within IS as an important complement to the prevalent behavioral science. Behavioural science often involves the development of a hypothesis, which is either proved or disproved with the collection and analysis of data by the researcher. Resulting theories provide insights pertaining to the interactions among people, organisations and technology that need to be managed. While this research paradigm is appropriate for studying existing and emerging organisational phenomena, there is a danger of over emphasising contextual theories at the expense of failing to anticipate new technological capabilities. This may result in behavioural science theories referring to out-dated or ineffective technologies. Further, the behavioural science paradigm is not sufficient for addressing the types of problems that call for human creativity and innovative and novel solutions (Hevner and Chatterjee, 2010; Peffers et al, 2007), for example, "What IT artifacts will increase firm value?" (March and Storey, 2008). In other words *"science, the process of understanding "what is," may be insufficient for design, the process of understanding "what can be.""* (Hevner and Chatterjee, 2010). These types of problems that require innovative solutions are regarded by Pries-Heje and Baskerville (2008), as ill-structured or "*wicked problems*", where requirements may be unstable, there may be complex interactions between problem subcomponents, and human cognitive and social abilities may be important in developing solutions (Hevner et al, 2004). Addressing these types of problems is the remit of DS research (March and Smith, 1995; March and Storey, 2008) and many such problems exist in the IS field.

While the behavioural science paradigm seeks to identify what is "true", the DS paradigm aims to create what is effective. DS is a problem solving approach that involves building and evaluating innovative artifacts in a rigorous manner to solve complex, real world, relevant problems, make research contributions that extend the boundaries of what is already known, and communicate the results to appropriate audiences (Gregor and Jones, 2007; Hevner et al, 2004; March and Smith, 1995; March and Storey, 2008; Pries-Heje and Baskerville, 2008; Purao, 2002; Venable, 2006). Knowledge and understanding of the problem domain is achieved through artifact construction and evaluation (Hevner et al, 2004). Knowledge and understanding of the problem domain is achieved through artifact construction (Hevner et al, 2004), which must have novelty and utility in the application environment (Hevner and Chatterjee, 2010; March and Storey, 2008; Simon, 1996).

Analysis of the utility and performance of the developed artifacts provide improved understanding and identification of further improvements that enable the business problem/need to be addressed more effectively. According to Peffer et al (2007) the "*design and the proof of its usefulness is the central component*". The DS approach adopted in the IT CMF development (Table 2) is closely aligned with the three DS research cycles proposed by Hevner (2007). (For a detailed discussion of its development, see Carcary (2011)).

Table 2: DS Cycles of the IT CMF development

DS Cycle	IT CMF
DS Relevance Cycle	Relevance of the IT CMF artifact is driven by the problems organizations experience in optimizing how they currently manage and measure the business value of their IT investments. Field testing of the IT CMF in the application environment helps determine if further development work is required to ensure its relevance in addressing the business problem.
DS Rigor Cycle	Development is grounded in existing artifacts, methodologies, foundational theories and expertise and draws from an extensive base of industry and academic literature and existing IT standards and frameworks. Contributions to the knowledge base include a detailed framework and set of practices that help drive innovation and change in how organizations manage and use their IT investments to optimize business value.
DS Design Cycle	Development focuses on iterative build and evaluate activities by the CC workgroup to address the identified problem, while drawing on existing theoretical foundations and methodologies in the knowledge base. The build process is evolved and refined through evaluation feedback, including technical committee stage gate reviews to identify further development refinements and field testing of the artifact within contextually diverse organizations.

4.1 An examination of the risk management critical capability

Located within the IT-CMF's "Managing IT like a business" macro capability, the Risk Management CC focuses on proactively assessing, prioritizing, handling and monitoring risks in order to minimize exposure to and the potential impact of IT risk. This CC aims to be holistic in addressing the key categories of IT risk facing organizations, including for example IT security; data protection and information privacy; operations/ business continuity and disaster recovery; IT investment; IT programme, project and product life cycles; IT service contracts and suppliers; IT image/ brand; IT personnel; regulatory/ legal and ethics policy compliance, as well as emerging risks in these and other categories. The assessment provides key insights into an organizations maturity with respect to three key areas - governance, risk profile design and the actual risk management processes. These three categories are comprised of ten capability building blocks (CBBs), as outlined in Table 3.

Table 3: Capability building blocks of the RM CC

Governance	Profiling and Coverage	Process
Policies for Risk Management	Definition of risk profiles	Risk assessment
Integration into IT leadership and governance structures	Risk Coverage	Risk prioritization
Management, governance and performance management		Risk handling
Communications and training		Risk monitoring

The above ten CBBs are the focus areas of a RM assessment, with dedicated maturity questions developed within each of these areas. Examples of RM maturity assessment question topics are outlined in Table 4.

Table 4: Example RM maturity assessment question topics

Key areas of the IT CMF RM Maturity Assessment
Definition and implementation of risk policies; Establishing risk policies ownership and responsibilities; Integrating RM into IT leadership and governance structures; Identifying RM roles and responsibilities; Identifying levels of senior management support; Measuring the effectiveness and efficiency of RM activities; Training stakeholders in RM; Disseminating RM policies, processes and results;

Determining collaboration levels between risks managers;
Defining risk profiles by their potential impact;
Using risk profiles in risk assessment and mitigation;
Identifying subject matter experts for risk assessments;
Identifying and scoring risks and their impact;
Prioritizing risks and risk handling strategies;
Identifying tools to support risk handling;
Assigning ownership to identified risks;
Defining and implementing appropriate risk controls;
Monitoring and reporting identified risks and the effectiveness of risk controls.

Assessment questions in these and other areas describe maturity level statements that follow IT CMF prescribed maturity level logic, across five stages – initial, basic, intermediate, advanced and optimized. Maturity assessment participants are invited to score the organization's maturity across these five levels, as well as identify the future desired state. Aggregated scores support reporting of the organization's self-assessed current and desired maturity levels; in addition an IVI assessment, based on both the survey assessment results and in-depth interviews with key RM stakeholders result in a formal IVI maturity assessment score and presentation of a set of practices to support the organization transitioning to higher maturity levels. A detailed set of IVI RM Practices, Outcomes, and Metrics (POMs) at the various maturity stages support closing the gap between organizations' current and desired maturity states. Example practices, outcomes and metrics related to the RM policy CBB are outlined in Table 5:

Table 5: Example POMs pertaining to Risk Policies

Maturity Level	Practice	Outcome	Metric
5	Develop the RM policy with the extended enterprise and ensure continuous refinement and update of the policy using a well-defined and implemented process	The RM policy is derived in cooperation with the extended enterprise. The policy reviews include optimization of enterprise-wide RM effectiveness and efficiency.	Ratio of actual RM policy reviews to required reviews (set out in the policy)
4	Develop the RM policy via a process of enterprise-wide cooperation and review the policy regularly. Benchmark the RM policy against industry best known practice	The RM policy is derived via enterprise-wide cooperation of RM functions and kept up-to-date. Benchmarking ensures improved validity and completeness of the RM policy	Ratio of actual RM policy reviews to required reviews (set out in the policy) Ratio of actual RM policy benchmarks to planned benchmarks (set out in the policy)
3	Implement a detailed RM policy within IT and within some business functions. Formalize a process and schedule for policy review. Review and refine the RM policy/ procedures, the business continuity plan and the alignment with corporate strategy	A consistent and holistic RM policy is in place covering for example assets, processes, people, key emerging risks, risk avoidance, mitigation etc. A process is in place to proactively update policies and keep them up-to-date.	% of IT staff/management staff/general staff who have signed the RM policy Ratio of actual RM policy reviews to required reviews (set out in the policy)
2	Develop an initial Risk Management policy and execute reviews of it as needed	An RM policy is derived from reviews of risk relevant systems by the IT organization. It is reviewed but only reactively to major events; there is an increasing risk of inconsistency as not all changes are reflected in the policy	Existence of a RM policy Ratio of actual RM policy reviews to required reviews (set out in the policy)
1	No formal practices are expected at this level	An inconsistent approach to risk management is adopted. An RM policy is not formalized and is only defined ad hoc, usually after incidents	No metric

