Concordia University College of Alberta

Master of Information Systems Security Management (MISSM) Program

7128 Ada Boulevard, Edmonton, AB

Canada T5B 4E4

Elements of a New Comprehensive Risk Methodology

by

PASULA, John

A research paper submitted in partial fulfillment of the requirements for the degree of

Master of Information Systems Security Management

Research advisors:

Pavol Zavarsky, Director of Research and Associate Professor, MISSM

Dale Lindskog, Assistant Professor, MISSM

Elements of a New Comprehensive Risk Methodology

by

PASULA, John

Research advisors:

Pavol Zavarsky, Director of Research and Associate Professor, MISSM

Ron Ruhl, Director and Associate Professor, MISSM

Reviews Committee:

Andy Igonor, Assistant Professor, MISSM
Dale Lindskog, Assistant Professor, MISSM
Ron Ruhl, Assistant Professor, MISSM
Pavol Zavarsky, Associate Professor, MISSM

The author acknowledges the significant contributions to the work by Academic Advisors and Review Committee Members and gives the right to Concordia Univeristy College to reproduce the work for the Concordia Library, Concordia Websites and Concordia MISSM classes.

Elements of a New Comprehensive Risk Methodology

John Pasula

1. Abstract

Organizations may have multiple forms of risk management used within different organizational units. This paper presents the benefits of a comprehensive risk management framework which can be used to tie the different levels of risk management together into one comprehensive framework. These key elements may be used to develop a comprehensive risk management framework, which will bridge any gaps left by the individual risk management areas.

This paper will start with a brief introduction to risk management which will clarify the terminology used within the paper because there are numerous definitions of what risk management is, and that it needs to be clear on what the author means by different levels of risk management. While the concepts may be familiar to risk management professionals, the terminology differs in many frameworks, for example one framework may use the term “impact” and another may use the term “consequence” when they are both referring to the same thing. From there, the concept of different levels of risk management is introduced and explained and then issues with current risk management frameworks are identified with case studies on some common frameworks. Next in the paper are the key elements of a new risk management framework, followed by the benefits of a new risk management framework. The paper concludes with examples of how the suggestions can be used and criticisms of the suggestions.

2. Introduction

Risk management is important within an organization, however there is no clear framework to link multiple levels of risk management together. In order to increase efficiency in risk management, different levels of risk management must work together in synergy. This paper provides key elements that are necessary for those different levels to work in synergy.

The paper is written to be neutral to all levels of risk management and briefly introduces each level, with examples on how methodologies are used within each level. Risk management is not specific to one domain (information security, financial, enterprise wide) instead it is important to all domains. To illustrate examples within the paper, there will be a focus on information security risk assessment examples. The paper will provide key elements which need to have a centralized approach within a comprehensive risk management program. These elements are not unique to an individual domain, instead are being duplicated across all domains in the risk management world. It will provide ways to optimize efficiency of the risk management process by removing duplication of work effort, improving communication channels between risk management areas and the end user, and increasing the ease of use of the risk management work tools and information.

These concepts have been identified through practical application within government organizations at the provincial level, and thus are based off of this knowledge. In addition, multiple risk management frameworks have been identified, however the OCTAVE methodology and AS/NZ 4360 have been examined in depth to provide illustrations on how a single methodology cannot be expanded to meet the requirements of all levels.

A) Definition of risk assessment

Risk assessments come in many forms, are used for many purposes, and can be implemented in many ways, but they all serve one main purpose which is to reduce the risk of an event occurring. There are two components to risk, consequence and likelihood, which risk is a combination of both.[i] Risk can have both negative and positive outcomes and thus is looked at from both perspectives.[ii] Risk management deals with threats from all different sources, including the environments, technology, humans, organization and politics.[iii]

Risk assessments are conducted to manage the risk within an organization, and to reduce the residual risk for negative events occurring. These assessments may often comply with legislation, and provide assurance of completing a project or business goal. Newer legislation may require periodic risk assessments to be conducted[iv].

3. Overview of basic risk assessment

All risk assessment methodologies can be broken down into a simple four step process[v]:

1) Identify the objective of the risk assessment (scope)
2) Identify the risks to the objective
3) Identify existing controls mitigating risk
4) Assess the risks developing new mitigation plans

This basic methodology is incorporated into many different risk assessment methodologies out there, including the Operationally Critical Threat Asset and Vulnerability Evaluation (OCTAVE), Fundamental Information Risk Management (FIRM), Information Risk Analysis Methodologies (IRAM), The Australian/New Zealand Standard on Risk Management (AS/NZS4360:2004), and The Committee of Sponsoring Organizations of the Treadway Commission (COSO). Each methodology tailors this method to meet specific criteria, however the fundamental concepts described previously are contained within the individual methodology.

Identifying the objectives of the risk assessment is simply determining what the scope of the risk assessment is, and what the ultimate goal of the risk assessment is. Different organizations have different priorities on which risk impacts affect the organization more, and this is the stage in which those are identified, along with how detailed the risk assessment will be.[vi]

The next fundamental step involves identifying the risks to the objective identified in the first part. Risks can have both a negative and positive impact. A negative impact risk is something that will prevent the objective, whereas a positive impact risk is something that may help complete the objective. The OCTAVE methodology for risk assessment involves identifying all the risks, and then focusing on the most critical risks.[vii]

In risk management there is a concept of inherent risk versus residual risk. The inherent risk involves the risks to the objective before any controls are in place[viii]. The residual risk is the risk after controls are in place.[ix] This stage of the risk assessment often involves an analysis of the effectiveness of existing controls.[x] Controls that are in place may not actually lower the residual risk to the objective.

The final fundamental stage involves assessing the risks. Risks may be dealt with in four generic ways: Avoid, Reduce, Transfer, Retain (Accept)[xi]. Often risks are assigned a value to determine which course of action is appropriate. This value, called the expected value[xii] is simply a mathematical combination of the probability of the risk occurring and the overall impact if the risk is realised. High expected values are reduced (mitigated), whereas low expected values are retained.[xiii]

4. Different levels of risk management

There are multiple perspectives of risk management, each having their own standard, and guidelines. The view of these levels differs, with the highest level looking at risks from an organizational view at a high level, and the lowest level looking at risks from a specific project view. In order to have a comprehensive risk management program within an organization, all levels of risk management must be present[xiv]. The fundamental problem is that the different levels of risk management are not always interconnected, which results in duplication of work, confusion for the end-user and overall loss of efficiency.

In addition to the tiered level approach to risk management, there may be a dichotomy within a specific domain. Within information security, there may be a comprehensive program that encompasses all information security assets while there may be another stream of project based risk assessments.

There are three main perspectives of risk management: high level enterprise risk management, specific area risk management, and low level project based risk management[xv]. High level enterprise risk management looks at risks to the organization as a whole such as business goals and objectives. Methodologies such as AS/NZS4360 or COSO are used, and risks are treated at a high level. The middle tier of risk assessments involve financial and information security risk management. These risk management areas are more detailed than enterprise risk-management, but still provide a broad view for their subject area. Methodologies such as OCTAVE and FIRM are used for information security, and there are legislative guidelines which are generally used for financial risk assessments. At the lowest tier of risk assessment lies project based risk assessment. Methodologies for these assessments may be developed by the project team, and usually are a quick scan of the risks to the project.

With a decentralized and non-integrated approach to risk management, it is possible for a specific risk management project to fall into multiple perspectives. That is, a project can easily have a financial and information security focus. With no integration between the different risk management areas, questions arise as to which area will be responsible for completing the risk assessment, and in addition there may be organizational lost if all the right stakeholders are not included in the discussion.

