



Ascendant Services, Inc.

Information Protection Assessment

Overview

Are you confident that your information assets are well protected? Do you seek assurance regarding the security of your technology infrastructure and confidential information?

An Information Protection Assessment takes a management perspective to security that is understandable and actionable.

We view information as an organizational asset. Like other important assets (such as vehicles), information has value and consequently needs to be suitably protected.

We will assist you in identifying your most important information assets (i.e., confidential information about employees) and the security attributes relevant to those assets (i.e., privacy, access control, backup).

We take this knowledge and diagram the relevant components of your technology environment, emphasizing security concepts. We also interview your staff and perform site visits to gain an understanding of your environment.

In addition to our detailed findings, a summary is prepared that includes recommendations that will be understood and actionable by executive management. At the conclusion of the assessment, you will have a much clearer picture of how well your information is protected and what gaps (if any) to address.



Benefits

- Identify and understand your organization's information protection requirements.
- Gain insight into what information security techniques are relevant to your organization.
- Visually see your organization's technology infrastructure and its security posture.
- Receive an assessment of how well your organization protects its information assets.
- Understand root causes for information protection gaps.
- Have actionable initiatives to improve your information protection posture.

Methodology

Ascendant Services uses the leading, international standard for information protection – ISO 17799 – as a framework for the Information Protection Assessment. Our experienced, information security professionals will:

- Conduct interviews to identify information protection requirements and security attributes.
- Prepare a prioritized list of information protection requirements, along with a list of the most relevant 4-6 security attributes (i.e., authentication, access control, privacy, availability, etc.)
- Perform site visits, examine component configurations, and review policies & procedures.
- Prepare security diagrams that identify key technology components and their security posture.
- Document our detailed findings, including comparisons to best practices.
- Search for root causes of information protection gaps and make recommendations that are actionable by executive management.
- Prepare a summary report and/or presentation for delivery to executive management and project sponsors.



Solutions

Ascendant Services, Inc.

Creighton Grenoble

310.567.7432

info@ascendantservices.com

