



## Your First Step in Coordinated, Defense-Oriented approach to security

Security breaches and attacks mean downtime and unwanted expense for organizations. Keeping up with the latest vulnerabilities and threats require a considerable time and effort. For this purpose Secure-Bytes provides Security Assessment Services.

SAS will provide assessment of organizations current IT security infrastructure. In this process security risks and exposures are identified within enterprise policies, processes, procedures, practices, networks, systems and applications. This gives the benefit to the Secure-Bytes customers of an outside security review of their environment which analyzes and measures their level of security versus industry standards and best practices.

### Why Secure Bytes?

#### Knowledge and Expertise

- Secure Bytes staff has more than 150 years of accumulated Information Technology Network and Security experience.
- Secure Bytes security experts hold different security certifications, such as CISSP, CISM, CISA, CCIE & CCNP.
- Secure Bytes maintains a staff of multiple network engineers.
- Secure Bytes is Microsoft, Oracle and McAfee, Partner.

### How we Differ !

- A mix methodology is utilized during assessment process
  - o For InfoSec management we use ISO 27001
  - o For Risk Assessments we use a combination of CERT OCTAVE, and ISO 13335.
  - o For application testing we adhere to the Open Source Security Testing Methodology Manual (OSSTMM).
  - o For Vulnerability Assessment we use NSA's Information Sec Assessment Methodology (IAM).
- Different tools are utilized for facilitating assessment
- Regulatory reference included in report
- Step by Step remediation recommendations included in report
- Information on new regulations and the latest examiner findings
- Secure Bytes provides easy-to-read reports with findings sorted by associated risk and cost.

## Secure Assessment

Security assessment services facilitate management to keep pace with latest security threats and vulnerabilities with minimal time, effort and highest level of specialization. It reduces chances of breach which results in reduced downtime and higher economies of scale.

SAS provides in depth appraisal of security risks associate with enterprise policies, processes, procedures, practices, networks, systems and applications. It provides a neutral security overview of an organizations security measures versus industry imposed standards and best known practices.

Some of the services offered are as follows:

- Application / File Server Vulnerability Assessment Service.
- Database Server Vulnerability Assessment Service.
- Network Architecture Assessment Service.
- Router Vulnerability Assessment Service.
- Server Vulnerability Assessment Service.
- Web Server Vulnerability Assessment Service.
- Wireless Network Vulnerability Assessment Service.
- Wired Network Vulnerability Assessment Service.

For further information:  
[sales@secure-bytes.com](mailto:sales@secure-bytes.com)

## Service Benefits

- Exact identification of exploitable configuration weaknesses.
- Segregate security risks on the basis of their potential impact and frequency of occurrence prioritize safety measures.
- Recommendations for eradication of exploitable weaknesses simplify the task of security administrators.
- Review implementation of company policies and level of difference between current policies and industry known best practices.
- Comparative reports for multiple assessments helps management to trace the level of improvement in their response and vulnerability update mechanism.
- Detailed instructions regarding methods to prevent events that threaten business continuity and increase uptime.
- Detailed and Flexible Reporting allows an organization and its members to inspect, compare and have better visibility of policy compliance.
- Customized reports in accordance with the needs and requirement of different audiences including IT staff, Executive Management and Auditors facilitate high pace decision process.