5. Issues with Risk Management Frameworks

The fundamental issue with all levels of risk management involves the interaction between them. In some organizations, not all risk management areas are synced with each other, which lead to a host of issues, including duplication of work effort, ambiguity with risk terminology, missing risks, and difficulty for the end user. There is very little existing work which ties all levels of risk management together, instead all methodologies focus on improving a specific area of risk management, or expanding a specific methodology from one tier to another. One example of a framework which does take into consideration the different levels of risk management is from the Mitsubishi UFJ Financial Group[xvi]. This framework focuses on the financial sector but does acknowledge the other areas of risk management. Another comprehensive framework is the NIST Special Publication 800-30[xvii], which also incorporates all the different areas of risk management, but has an information security focus. This paper will focus on ways to which a comprehensive risk management framework will benefit an organization, and will not deal with the implementation of the framework. The paper will not provide a new framework, but will discuss the different areas in which all levels of risk management can be merged and provide key elements of a new comprehensive risk management framework. As a result, the paper is different from the frameworks above in that it is not a framework itself, nor is prescriptive. It describes the different areas in which a comprehensive risk management framework can be expanded upon. The information presented is based off of practical experience within the Government of Alberta, as well as the Regional Health Authorities in Alberta. In discussion with other jurisdictions, the claims made in this paper can be applied to them as well, however the authors practical experience deals only with the jurisdictions above.

A new framework must start off with a clear, concise policy statement which outlines the ultimate goal for risk assessment within an organization, and gives authority to combine the different levels of risk assessments. In addition, it must be methodology/framework independent, allowing any framework to be used at any tier, removing any common elements. The large gap in existing frameworks involves the interoperability between the different levels of risk assessments, and this paper will address these issues.

A) OCTAVE

The OCTAVE methodology is tailored at information security risk management. It's composed of three phases which each are divided up into processes. OCTAVE has been criticised that it is a heavy framework and very paper intensive.[xviii] The frameworks reliance on a lot of paper forms can be seen by the multitude of official forms included in the methodology, however this can be alleviated by computer software which would make the information gathering process simplified. However, the methodology is still heavy.

The first phase of OCTAVE is the Organizational View in which critical assets and threats are identified. The methodology requires that you have three sets of meetings with different business areas, one with the senior management, one with general staff, and one with IT staff. Having

attempted to put this methodology into practice, some responses from staff have been "why are you asking me about this, doesn't IT take care of it", "how am I supposed to know", and many other responses along the same line. The complexity and time requirement of the first phase of OCTAVE does not lend itself well to the lower tier of risk management, where you want a very quick risk assessment completed.

The second phase of OCTAVE is the Technological View in which the critical assets are tested for technological vulnerabilities. This phase is revolves around vulnerability scans and other means to identify issues on an IT level. There is no direct translation to non-technological assets and as a result this phase cannot be easily translated into an ERM style methodology or a project based one.

Overall the OCTAVE methodology is a good choice to use for IT related comprehensive risk assessments, however there are better choices for the quick project based assessments for IT related assets. The methodology does not lend itself to being scaled down for the project levels, and because of its clear IT focus cannot be scaled up to a more organizational view ERM type of risk management.

B) AS/NZ 4360

AS/NZ 4360 is designed for high level ERM within organizations and as such is designed to be comprehensive and thorough. It is often compared with COSO, and has been suggested as a better alternative to that risk management standard[xix]. Also new with the AS/NZ 4360 standard is the concept of risk that is identified. Risk in the standard has both negative and positive outcomes. The standard has seven steps which are: Communicate and Consult, Establish the Context, Identify Risks, Analyse Risks, Evaluate Risks, Treat Risks, and Monitor/Review. The Government of Alberta has adopted this standard for use with ERM activities within the government.

Within the standard, it states that "this Standard should be applied at all stages in the life of an activity, function, project, product or asset"[xx]. This has the implication that the standard is designed for more complex, in-depth projects and as a result may not be suitable for the low end project based assessments. In addition, the flow from the final step of the standard is that Treat Risks leads to Monitor and Review which then leads to the starting step of the standard Establish the Context. This means that process cyclical, and really doesn't end. With the low level risk assessments they usually are considered "one-offs" where examining the results is not critical.

Both OCTAVE and AS/NZA 4360 are excellent methodologies for the role they play. However, the break down when you try to translate them to another tier of risk management. In addition, they have excellent lines of communication within them, however there is very little to no communication outside the process aside from some specific repositories of information. This breakdown within the respective methodologies is why the ideas presented in this paper are important in a multi-level risk management program.

6. Key Elements of a New Comprehensive Risk Management Framework

Current risk management frameworks deal with managing risk at a specific tier. The AS/NZ 4360 standard is tailored at providing risk management at an enterprise level, and there is no focus on working with different levels of risk management.[xxi] The fundamental concepts behind the standard can be applied to any level of risk management, however the details on how multiple levels of risk management can coexist and integrate within an organization is not covered. The OCTAVE methodology is similar to AS/NZ 4360 in that it is tailored for a specific level of risk management, can be applied to other levels, but there is nothing regarding the interoperability between different levels of risk management. A comprehensive risk management framework must take into account that there may be different levels of risk management within an organization, each with a specific role within the organization.

A) Project Risk Management Frameworks

Project level risk management frameworks are focused at the low level, on a specific topic. Generally they do not take into account over multiple projects, and are quick to complete. Some project based risk assessments are simple check lists[xxii] which provide a quick level of assurance that the project will be complete. Overall, these types of risk management frameworks are easy to plug into any type of project, provide a level of assurance to the project team that the project risks are addressed. These assessments may often be custom made by the project managers, or project management office (PMO) of the organization to fit into the project charter or to comply with internal standards. As a result, they may not use the same terminology and may duplicate effort done in different levels of risk management. In addition, the PMO may be responsible for tracking the risks, or the project manager, however the risks may not be entered into a single, global tracking system for the organization.

B) Financial Risk Management Frameworks

Financial risk management frameworks are more mature than other types of risk management, having been in existence longer, however they have issues which have led to major legislation changes[xxiii]. Financial risk management frameworks deal with financial risks within the risk universe and focus on limiting financial loss[xxiv]. These risk assessments are generally handled by the financial departments in an organization, and are tailored to meet the specific requirements imposed by financial legislation or auditor requirements[xxv]. As with project management risk frameworks, financial risk management frameworks have their own set of terminology, which may not be synced with other terminology in the organization. The finance department in an organization is generally responsible for tracking the risks, however they will not be entered into a central database.

C) Information Security Risk Management Frameworks

Information security risk management frameworks such as OCTAVE, FIRM, or NIST are tailored towards the IT aspect of an organization, and as a result often employ some sort of vulnerability

assessment for the IT components used within an organization. These risk assessments may use their own terminology, and have their own forms and standards, and are generally completed by the information security department in an organization. Information security risk management frameworks are becoming well standardized with publications from ISF, BSI, and ISO providing guidance and support for information security risk assessments. While these frameworks are standardized, the information provided is generally used within the information security domain. As stated in the research paper about Holonic Risk Management, IT is central in the economy, and is extremely vulnerable[xxvi]. As a result, the divergence between a central risk management area and information security risk management may have serious consequences.

One component of information security risk assessments involves a technical scan of the information technology devices used within the organization. This may often be a network vulnerability scan along with a port scan of specific machines.[xxvii] This is unique to the information security field as the other risk management domains do not have automated scanning tools to detect vulnerabilities, and instead rely on other methods to obtain this information. These tools may often have a large database of known vulnerabilities and exploits[xxviii], and in addition to this the vulnerabilities may be ranked according to severity[xxix].

