Risk assessment procedure

Overview

A risk assessment takes each threat to the organization's key processes in turn and assesses the current exposure of the organization to it through identifying controls to prevent the threat occurring or limit its impact, making practical recommendations for control improvements. The policy is drafted by Mr. Subhendu Sarkar.

A Risk Assessment is
Identifying, analyzing, and weighing
All the potential risks, threats and hazards
To the business's internal and external environment.

Purpose

A risk assessment is required to understand the threats which could be materialized and the impact they would have on the organization.

Scope

This policy covers all kinds of business risk related to Information system security and applies to all information system infrastructure and their users i.e. all members of the organizations.

Definitions

Threat

A threat (or hazard) is anything that can go wrong or cause harm e.g. **power loss, theft, explosion, flood, accident, sabotage etc**. The impacts of threats materializing vary but they normally result in direct and indirect financial loss, in some cases reputation/brand damage and even, following severe incidents for which the organization is unprepared, failure of the organization to survive.

Risk

A risk consists of two components:

- the likelihood or probability that a particular threat will materialize
- the impact or consequences that might result, hence a risk is a measure of how likely a threat is to impact the organization given the level of control in place to avoid or manage the threat.

Control

A control is a means by which the likelihood of a threat materializing or the impact of the threat should it materialize is reduced. Controls come in many forms but can include **fire suppression systems, security access controls, an effective off-site data backup regime, manual workarounds for key processes, use of multiple offices to spread risk etc**. Controls need to be cost-effective and appropriate to the risk faced.

Information assets

All hardware, software, systems, services, personnel, information (printed and/or electronic) and any other related technology assets that are important to the business.

Sensitive assets

Information assets that require protection against unavailability, unauthorized access, or disclosure. Sensitive information assets may be confidential and/or critical.

Potential exposures to RISK may be classified as:

- **Facility Related**: Bomb Threat, Civil Disturbance, Electrical Failure, Fire, Water Leaks, Work Stoppage / Strike
- **Technology Related**: Human Error, Loss of Telecommunications, Data Center Outage, Lost / Corrupted Data, Loss of Local Network Services, Power Failure, Prolonged Technology Outage, UPS / Generator Loss of service.
- **Nature Related**: Earthquake, Flood / Flash Flood, Hurricanes / Tropical Storms, Severe Thunderstorms, Tornado, Winter Storms

Responsibility

This policy provides guidelines for procedures and responsibilities for management, system administrators and users. All staff must understand and accept the need for Risk assessment and it should be seen as a common responsibility. All Staff members can raise their concerns or report observations.

Procedures

Assessing Risk

- Identifying – Risk, hazards and threats
- Prioritize Risks- top the risks who will more affect the critical assets and activities
- List and Define Risk- in a sequential manner with a brief explanation to each
- Probability - of Occurrence of a threat/ hazard
- Vulnerability- to Risk of critical activities
- Potential -Impact on Organization and its resources and business
- Set- Risk Appetite
- Preventative -Measures in Place to control the risk
- Carry out a cost benefit analysis
- Insurance Coverage – transfer of risk
- Past Experiences
- Design - Business Continuity Strategy to maximize operational resilience.

Analyzing the results

- Review and Interview Notes
- Implement Risk Management Control Program – where proposed solutions are easily implemented
- Follow-Up Meetings - of management and departments related for other solutions the decision on what to do and when to do it
- Look for an economic balance between the impact of each risk and the cost of security solutions intended to manage it.
- Report the Results - Each departmental business impact analysis/risk assessment team is expected to complete a report that can be easily shared with those parties involved in the process

Final Report & Presentation

- **Presenting the Results**-The departmental business impact analysis/risk assessment team will meet as needed to review what work has been accomplished and to discuss specific strategies. This review will be determined by actions taken or a possible major change in technology. The team should record what has been done to address specific risks and maintain for a "year-ending" report to management.

- **Next Steps** - This report and presentation can also be used to address new issues and to consider if any risks might need to be discussed on a organization -wide basis.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Conclusion

Risk assessment is important tool to protect human resources and business of the organization; it should be reviewed on an ongoing basis and kept up to date and effective.