As such, the RM maturity assessment represents the basis for organizations understanding their key strengths and weaknesses in their ability to mitigate potential IT risks. The output from the IT CMF RM assessment enables an organization to put action plans in place to mature their capability in effectively managing IT risks on the horizon. In general, transitioning to higher maturity levels requires for example, an organization to align and integrate business objectives with RM practices; define and implement effective processes for risk assessment, prioritization, handling and mitigation for all risk areas, including new and emerging risks, and integrate them into enterprise RM processes; create an effective and integrated risk register; obtain support from senior management; ensure long-term training and retention of skills; and embed RM into IT and business activities. Adopting these and other practices in order to mature RM capabilities and proactively manage risks becomes an important step in deriving business value from IT investments. In addition, the RM capability framework also provides insights into the actions and mindsets that can typically prevent an organisation in maturing their RM capability. These include for example a lack of a holistic view of RM, where the focus is on reactive approaches to "survive", where there is a lack of cohesion to overall business objectives, and a failure to integrate IT risk management in enterprise RM approaches; a lack of senior management support, funding and resources, where RM is regarded as a low priority activity; a lack of clarity on the organization's overall risk tolerance; and a lack of RM training/ knowledge throughout the organization and failure to define required skill sets. A particular barrier is the assumption that IT RM is a non-value add to the business.

The following section provides an analysis of the value of this maturity model and the maturity model approach in supporting the transition to higher maturity levels and more effective IT capabilities.

5. Discussion and conclusions

Growth in the development and use of maturity models provides strong support for the relevance of the maturity assessment approach in practice. As stated by Mettler (2009), "*as organizations constantly face the pressures to obtain and retain competitive advantage, invent and reinvent new products and services, reduce cost and time to market, and enhance quality at the same time, the need for and the development of new maturity models will certainly not diminish given that they assist decision makers to balance these sometimes divergent objectives on a more or less comprehensive manner*". Based on the literature, the greatest concern regarding this assessment approach is the processes involved in maturity model development – rather than building on a theoretical basis, many models are simply based on practices drawn from organization or industry specific projects that demonstrated favourable results, for many models there is a lack of model testing in terms of validity, reliability and generalizability, and little documentation on how the model was designed and developed (Mettler, 2009).

Based on the above, it can be suggested that given the relevance of maturity models to organizations in informing and supporting prioritized stepped improvements in capabilities, a maturity model that addresses the concerns in the literature pertaining to their theoretical foundations and rigorous development and testing approaches should be a useful contribution. The framework for IT management outlined in this paper, and more specifically for maturing the RM capability, therefore should reflect an important contribution from the perspective of organizations seeking to optimize their RM capabilities and the value they derive from IT. Through adopting the maturity modelling approach to RM and improving maturity overtime, it is proposed that CEOs and CIOs can improve the organization's ability to manage risks and protect the business from risk impacts; they can reduce the organization's exposure to risks such as IT security, IT sabotage, data protection and information privacy, and IT investment risks; they can increase the likelihood of meeting the scope, cost, time and quality targets of projects by effectively managing associated IT risks; they can increase the likelihood of compliance with external regulations and ethics policies; and they can increase transparency of how IT risks map/ relate to business objectives and decisions. In essence, organizations with a mature RM capability are more effective in proactively managing IT risks, and in reducing the exposure to and the potential impact of IT risks. The RM capability framework presented here does not exist in a silo – its interdependencies with all other IT critical capabilities are recognised, and therefore offers an opportunity to support integrated, cohesive development of the overall IT capability over time.

As outlined above, the presentation of the IT-CMF's risk management critical capability is a prescriptive contribution; further research is needed to investigate the extent to which this maturity model supports capability maturity progression in a real world setting over time. While some companies are expected to be assessed between Maturity Level two and Maturity Level three; it is recognised that across some industries/regions etc, that minimum RM requirements are defined by law and regulation. As such, future research will involve conducting multiple assessments to determine the average IT RM maturity level across different industries and organization sizes; and to determine the impact of regulatory requirements on the maturity level uncovered. Further a series of multiple cases studies on a longitudinal basis will be carried out to determine the real-world value of this approach in improving organizations capabilities in managing existing, and new and emerging risks.