D) Enterprise Risk Management Frameworks

Enterprise risk management (ERM) is a buzzword that is being thrown around in the past few years by corporate executives[xxx]. While not the silver bullet to risk management, ERM provides an organizational wide view on risk management activities, and attempts to encompass all possible risks within an organization. ERM focuses on risk at an organizational level, however there is a disconnect between ERM and the other levels of risk management in an organization, which leads to gaps within the risk universe of an organization. Because ERM has a cross-organization view on risk, there may be difficulty with roles and responsibilities. In addition, ERM has its own risk universe, tracking mechanism, and forms.

E) Difficulties with Risk Management Frameworks

Currently risk management is spread out amongst the different business units, which causes problems relating to end user uptake, efficiency, roles and responsibilities and adaptability. A problem is that the different risk management areas are isolated, and there may be little to no interaction between them. This leads to a host of issues, including duplication of work effort, loss of risks in the risk universe and different risk appetites which may not be consistent with the organizations risk appetite. Examples of these problems will be discussed in section 4 of this paper, and will outline reasons for having a hybrid of a centralized and isolated system. Each individual risk management area are subject matter experts within the domain they work in, however there are a multitude of risk management projects that cross domain boundaries. This is not to say that a financial risk assessment of expenditures for a fiscal year needs to be discussed with the other areas of risk management, or that a technical network vulnerability scan and the resulting risk assessment in the information security field needs to be discussed with other areas of risk management, however there will be projects where input from all areas will improve the overall result of the risk

assessment and provide better value for the organization. For example, the implementation of a wireless network within an organization while primarily an information security focus, will have financial considerations as well overall ERM considerations to be taken into account. A possible setup for risk management in an organization is depicted in figure 1.

In the figure, Information Security, ERM, and the financial area are responsible for their own risk assessments, in addition Project 1, Project 2, and an IT Project are handled by the project teams. There is no communication between the different areas, there is a multitude of work duplication between the different areas, and not all projects are working with their respective areas of responsibility. This figure is a fictitious example of risk management in a mature organization. The organization is mature enough to realize that risk management is needed for all different areas within the organization, however there is no connection between the different areas.

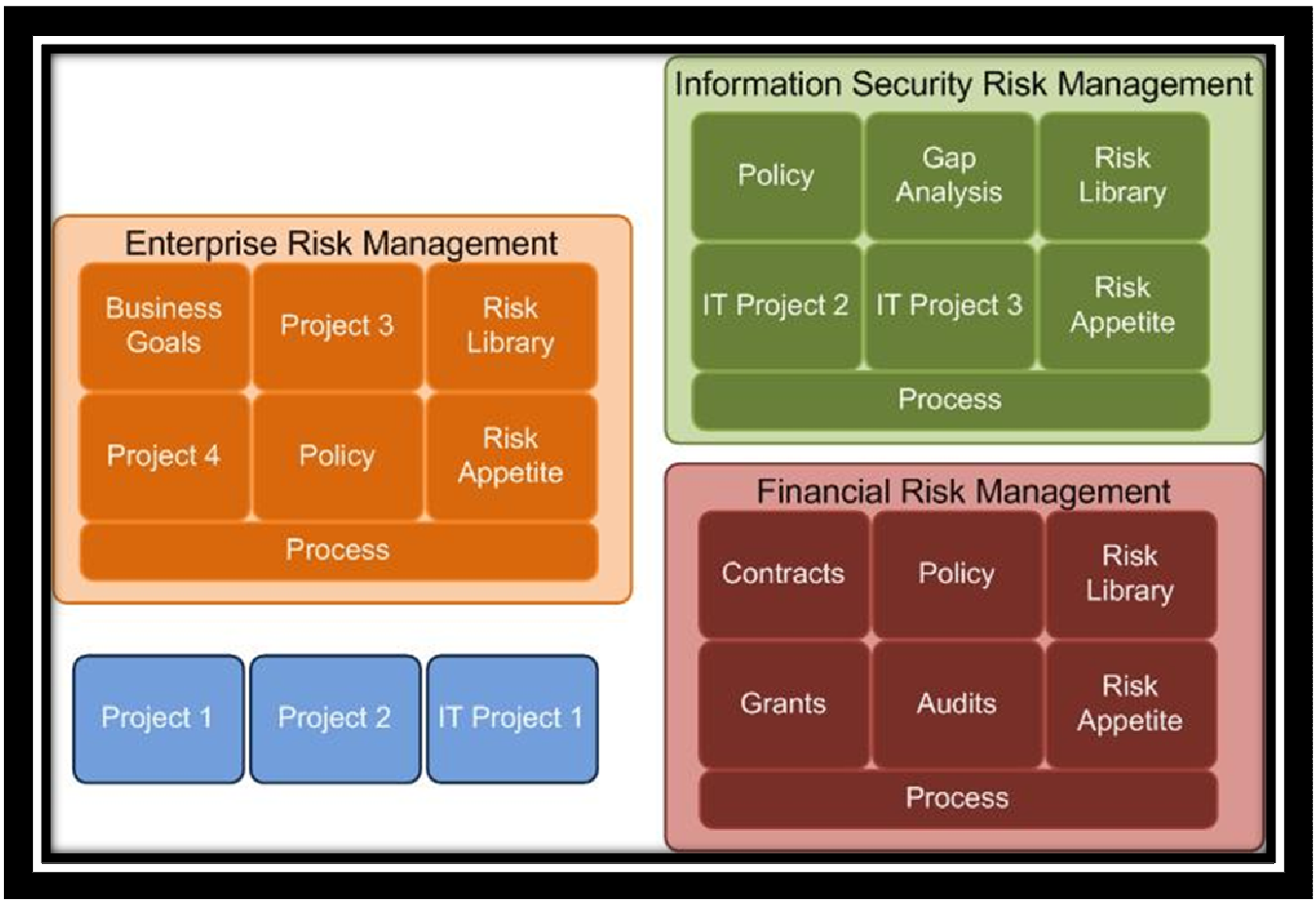

Figure 1

7. Benefits of a Comprehensive Risk Management Framework

A comprehensive risk management framework is about improving overall efficiency of the risk management process. This can be done by:

1. Clearly defining processes
2. Streamlining processes
3. Defining common terminology
4. Identifying roles and responsibilities
5. Developing common work tools
6. Allowing for adaptability

These improvements have other affects than just increasing efficiency of the entire process. Overall organizational knowledge will increase by having a centralized risk library, end-users will have an easier time with centralized points to enter the risk management process, there will be less duplication of work, and more cooperation with clearly defined roles and responsibilities, and the organization will have a higher level of assurance that the risk appetite is being followed.

Figure 2 demonstrates an optimized version of risk management framework within an organization. This figure is an ideal version of what this paper hopes to achieve, integrating the different risk management areas.

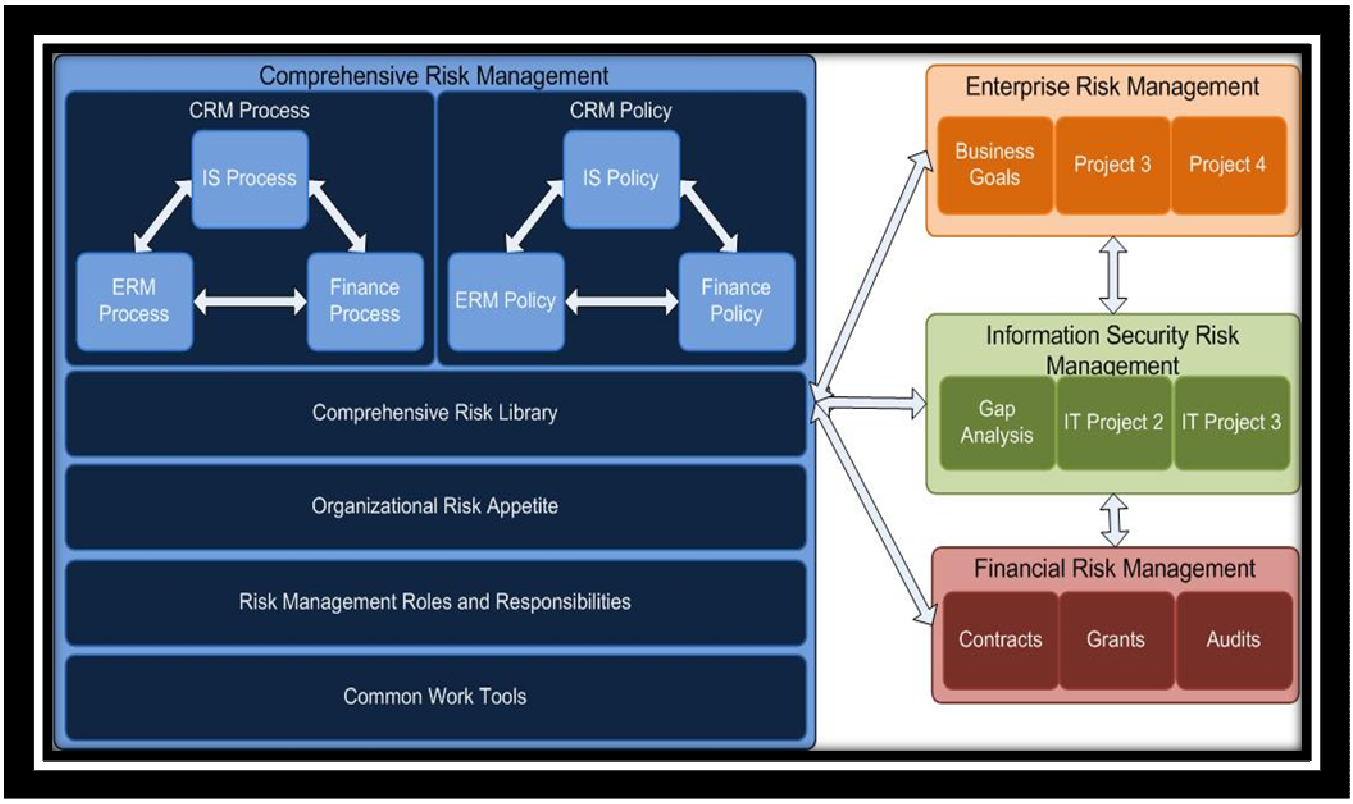

Figure 2

A) Defined Processes

Defining processed in a comprehensive risk management framework involves outlining how all the different risk management areas will work together, and ultimately will provide a clear and logical work flow for both the end user and the risk management professionals. Essentially, this will allow the entire risk management process to be understood without any conflicts from the different business units. Defining the comprehensive risk management processes will help ensure that all projects are covered by risk management, and more specifically by the appropriate areas. It will also create a central area which will provide governance for the entire risk management process. Figure 3 identifies the miscellaneous projects being assigned to a respective business unit, as well the creation of an overall comprehensive risk management process.

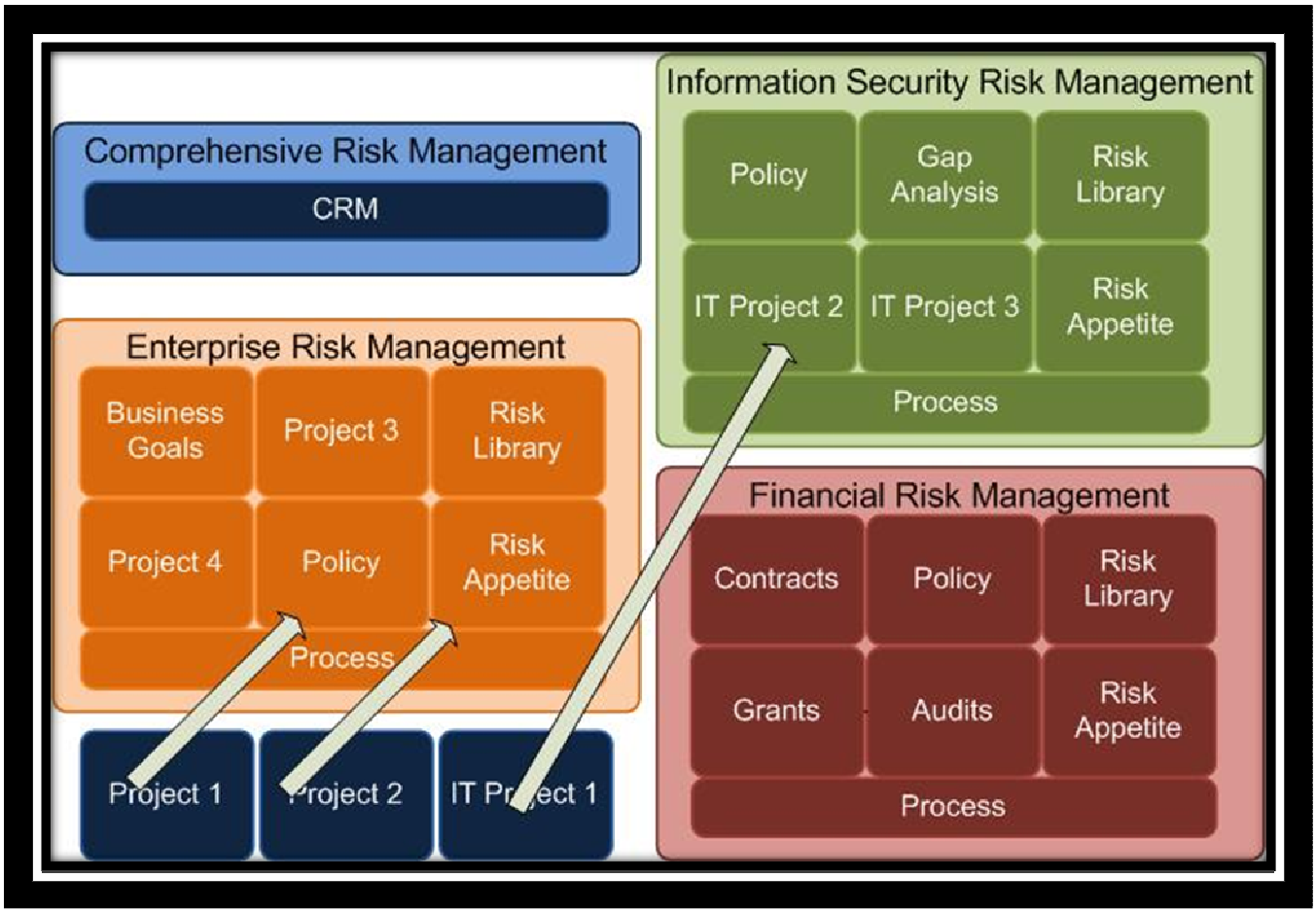

Figure 3

B) Streamlined Processes

Each individual business area may have its own risk management process which may lead to some duplication of work effort within a comprehensive risk management process. Individual business units will still require specific risk management processes to complete risk assessments for their respective business areas, however all areas will have commonalities between them. The concept of streamlining the processes involves moving the commonalities from the individual processes into the comprehensive risk management process, and to make all risk management processes work together, and to be aware of each other. This will allow the processes from the different business units to coexist with each other, and will improve the overall efficiency of the risk management process. In addition, it will remove redundancy from the processes, and as a result will increase ease of use to the end user. Figure 4 demonstrates the individual processes being transferred from the respective business units into the comprehensive risk management scope, and increasing the interaction between the processes.

