EMC

The major benefit of this offering is that organizations are enabled to apply security controls appropriately according to sensitivity and criticality of information assets. Once the information classification has been established, the security controls for each level of information are defined; resources can be directed at protecting the assets with the highest value to the business first.

This service addresses the following areas:

- Sets standards across the organization for the required protection of information assets
- Apply security controls appropriately according to sensitivity and criticality of information assets
- Define appropriate security controls for each level of information
- Direct resources at protecting assets based on business value

Information Risk Assessment: This service Assessment is based on the ISO 27002 standard and emcompasses an overall assessment of governance, policy, data protection, authentication, access and other business and technical infrastructure security controls mapped to established best practices.

This service considers the following:

- Vulnerability: Where is my organization exposed to information risk?
- Threats: What threats can exploit these vulnerabilities?
- Likelihood: How likely is it a particular type of threat will occur, especially when compared to other threats?
- Countermeasures / Controls: How effective is that we have done to protect against the threats and vulnerabilities?
- Do we need to do more and if so, what should we do?
- Materiality: What will be the impact of a security breach to my organization?

Policy Driven Management: This service establishes the overall framework for driving policy management by evaluating all of the company's GRC business processes, including associated processing audit and global sourcing processes, and identifying timelines and dependencies for business processes which will be implemented within the