Abstract: Increasing IT budget and over-dependence of business on IT infra-structure makes risk management a critical component of enterprise management. The creation and sustenance of an IT risk management framework is one of the crucial and challenging tasks of modern corporate enterprise management. This paper presents the risks that organizations face with respect to IT, discusses the key risks in IT related functions and proposes a framework to monitor the risks. Our framework organizes IT risks into five categories: infrastructure development and support, operations and maintenance of business process, office level support, software development and outsourcing management. The framework becomes the basis for an enterprise risk assessment model.

Key-Words: Enterprise Level, Risk Management, Information Technology

1 Introduction
Risk management provides a clear and structured approach to identifying risks. It gives a good foundation to understand what threats and vulnerabilities can affect the business and what are the likelihoods of them happening. It gives a formal methodology for helping to determine what the real risks are, enabling the business to focus on its true needs.

Simply implementing or reviewing processes, policies and procedures can help mitigate much risk. Undertaking risk management is crucial so that organisations know what they are dealing with. Having a clear understanding of all risks allows an organization to measure and prioritize them and take the appropriate actions to reduce losses. Given that the biggest elements of operational infrastructure these days are IT-based, and given that the business runs on IT, it means that this is where most of the risks are.

Despite the increasing emphasis on risk awareness, the adoption of risk policy is still patchy across organizations. Some firms are ahead of the game, with many blue-chip organizations in highly regulated industries, such as financial services and pharmaceuticals, having whole departments dedicated to risk management. Although some organizations do risk management on an ad-hoc basis as part of their everyday operations, they do not formally document it as a process, and the results are not formally captured.

This paper presents a framework for enterprise risk management. This framework becomes the basis for an enterprise risk assessment model.

2 Background
Not much research work has been done in the area of enterprise risk management. An Alternative Risk Management Framework (ARMF) [1] was developed covering three major components: theoretical risk management, applied risk management and model implementation. ARMF works on the principle of continuous feedback, similar to automatic control systems. Feedback loops are used to adapt the model at any phase of its development.

In IT, there are many frameworks that have been formulated to provide guidelines to the governance of IT related activities organisations. These are:

- Service Delivery (e.g. ITIL (IT Infrastructure Library))
- Organisation, IT Management & Governance (e.g. COBIT (Control Objectives for Information and related Technology))
- Project Management (e.g. P3M3)
- IT Security (e.g. ISMS)

The following portion discusses existing major frameworks.

ITIL (IT Infrastructure Library)
ITIL provides a framework of best practice guidance for IT services. ITIL has been widely...
used by big organizations such as Microsoft, Fujitsu and Hewlett Packard. It has 5 main components [2] and they are Service Strategy, Service Design, Service Transition, Service Operation and Continual Service Improvement.

**COBIT (Control Objective for Information and related Technology)**

COBIT is a framework for IT management created to ensure that IT is aligned with business, IT maximizes the benefits of the business, IT resources are being used responsibly; and IT risks are managed properly [3]. COBIT has 4 domains, which are:

- Plan and Organize
- Acquire and Implement
- Deliver and Support

**P3M3 (Portfolio, Programme & Project Management Maturity Model)**

P3M3 is the enhanced version of the Project Management Maturity Model. This framework provides the basis for improving program and project management processes. This model can be used to understand the portfolio, program and project management processes key practices; and to identify the key practices that need to be fully embedded within organizations [4].

It has five levels of maturity and each of these levels has a consistent structure that describes and focuses on outcomes. The structures are functional achievement/process goals, approach, deployment, review and perception and performance measures.

**ISMS (Information Security Management System)**

ISMS [5] stands for Information Security Management System. Information security is a very crucial issue in current environments. This is because current business scenario depends heavily on information systems. In most cases, information has become a key asset for the business. Therefore, it is important to ensure information confidentiality, integrity and availability is safeguarded.

Unsecured or misused information can lead to loss of business and reputation. The information can be in various forms such as documents, communications, messages, recordings, images and many more. Therefore, information security basically means protection of all related assets including software, hardware, network, Internet connectivity, application, database, data (both at rest or in transit), file, hard copy reports and many more. We will look at the cross-sections of IT related risks including some viewpoints and guidelines.

### 3 The Framework

In order to cover risks at the enterprise level to adequately support business processes, an enterprise risk management framework is proposed. Five risk components make up the proposed enterprise risk framework. These are seen to be components that critically support enterprise level IT management.

They are:

- Infrastructure Development & Support – covering servers, networks and knowledge structures
- Operations & Maintenance of Business Process Related Software & Hardware
- Office Level Support (Software & Hardware)
- Software Development
- Outsourcing Management

Fig.1 gives the structure of the Enterprise IT Risk Management (EIRM) Framework. Each of the 5 components is evaluated based on 2 attributes which are:

- Control Mechanism
- Capacity to Support Current and Future Requirements

The risk assessment questions supporting the enterprise risk assessment model cover the 5 risk components based on the 2 attributes. Questions asked under control mechanism are to identify control mechanisms in place that help reduce risk levels for the current situation in the organization while the questions under capacity to support current and future requirements are to identify the risk level based on past, current and future capacities. The risk level for each component will be identified by calculating from answers given by the users. The capacities of the past and current can affect the future. As such, immediate action must be taken to prevent the organization from losing its business and trust.

#### 3.1 Enterprise Risk Components

This section gives the breakdown on the 5 components and highlights factors under each.
3.1.1 Infrastructure Development and Support
Infrastructure Development and Support basically is the area for the data storage, transmission and the management of knowledge within an organization. Risks for this component are identified based on ISMS, P3M3 and ITIL. There are 7 factors in this component. These are:
- Servers
- Networks (LAN)
- Networks (WAN)
- Internet Connection Bandwidth
- Knowledge Management Structures
- Network Security
- Server Security
- Human Resources

3.1.2 Operations and Maintenance of Business Process Related Software and Hardware
This component focuses on the identification of risks that are related to software and hardware business support. In order for the business to run smoothly, all aspects of operation and maintenance need to be considered. There are 4 factors in this component. These are:
- Software Maintenance Procedure
- Human Resources
- Project Management
- Security

3.1.3 Office Level Support
Office Level Support represents the internal support mechanism of the business environment. Without internal work support, business will collapse. There are 3 factors in this component. These are:
- Software
- Hardware
- Security

3.1.4 Software Development
This component helps identify risks in the software development area. If there are risks occurring in the area, the development of the new projects will be affected or the project may be behind its schedule. There are 2 factors in this component. These are:
- Human Resources
- Project Management

3.1.5 Outsourcing Management
Sometimes, when the organization does not have enough resources to develop systems, they will outsource it. As such, they must identify the risks that will occur before, during and after the outsourcing process. There are 3 factors in this component. These are:
- Agreement
4 Conclusion
In this paper we describe our approach to enterprise risk management covering 5 critical components. The proposed framework attempts to cover all important categories and processes. Each of the 5 components is evaluated based on 2 attributes: control mechanism and capacity to support current and future requirements. The framework becomes the basis for an enterprise risk management model. The next phase of research will include development of a tool to support the model.

References: