VantagePoint

Initech Security Assessment

ISO27001 Compliance

VantagePoint benchmarked the security posture of Initech's Security Program against ISO27001:2013 Information Security standard.

Security Assessment Performed by Independent Experts

This document confirms the results of the recent security assessment undertaken by Initech Solutions and performed by VantagePoint. Between the dates of September 1, 2017 and September 13, 2017, VantagePoint benchmarked the posture of Initech's Information Security program against the ISO27001:2013 information security standard. This process involved a full review of existing documentation, interviews of key stakeholders, and evaluation of the existing physical and technical security controls in place at Initech. During the assessment, a total of 91 security requirements were evaluated, 37 were not implemented, 16 were partially implemented, and 38 were fully implemented. These gaps require 31 security controls to be implemented to remediate all gaps. Each control to be implemented is given a criticality (priority) based on risk to the organization and they break down as follows: 9 are categorized as critical to security posture, 4 are high, 16 are medium, and 2 are low.

VantagePoint would like to thank Initech for this opportunity to help the organization evaluate its current security posture. We look forward to continuing to work with you to improve your security posture.

INITECH

RKotian

Rohan Kotian
Chief Executive Officer, VantagePoint
rohan@vantagepoint.co
(512) 636-7912

Issued date

NOVEMBER 22, 2017

Guided by **the internationally recognized ISO27001:2013 standard**

ISO 27001:2013

| **vantagepoint.co**

INITECH

ISO27001:2013

ISO 27001 is a specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information security management processes. ISO27001 was developed to "provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system." ISO 27001 uses a topdown, risk-based approach and is technology-neutral. There are 114 security controls specified in the stadard that are spread across 14 groups. These groups include:

Information Security Policies
Organization of Information Security
Human Resource Security
Asset Management
Cryptography
Physical Security
Operations Security
Communications Security
System Maintenance
Suppliers
Incident Management
Business Continuity
Compliance.

VantagePoint benchmarked the security posture of Initech's Security Program against ISO27001:2013 Information Security standard.

VantagePoint Grading Report Card

The grade below is a representation of Initech’s current security posture relativite to the requirements of the standard. VantagePoint calculates grades based on the number and criticality of the controls recommended in the assessment.

Security	Grade
Poor	**D**

Grade	Security	Criteria Description
A	Excellent	The overall security posture was found to be excellent with a minimal amount of low and medium level criticality controls were recommended.
B	Good	Only a handful of low, medium, and a minimum of 1 high criticality security controls were recommended.
C	Fair	The current security posture relative to the standard it was measured against is not in good condition. Multiple high criticality control recommendations were made.
D	Poor	The current security posture relative to the standard it was measured against is poor condition. Multiple critical and high criticality controls recommendations were made.
F	Inadequate	Shortcomings were identified throughout most of the security controls examined and improved security will require significant resources.

INITECH

In total, VantagePoint is recommending 31 security controls for your environment.

Guided by **the internationally recognized ISO27001:2013 standard**

ISO 27001:2013

Findings and Control Recommendations

Findings are the results of the analysis performed by VantagePoint for Initech. VantagePoint first analyzes the security posture of Initech relative to the ISO27001:2013 security standard. Based on the gaps identified, VantagePoint recommends a series of security controls to close those gaps. A single security control recommendation can cover multiple gaps, which is why there are always fewer control recommendations than gaps. There are three types of control recommendations for remediation:

Documentation - Administrative policy or procedure documentation needs to be created or updated.

Recurring Procedure - A procedure needs to be performed on a recurring basis by an analyst and results reported to management.

Technology - A piece of security technology needs to be deployed into the environment.

Your Control Recommendations

Documentation	Recurring Procedures	Technology
16	8	7

Your Critical Control Recommendations

Documentation	Recurring Procedures	Technology
3	4	2

The Top 5

Below is a list of the top 5 security controls you should consider implementing as soon as possible based on the gaps identified in our analysis.

Control	Description
Recurring Procedure - User Rights Review	The user right review is a key security component to any organization. It is the process by which an analyst will review the user access privileges in key applications to ensure that privileged users are limited, that the appropriate level of authorization is granted, and that terminated employee accounts are all disabled. This process should be performed at least twice annually.
Recurring Procedure - Data Inventory	The data inventory process is performed to ensure that all data owned or managed by the organization is accounted for and appropriately protected based on its data classification. An analyst will ensure that all data existing in the organization has a classification, is placed in an inventory, assigned an owner and location, and that all data has the appropriate security controls in place.
Technology - Log Aggregation and Event Monitoring	It is critical to the incident response function that logs for all critical applications, servers, and other systems are aggregated into a single, ideally searchable location. This ensures that in the event of a security incident, the appropriate level of logging information is available to triage, timeline, and assist in the eradication of the security threat.
Technology - Vulnerability Scanning	It is critical to the security posture of the organization that they have a full inventory of vulnerabilities and missing patches from their servers and systems. A vulnerability scanner is required to perform this activity. This scanning ensure that the IT and Security teams in the organization can appropriately prioritize and address the risks caused by the vulnerabilities that exist in the environment.
Policy - Security Policy	The organization's security policy is the single most important piece of security documentation. It spells out the principles, repsonsibilities, and rules of the organization in related to information security. All staff, management, contracted third parties, and other relevant stakeholders should have access to the security policy and abide by its requirements