

In today's competitive world, no prudent management can afford to ignore business interruptions, be it a short one or a long one. Increasingly, businesses are getting dependent on IT (Information Technology), and the level of dependency obviously varies on business operations. Every business operation is threatened by a variety of risks operational, political, physical, and so on. It is practically impossible to operate businesses after eliminating all risks. Success depends on how efficiently the management perceives and manages the risks to ensure business continuity.

With many IT companies working as virtual back offices, it is important that all risks are evaluated & risk mitigation measures are carried out in the light of As Low As Reasonably Practicable (ALARP) principle. ALARP principle requires that the risk must be reduced not merely to a tolerable level but to a level which is as low as reasonably practicable.

Reality is that business operations can be disrupted, inspite of precautions, highlighting the element of 'uncertainty' in every business. An example could be the availability of alternate power source such as UPS or a diesel generator but, if the distribution feeder or panel fails due to fire, business can get interrupted. The electrical hotspot detection survey, carried out as part of the Risk assessment study can identify potential electrical hotspots in critical electrical installations. When a complex information system crashes in our networked world, the consequences could be serious triggering huge financial losses. Business interruption susceptibility of an organization depends on the kind of service that organization provides.

The backbone of business processes include use of specialized equipment such as servers, UPS systems, telecommunication equipment and customized enterprise application systems (SCM, CRM, ERP, etc.) and needs to be protected from various threats to ensure business continuity. Statistics point to the fact that large percentages of business organizations that survived major accidents were not able to successfully sustain the business, and in turn were forced to exit business.

CMSRSL engineers apply the technique of, "Semi-Quantitative Risk Ranking" (SQRR) for evaluating risks arising out of fire, electricity, lightning, smoke movement, etc. that could result in business interruptions.

RiskGuard is designed to be a powerful tool to make workplace safer by identifying and controlling potential risks.



Identification, Assessment & Control of :

Fire Risks

- ⚡ Active Fire Protection
- ⚡ Fire Hazards (office rooms, battery rooms, switch rooms, server rooms, stores, data storage room, etc.)
- ⚡ Flammability of Building Materials used

Electrical Risks

- ⚡ Lightning
- ⚡ Cable Hazards
- ⚡ Transformer fires
- ⚡ Protection Devices
- ⚡ Earthing Defects
- ⚡ Overloading
- ⚡ Electrical Hotspots
- ⚡ Electrical Shock
- ⚡ Surges / Transient
- ⚡ Emergency Power
- ⚡ Panel Fires

Occupational Risks

- ⚡ Indoor Air Quality (IAQ)
- ⚡ Lighting
- ⚡ Ventilation
- ⚡ Noise levels
- ⚡ Ergonomic Issues

Security Risks

- ⚡ Arson / Malicious Damage Possibilities
- ⚡ Access Control

External Risks

- ⚡ Natural Calamities (Flood, Storm) Riot / Strike

Construction Risks

- ⚡ Working at Height
- ⚡ Slips, Falls and Trips
- ⚡ Construction Safety Management (CSM)
- ⚡ Welding

Review & Suggestion for Improvements in :

Disaster Preparedness Plan

- ⚡ Evacuation System
- ⚡ Control of emergency
- ⚡ Emergency Communication Facility

Environment Management System

- ⚡ Waste Disposal
- ⚡ Use of ODP (Ozone Depleting Potential) materials (like CFCs, Halon, etc.)

Business Continuity Plan

- ⚡ Review to check if all BI risks are identified and controlled

Building Management System (Integrated)

- ⚡ Review to assess the integration of various systems (Fire detection / Protection), HVAC, electrical, access control, enterprise applications, etc.)

Maintenance Practices