References

Ali, M., Kurnia, S., Johnston, R. (2011). Understanding the Progressive Nature of Inter-Organizational Systems (IOS) Adoption. *E-Collaboration Technologies and Organizational Performance: Current and Future Trends*, Ed. 1, pp. 124-144.

Amberg, M. and Okujava, S. (2005). State of the art of IT project value analysis. In (Ed. D. Remenyi), *Proceedings of the 12th European Conference on Information Technology Evaluation*, pp. 21-34. Turku, Finland, 29th-30th September, Academic Conferences, Reading.

Becker, J., Niehaves, B., Poppelbus, J., and Simons, A. (2010). Maturity Models in IS Research. *Proceedings of the 18th European Conference in Information System*, pp 1-12. Available at: http://web.up.ac.za/ecis/ECIS2010PR/ECIS2010/Content/Papers/0320.pdf

Benaroch, M., Lichtenstein, Y. and Robinson, K. (2006). Real options in Information Technology risk management: an empirical validation of real-option relationships. *MIS Quarterly*, **30**,(4), 827-864.

Brown, A. (2005). IS evaluation in practice. In (Ed. D. Remenyi), *Proceedings of the 12th European Conference on Information Technology Evaluation*, pp. 109-118. Turku, Finland, 29th-30th September, Academic Conferences, Reading.

Carcary, M. (2011) "Design Science Research: The Case of the IT Capability Maturity Framework (IT CMF)" *Electronic Journal of Business Research Methods*, 9,(2), p109-118.

Casey, T. (2007). *Threat Agent Library Helps Identify Information Security Risks*, Intel White Paper

Centre for Strategic and International Studies (2010). A Human Capital Crisis in Cyber Security. Available at: http://csis.org/files/publication/100720_Lewis_HumanCapital_WEB_BlkWhteVersion.pdf

Curley, M. (2004). *Managing information Technology for business value – practical strategies for IT and business managers*. Intel Press.

Curley, M. (2007). Introducing an IT Capability Maturity Framework, *International Conference on Enterprise Information Systems.*

Crawford, J.K. (2006). The project management maturity model. *Information Systems Management*, 23,(4), pp. 50-58.

Da Veiga, A. and Eloff, J.H.P. (2007). An Information Security Governance Framework. *Information Systems Management*. 24, 361-372

Elky, S. (2006). An Introduction to information systems risk management. SANS Institute. Available at: http://www.sans.org/reading_room/whitepapers/auditing/introduction-information-system-risk-management_1204

Ernst and Young, (2011). Global Information Security Survey. Available at: http://www.ey.com/GL/en/Services/Advisory/2011-Global-Information-Security-Survey---Plugging-the-data-leaks

Fraser, J. and Simkins, B. (2010). *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives,* Wiley

Frost and Sullivan (2011). The 2011 (ISC)^2 Global Information Security Workforce Study. Available at: https://www.isc2.org/uploadedFiles/Landing_Pages/NO_form/2011GISWS.pdf.

Gaudin, S. (2007). TK Maxx security breach costs soar to 10 times earlier estimate. *Information Week.* August 15, 2007.

Glass, R. (2006). Looking into the challenges of complex IT projects. *Communications of the ACM*, 49,(11), 15-17.

Goodin, D. (2011). Sony says data for 25 million more customers stolen. Available at: http://www.theregister.co.uk/2011/05/03/sony_hack_exposes_more_customers/Goodin, D. (2001b). Hackers breach chocolate recipe on Hershey website. Available at: http://www.theregister.co.uk/2011/08/08/hershey_website_hacked/

Gottschalk, P. (2009). Maturity levels for interoperability in digital government. *Government Information Quarterly,* 26 (1), pp75-81.

Gregor, S. and Jones, D. (2007). The anatomy of a design theory. *Journal of the Association of Information Systems*, 8,(5), 312-335.

Grossmann, S. (2012). Mom Hacks into School Computer System, Changes her kids Grades. Available at: http://newsfeed.time.com/2012/07/22/mom-hacks-into-school-computer-system-changes-her-kids-grades/

Hevner, A., March, S. and Park, J. (2004). Design Science in Information Systems research. *MIS Quarterly*. 28,(1), 75-105.