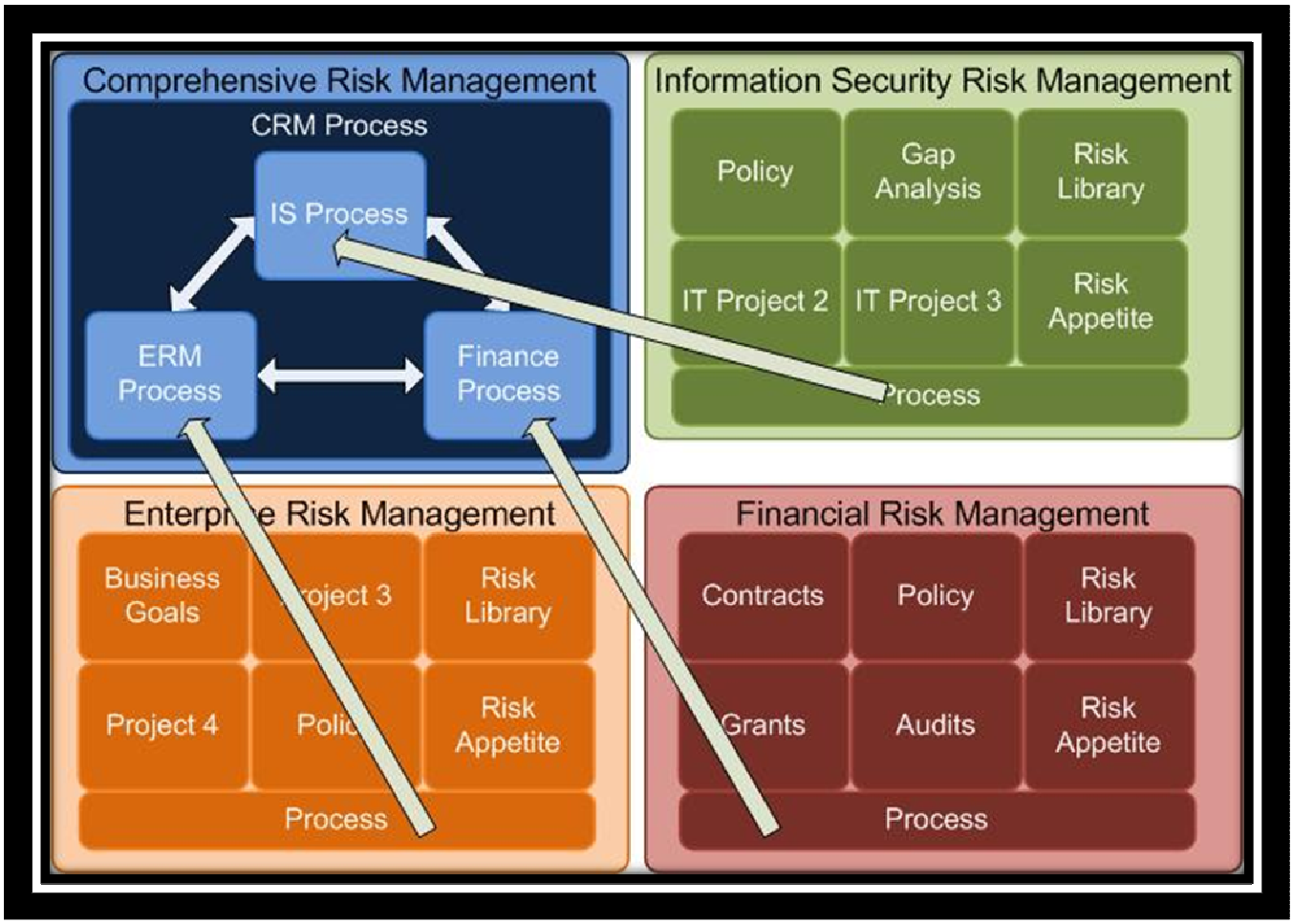

Figure 4

C) Common Terminology

Common terminology for the risk management process follows the similar ideas of the Information Technology Infrastructure Library (ITIL). ITIL is about defining processes and terminology within the IT environment[xxxi], which is what needs to be done with risk management. A risk library is a living document which identifies all the risks that an organization has faced[xxxii]. It is used to assist with assessing risks as you have historical references to refer back to during the assessment. A best practice with risk management is to list various risks for a business area[xxxiii], which if each different risk management area does this leads to multiple libraries and no shared information between the business units. As a result, a centralized risk library will improve the overall risk assessment process for an organization as it will provide more content to each of the different risk management areas.

In addition to a risk library, risk management processes have defined risk impacts, risk probabilities, and risk levels. It is possible for different risk management areas to have different impact, probability and level definitions. For example, with financial risk one business area may dictate that a low impact is $25,000 or less loss, and a low probability involves it occurring once every decade. Another business area may dictate that a risk level of 1 is $50,000 or less loss, and an infrequent

probability is once in the history of the organization. Different definitions make it difficult for assessments to be compared and make it difficult for management to understand where the real risks are within an organization. Therefore common risk impact, risk probability and risk level scales are needed between the different risk management areas. Figure 5 demonstrates the different risk management areas having individual risk libraries, which are then merged into a comprehensive risk management library.

