



BACKUP AND RECOVERY AUDIT



The backup and restore of an organization's data is a critical function for IT groups. Unfortunately, backup and restore processes rarely evolve with IT infrastructures, leaving organizations exposed and vulnerable. This exposure is not usually recognized until it's too late.

With new legislation in the area of data retention, such as Sarbanes Oxley and new anti-trust legislation, an organization has to have formal data retention policies, including email archiving. An organization not only needs effective policies, but also it needs to demonstrate that it has the people and processes in place to enact those policies. That's where a Backup Audit can add value. A Backup Audit can help an organization assess the impact of legislation, changes in technology, backup architectures, corporate requirements and best practices and identify the risks. It helps an enterprise develop a framework for future data growth.

What is a Backup Audit?

A Kanatek Backup Audit is a comprehensive independent review of an organization's IT infrastructure and backup processes. It provides an assessment of organizational risk and develops recommendations for new backup processes. It reports on best practices in the industry and helps an organization improve backup performance, reliability, and manageability.

An external Backup Audit gives stakeholders an objective assessment of risk and exposure, and helps justify additional spend, where needed.

Why do you need one?

Not all of today's organizations are matching the growth in their data volumes with corresponding increases in their backup and recovery capabilities. Many enterprise backup systems today still amount to nothing more than a patchwork of standalone drives attached to individual servers with no centralized control. That lack of control can lead to lost data that can't be restored, which can have a serious impact on the enterprise as a whole and its IT group in particular. Kanatek assists organizations in assessing their current and future backup and recovery requirements.

A Backup Audit helps protect the organization's data and validates whether the organization is compliant with its formal policies.

How long does a Backup Audit take?

The duration of an audit depends on the size and complexity of the network and the maturity of the existing backup processes. The initial audit phase assesses the backup infrastructure. The technical consultant sits down with the organization's IT team to review existing policies. Has the organization determined which data is to be backed up? Is it compliant with local and international laws around data retention? Has it determined data restore policies and priorities? Are current off site storage practices meeting the disaster recovery or business continuity requirements? The remaining phases of GAP analysis, recommendations and implementation plans are based on Kanatek's in-depth experience in the area of backup and restore. At its minimum, an audit is a few days work.



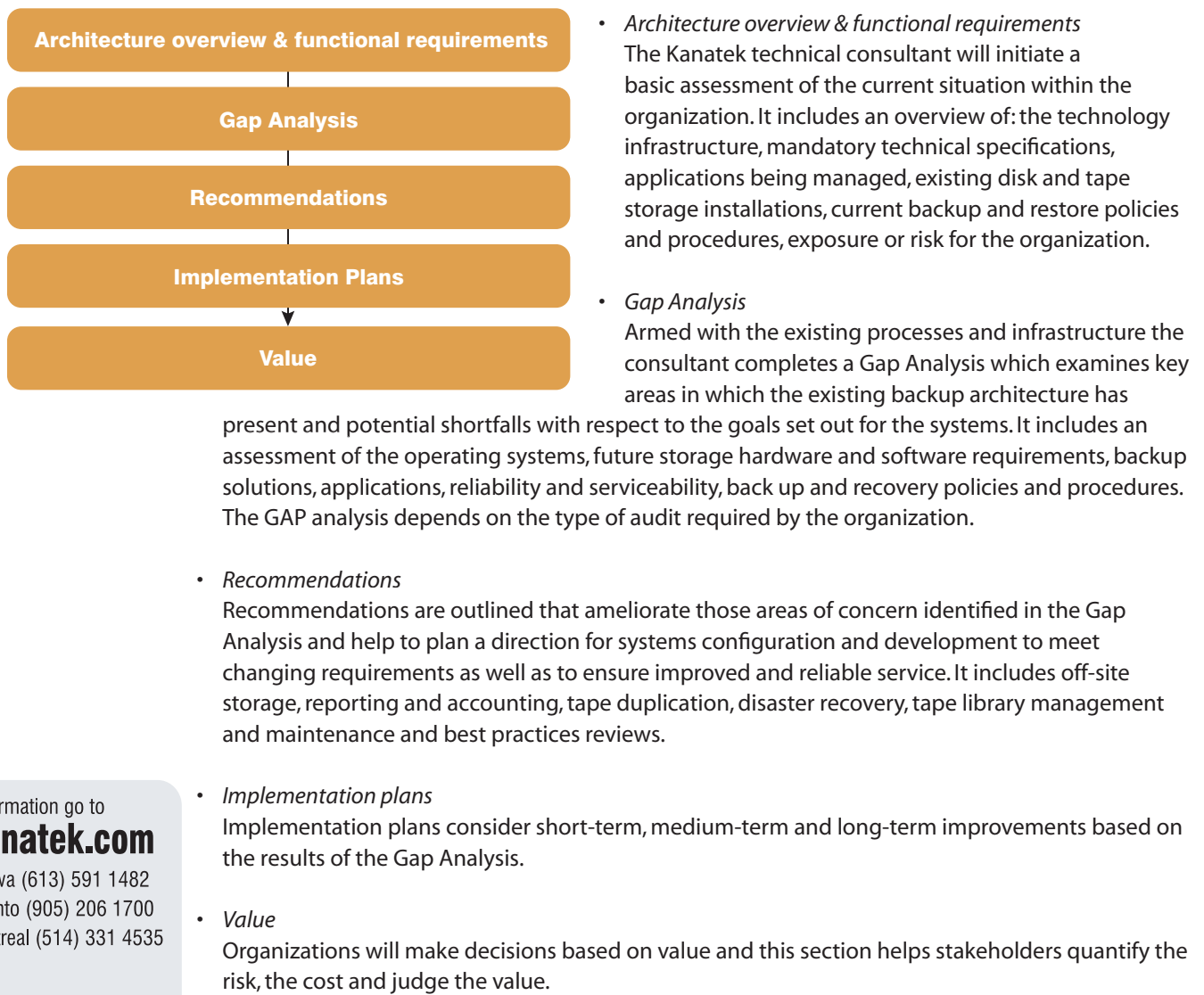
BACKUP AND RECOVERY AUDIT

Kanatek offers two types of Backup Audit, each with different objectives, depending on the needs of the organization.

1. Review and assessment of existing backup infrastructure with the objective of identifying performance gaps
2. Review of backup/restore policies and procedures to confirm organization is meeting compliancy requirements.

What does the Backup Audit report include?

There are five key sections to a Kanatek Backup Audit and the report reflects those five areas.



For more information go to

www.kanatek.com

Kanatek Ottawa (613) 591 1482
Kanatek Toronto (905) 206 1700
Kanatek Montreal (514) 331 4535