Hevner, A., Chatterjee, S. (2010). *Design Science Research in Information Systems*, Springer Science and Business Media.

Hewlett Packard, (2007). The HP Business intelligence maturity model. Available at: http://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA1-5467ENW&cc=us&lc=en

Holland, C.P. and Light, B. (2001). A stage maturity model for enterprise resource planning systems use. *Database for Advances in Information Systems*, 32(2), pp 24-45.

ISACA (2010). ISACA US IT risk/reward barometer survey. Available at: http://www.isaca.org/About-ISACA/Press-room/News-Releases/2010/Pages/ISACA-US-IT-Risk-Reward-Barometer-Survey.aspx

Khaiata, M. and Zualkernan, I.A. (2009). A simple instrument to measure IT business alignment maturity. *Information Systems Management*, 26(2), pp 138-152.

King, M. (2012). RBS IT Fallout: Ulster Bank Customers Still Without Account Access. Available at: http://www.guardian.co.uk/money/2012/jul/02/rbs-it-ulster-bank-customers-without-access

Kirk, J. (2007). Estonia recovers from massive denial-of-service attack. *NetworkWorld.* May 17, 2007.

Kouns, J. and Minoli, D. (2010). *Information Technology Risk Management in Enterprise Environments*, Wiley

Luftman, J. (2003). Assessing IT-Business Alignment. Information Systems Management. 20(4) pp 9-15.

March, S. and Smith, G. (1995) Design and natural science research on information technology, *Decision Support Systems* 15,(4), 251–266.

March, S.T. and Storey, V.C. (2008). Design Science in the Information Systems discipline: an introduction to the special issue on design science research, *MIS Quarterly*, 32,(4), 725-730.

Mettler, T. (2009). A design science research perspective on maturity models in Information Systems. St. Gallen: Institute of Information Management, Universtiy of St. Gallen.

Peffers, K., Tuunanen, T, Rothenberger, M.A. and Chatterjee, S. (2007). A Design Science research methodology for information systems research. *Journal of Management Information Systems*. 24, (3), 45-77.

Pries-Heje, J. and Baskerville, R. (2008). The Design Theory Nexus, *MIS Quarterly*, 32,(4), 731-755.

Purao, S. (2002). “Design Research in the Technology of Information Systems: Truth or Dare.” *Georgia State University, Department of CIS Working Paper.* Atlanta.

Rosemann, M. and de Bruin,T. (2005). Towards a business process management maturity model. In *Proceedings of the European Conference on Information Systems*, Regenburg, Germany.

Rosenquist, M. (2007). *Measuring the Return on IT Security Investments*, Intel White Paper.

Silicon Republic (2010). Closing the gaps between ICT and enterprise risk management. Available at: http://www.siliconrepublic.com/news/item/16901-closing-the-gaps-between-ic

Simon, H. (1996). *The Sciences of the Artificial*, Third Edition. Cambridge, MA, MIT Press.

Siponen, M. (2002). Towards maturity of information security maturity criteria: six lessons learned from software maturity criteria. *Information Management & Computer Security*.

Stoneburner, G., Goguen, A. and Feringa, A. (2002). Risk Management guide for Information Technology systems. National Institute of Standards and Technology. US Department of Commerce.

Sumner, M. (2009). Information Security Threats: A Comparative Analysis of Impact, Probability, and Preparedness. *Information Security Management*. 26 (1), 2-12

Sun, (2005). Information lifecycle management maturity model. Available at: http://www.dynasys.com/Downloads/Sun_ILM_Maturity_Model_2005.pdf

Taylor, H. (2006). Critical risks in outsourced IT projects: the intractable and the unforeseen. *Communications of the ACM*, 49,(11), 75-79.

Venable, J.R. (2006). The role of theory and theorizing in design science research. *In Proceedings of the First International Conference on Design Science Research in Information Systems*. 24th-25th February, Claremont, CA.

Westerman, G. and Hunter, R. (2007). *IT Risks.* Harvard Business School Publishing