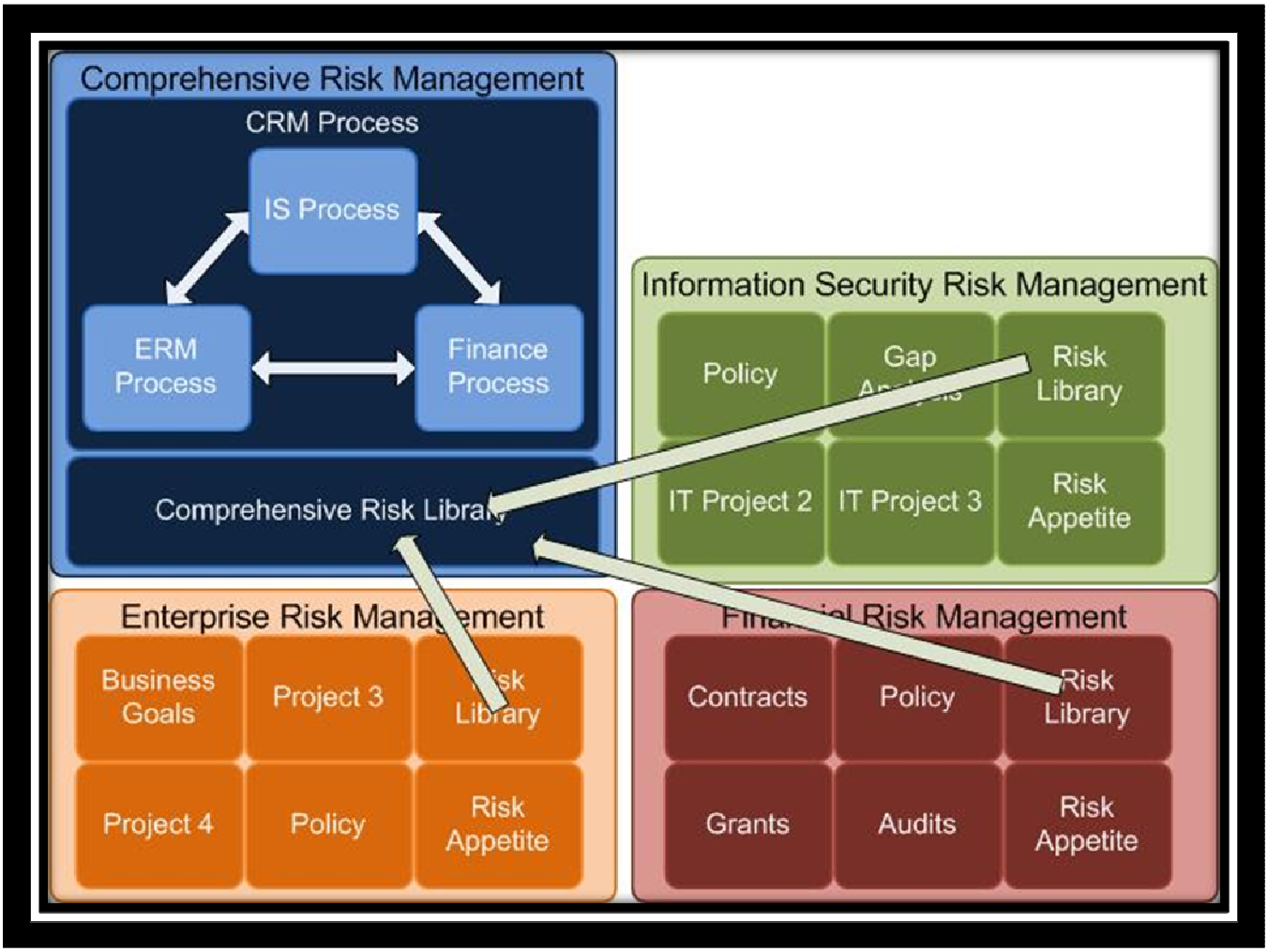

Figure 5

D) Roles and Responsibilities

Having multiple risk management areas in an organization presents a difficulty on which area is responsible for performing a specific risk assessment. Clearly defining the roles and responsibilities of each risk management area in the organization will ensure that each individual project is handled appropriately within the realm of risk management.

Another concept that must be addressed is authority levels, and specifying the organizational risk appetite. Risk appetite involves which level of residual risk is acceptable to the organization, and there may be multiple risk appetites for each individual risk management area. These individual risk

appetites may not be consistent with the organizational risk appetite. By defining roles and responsibilities, you also define how much authority each risk management area has, and which area will dictate the organizational risk appetite which will then in turn drive the risk management risk appetites. Figure 6 demonstrates the individual risk appetite being merged into a centralized risk appetite for the organization, and the creation of a centralized area for determining roles and responsibilities for each risk management area.

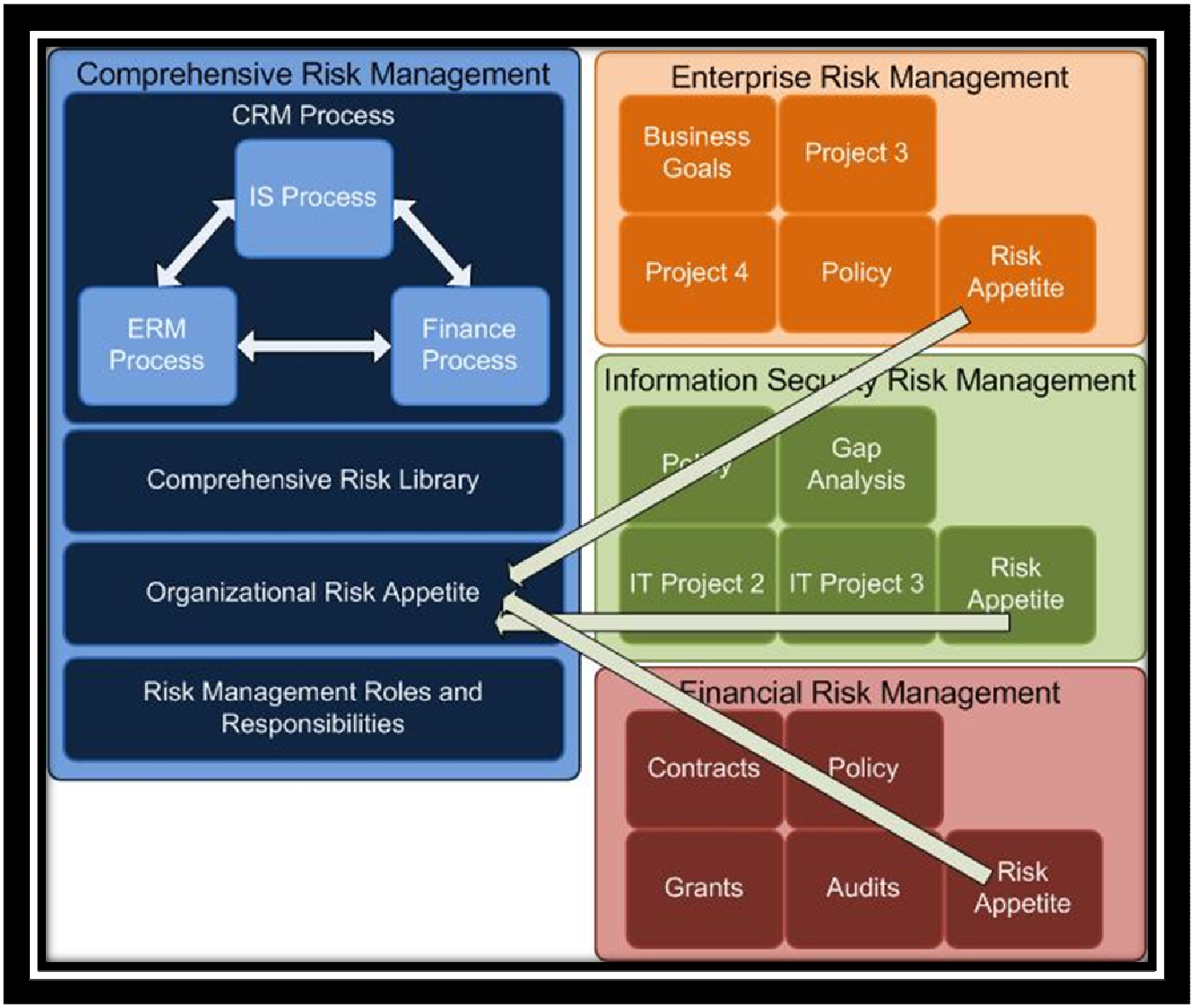

Figure 6

E) Common Work Tools

Risk management areas will have individual forms, tracking systems, etc. for their own areas, which can be considered work tools. These work tools are customized to meet the needs of the individual risk management areas, however there will be commonalities amongst the tools. The work tools used must comply with a similar look and feel for visual identity of the forms, same underlying logic

for the layout of the forms, and the same overall concept for the design of the forms. This will improve communication between the different business units, as they will not have to learn a new system when reviewing risk assessments from another area, and it will improve end-user use as they will be familiar with the work tools regardless of which area they have had to work with. Figure 7 demonstrates the creation of a common work tools repository for the comprehensive risk management framework.

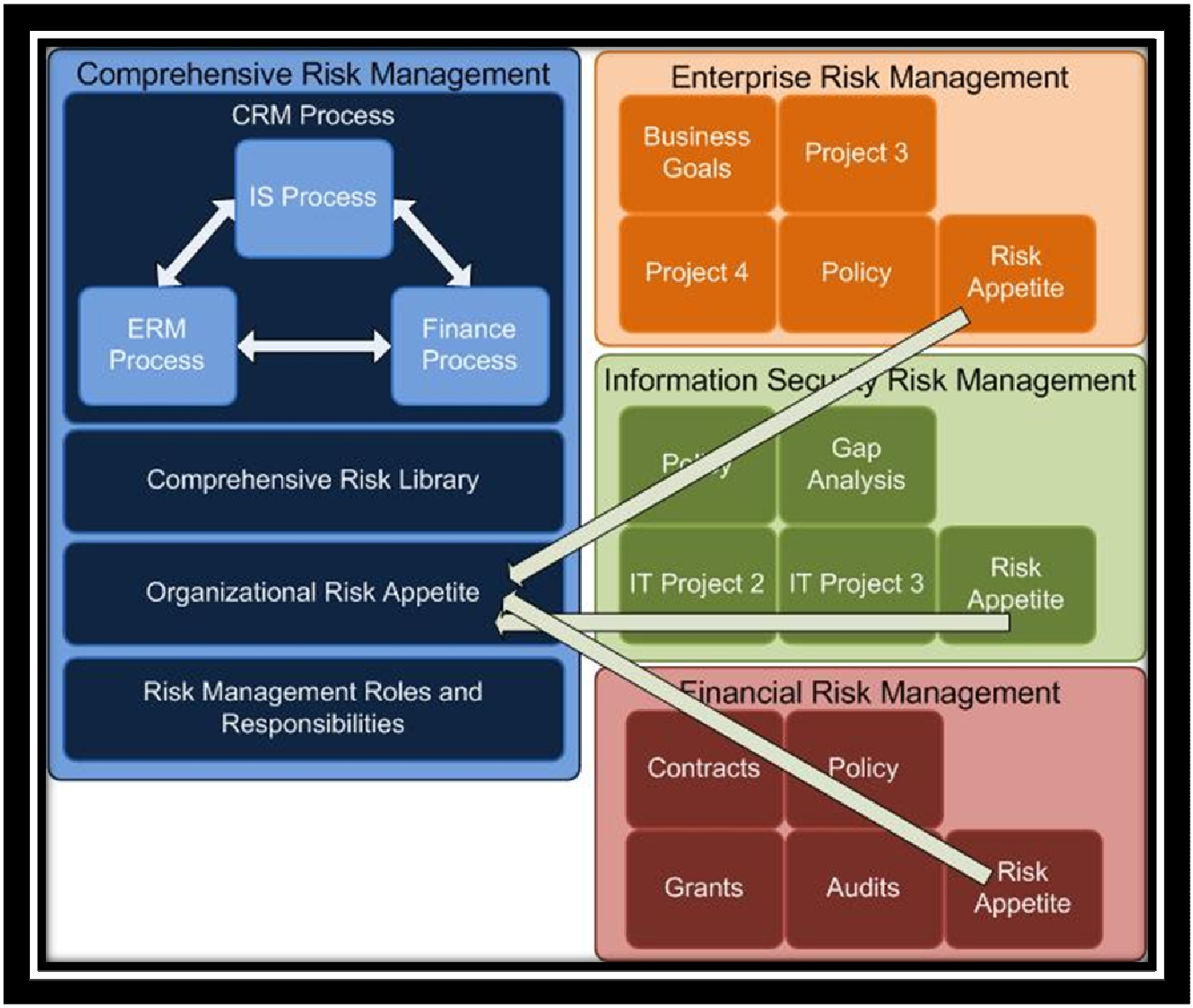

Figure 7

F) Policy

The policies within each different risk management area must align with each other, and interact with each other. The policies must interact and be linked, and take into account that there are multiple risk management areas responsible for the organizations overall risk management picture. Figure 8 demonstrates how each isolated policy can be pulled into the comprehensive risk

management framework, and the linkages needed. Best practices for what is needed in a policy is not within the scope of this paper, and this section is designated to convey the concept that the policies for each risk management area must be aware of each other.

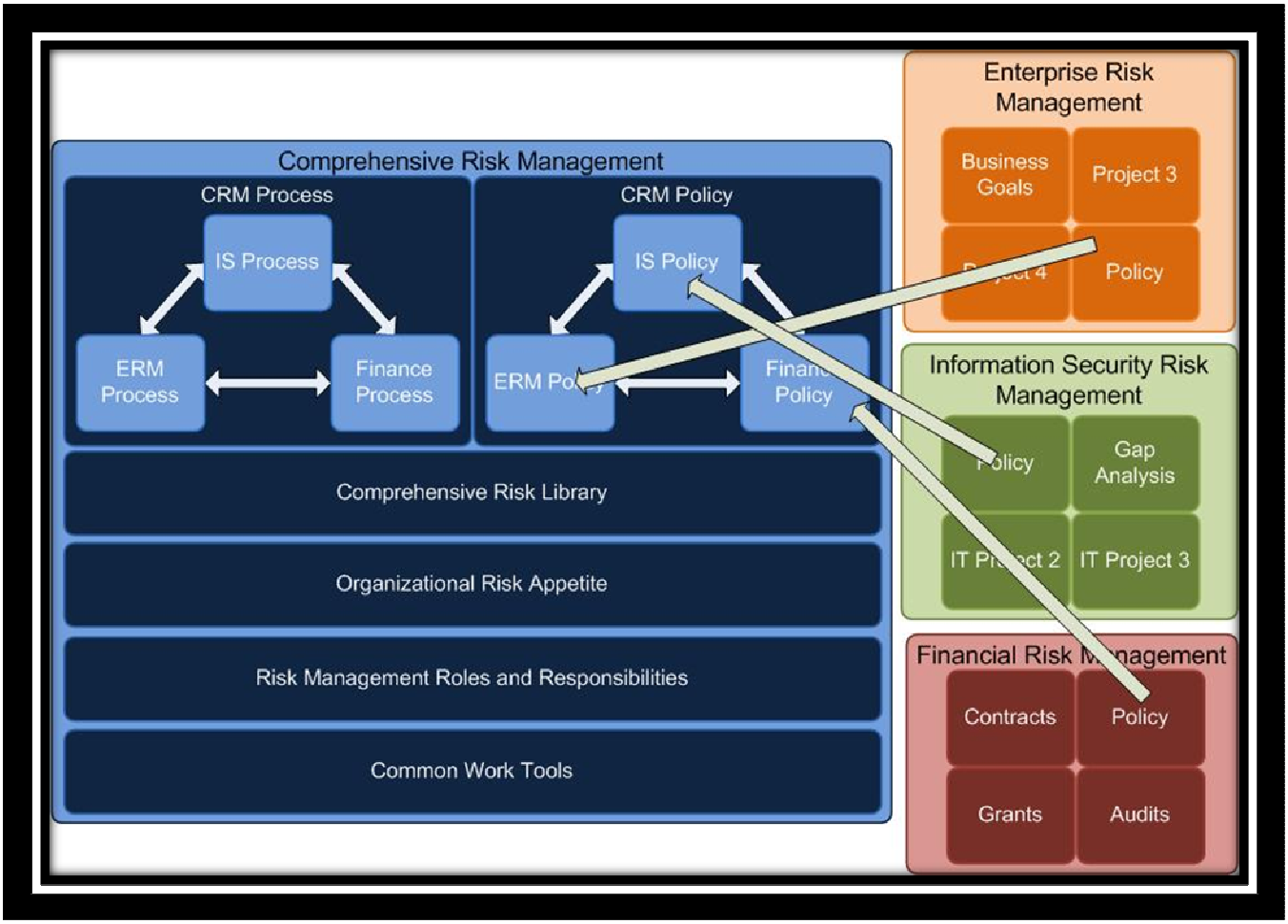

Figure 8

G) Adaptability

A comprehensive risk management framework must be descriptive, not prescriptive. It must be methodology independent, allowing any type of methodology to be plugged in to any level of risk management, and allow the risk management professionals to pull common elements out of the methodology into a centralized location. That is, at an enterprise level is should not matter if COSO or AS/NZ 4360 is used, or at an information security level it should not matter if FIRM or OCTAVE is used. All risk assessment methodology are compromised of the same basic key elements, which are found in practically all risk methodologies, and the end result of the assessments are the same in that a risk assessment is conducted which takes into account the impact, probability and provides the residual risk. This paper allows for the integration of different risk levels, without the need for implementing specific methodologies for each area, which will allow organizations to adapt this approach that much easier. However, any methodology used will have to be modified to meet the

needs of an integrated approach, such as having key terms redefined to match up with other levels. This will have no impact on the methodology itself as it only changed the name and definition of terms to fit within the confines of the organizational needs.

