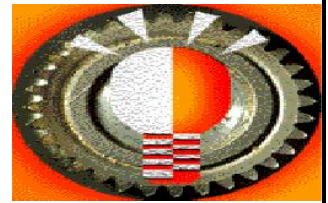
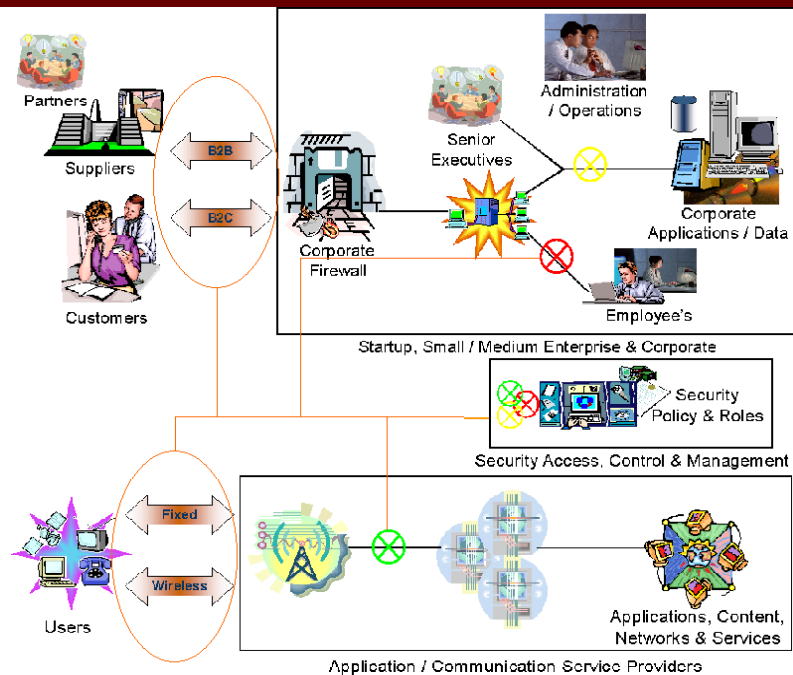


GenOmega

Achieving the Genesis and Omega



Security and Risk Management Policies



Every organization has a responsibility to protect their confidential information and information technology systems from unauthorized access and potential misuse. In general definitions, access to data and systems should be authenticated and authorized where data may be defined as corporate, customer, employee, partner and or supplier confidential information.

Australian corporations have another reason in the Australian Privacy Act of 2000, that mandates protection of confidential customer information under penalty, where relief is only available if it can be shown that due diligence and process was undertaken to protect such data. While the definition of what is confidential, who should have access, how it should be protected and policies and processes for control, management and audit are defined within an Information Technology Security Policy document.

Although Risk Management policy encompasses security, it primarily is concerned with protection and recovery of data assets in the event of a catastrophic system failure or natural disaster. Now both these sets of policies are pre-defined, contained in a single volume and available today to be tailored to your organization .

GENOMEGA

GenOmega Partners Pty. Ltd.
PO Box 144
Chimside Park, Victoria 3116
Australia

Phone: +61-3-9733-5913
Mobile: 0407 502 454
Email: Info@GenOmega.com

Although a component of our GenOmega Standard Operating Environment (SOE) framework, our Security and Risk Management Policies can be delivered individually and easily tailored to your Business or ASP / CSP Organization model.

Security Policies encompass protection of corporate and / or customer data for access control and management with establishment of audit, reporting and correction procedures. Further, they also need to cover firewall environments, virtual private networks, modem access from network attached personal computers and communications between partners, suppliers and corporate systems and employees.

Risk Management although partially concerned with security, is concerned with catastrophic system failure or natural disasters that can affect corporate operations. The absence of Risk Management policies can result in substantial losses due to prolonged interruptions in corporate operations that could last anywhere from hours to months. The definition and implementation of such policies can reduce the interruption from hours and months to minutes and small number of days, with potential total recovery of lost data and systems.

Security and Risk Management policies together, such as pre-defined and available from GenOmega today, have the potential to protect and reduce dramatically the potential of losses from misuse, indirect or direct attacks and system failures caused by hardware / software failure or natural disasters such as earthquakes, fires, floods extreme winds and other natural occurrences capable of causing interruptions to an organisations operations.

Application and / or Communication Service Providers also need to consider their responsibilities in offering hosted application or communication services. For application services, the provider has all the responsibility of any other corporate in ensuring Security and Risk Management are properly considered as well as protecting corporate data from other third party corporate users of the same service and indirect forms of attack that may originate from other components of the service or communication links associated with those component services. They also have essentially a mandate in ensuring that Risk Management policy is implemented, as they are now offering a hosted 24x7 service shared among multiple corporate customer dependent on this service for an aspect or entirety of their operations.

For Communication Service Providers, such as Internet, fixed and wireless services, there is currently some relief in consumers understanding that interruptions to services may occur. However the patience associated with this relief is not present with corporate customers and is ebbing with consumers as technology improves and matures. They must also consider Security policies around their customer information and authenticate users of their services to prevent misuse / theft. Therefore, although they require Security and Risk Management policies just like their corporate cousins, unlike their corporate cousins they are even more at risk through lawsuits and other legal proceedings when they fail to protect their customers information or deliver the quality of service as contracted.

GenOmega's pre-defined SOE Security and Risk Management Policy framework enables your business or service organisation to save months or even a year, in defining common policies from scratch and with the assistance of our experienced consultants it can be tailored to your specific needs in weeks instead of months.

Therefore contact us today for a no obligation discussion on Security and Risk Management Policy and how it applies to your organisation or for more information on other modular SOE framework documents and how they can be tailored to your specific needs in weeks rather than months or years.