8. Theoretical and Practical Examples

As mentioned previously, the information presented in this paper is based off of practical examples within the regional health authorities in Alberta along with the provincial government. This section will illustrate some examples where a comprehensive risk management framework would improve the overall risk management within an organization.

A) Duplication of Work

Without a centralized area for risk management within an organization, there exists a high probability for duplication of work. In 2007, a Government of Alberta top priority involved Protecting Peoples Private Information.[xxxiv] It was possible that both the enterprise risk management area and the information security risk management area would conduct risk assessments on the private information within the organization, without interacting with each other. This would have resulted in two complete risk assessments being conducted, which involved going to different stakeholders of private information within the organization. As a result, numerous stakeholders would have had to explain the same information twice, to two different risk management areas.

For this specific project, the different risk management areas worked together, following similar guidelines outlined in this paper for a comprehensive risk management framework. This reduced the amount of possible duplication of work substantially, as only one risk assessment was conducted, and stakeholders need to be contacted once only. If the different risk management areas did not work together, both areas could have done a risk assessment, which is a clear duplication of work.

This practice may be common in organizations, in that a project level risk assessment may duplicate some or all of the work completed by a more formal version of risk assessment. By having a centralized area which is the entry point for all risk assessments (the CRM process) you eliminate the issue of different projects or risk management areas conducting the same risk assessment, and can better split the work for interdisciplinary assessments.

B) Ranking System

A fundamental concept with risk management involves ranking impact and probability on some sort of scale indicating the severity of the risk. Different methodologies allow for different ranking scales, however this causes issues when attempting to compare risks using the different methodologies.

The information security area ranks impacts on a “Low, Medium, High” scale, whereas the enterprise risk management area uses a numerical ranking from 1 to 5. The question arises, how do

you equate a ranking of 2 on the 5-point scale with an equivalent rating on the “Low, Medium, High” scale. There is no direct comparison which makes it difficult to compare risks between the two areas. This is where a unified scale improves the operational efficiency of risk management. Having all risk management areas using the same ranking scale, or in at the very minimum developing a translation matrix will allow the risks from different areas to be compared, and ranked with each other.

C) Organizational History

One form of determining probability for a risk occurring involves looking at the past history of events. Having linked or a centralized repository of risks and events occurring allows this organizational history to be built, as well provides a means to communicate the risks from one risk management area to another. One area can easily see a listing of risks that have been identified, and in a more advanced repository would allow searching/filtering. In addition to maintaining organizational history, a repository would enable a listing of common risks to be maintained, allowing the overall risk assessment process to proceed more smoothly.

A centralized repository within CRM would increase efficiency for tracking organizational history, as well as searching through known risks, however it may be distributed in that each individual area has its own repository and just shares information through formal channels.

D) Work Tools

Within the organization, there are multiple risk assessment forms which need to be completed to fulfill the risk management process. These forms have many different formats, and have individual characteristics to them. This will lead to confusion as to which form needs to be completed by the end-user, and possibly some confusion between the different risk management areas. Adopting a similar approach as computer software does with the work tools will improve the overall ease of use for completing risk assessments.

Information security has one form for a specific type of risk assessment, another form for another type of risk assessment, projects have their own forms which need to be completed for the project level risk assessment, ERM has multiple forms depending on the type of risk assessment, and the financial area has forms to meet its own needs. All these forms can be analysed and the common elements extracted to minimize the amount of paperwork which needs to be conducted. In addition, the forms would also need the same look and feel so end-users will be more comfortable with them. This goes back to the analogy of computer software, in that within a suite of applications, they all have distinct purposes. One application is for word processing, another for spreadsheets, etc however there are common menu bars, common setups, etc for the entire suite of applications allowing users to become more familiar with the entire suit. This will not eliminate the need for specialized work tools as a financial risk assessment will have unique requirements that are not common, however it will reduce the overall duplication of work.

9. Criticisms

With any new type of framework, the biggest concern will involve the amount of work effort needed to implement it within the organization. To counter this, the different areas mentioned before do not need to be implemented simultaneously, and can be phased in. In addition, you can phase in each component of each area. For example, implementing this new framework would start with linking two different risk management areas together with a common entry point for end-users. From there, the areas can develop a risk library, and common work tools, and eventually expand to a third risk area. This would continue until the entire comprehensive risk management framework is implemented. There should be no additional cost to the organization, as no extra processes are created, no special technical hardware is needed, nor is any special software needed (at most you would need a spreadsheet or simple database to keep track of organizational risks).

In sum, the best practices mentioned in this paper can be implemented over time using a phased in approach using existing organizational resources. There will be a savings in work effort and more importantly there will be a better method for identifying and assessing risks within the organization.

10. Conclusion

A comprehensive risk management framework focuses on improving work flow, risk assessment efficiency, and ease of use for the risk management professionals and end-users. It removes duplication of work in the entire risk assessment process, focusing on enhancing the overall process. This is accomplished by allowing common elements from each level of risk management to be optimized so that they are integrated with each other and that the different levels of risk management within an organization can coexist with a minimum of duplication of work. The exact process on how to modify each level of risk assessment is highly dependent on the actual methodologies used, however this paper provides key elements which need to be addressed to have an efficient comprehensive risk management program in an organization. Integrating different elements of the various risk management levels will result in higher uptake by end-users, lower maintenance for the entire risk management process, and will improve communication flows between different risk management areas.

The material presented in this paper provides a guide on the elements which need to be addressed in order to develop a comprehensive risk assessment methodology. It is not a methodology itself, but may be used to create one.

[i] RMI Risk Management Standard
http://www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf
[ii] AZ/NZ standard/RMI Standard
[iii] http://en.wikipedia.org/wiki/Risk_management
[iv] HIA Reg 8, SOX 404 (http://en.wikipedia.org/wiki/Sarbanes-Oxley_Act)
[v] ORCA Model – BC Training
[vi] http://en.wikipedia.org/wiki/Risk_management and BC Training
[vii] OCTAVE
[viii] AS/NZ
[ix] AS/NZ
[x] AHW
[xi] OCTAVE/ http://en.wikipedia.org/wiki/Risk_management
[xii] OCTAVE
[xiii] OCTAVE
[xiv] Info security magazine (which issue?!?!)
[xv] magazine
[xvi] http://www.mufg.jp/english/csr/csrreport/2006/pdffile/14_e.pdf
[xvii] http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
[xviii] http://aegissecurityworks.com/files/EnterpriseRiskAssessmentOverview.pdf
[xix] http://www.riskreports.com/protected/archive/rmr0306.html
[xx] AS/NZ 4360 Section 1.1 Page 1
[xxi] AS/NZ 4360
[xxii] FRAPS
[xxiii] http://en.wikipedia.org/wiki/Sarbanes-Oxley_Act
[xxiv] http://en.wikipedia.org/wiki/Financial_risk_management MUFG CSR REPORT 2006
[xxv] http://www.rsa.com/solutions/financial/datasheets/FSI10_DS_1007.pdf
[xxvi] Holonic Risk Management Framework 2005
[xxvii] OCTAVE Phase 2
[xxviii] Nessus
[xxix] SANS and AHW Sans top 20
[xxx] http://www.fiercesarbox.com/story/tools-and-tips-for-enterprise-risk-management/2007-05-15
[xxxi] http://en.wikipedia.org/wiki/ITIL
[xxxii] GoA defs
[xxxiii] http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/RiskManagement/rm-pps1_e.asp#_Toc456660330
[xxxiv] http://www.im.gov.ab.ca/imf/pdf/InfoMgmtStrategicPlan.pdf