

REPORT

Gap Analysis - Results

Bank - Gap Analysis

Version Date: 12.7.2011
11:16:52

Version: 1

Gap Analysis - Results

Bank - Gap Analysis

Printed On: 13/07/2011

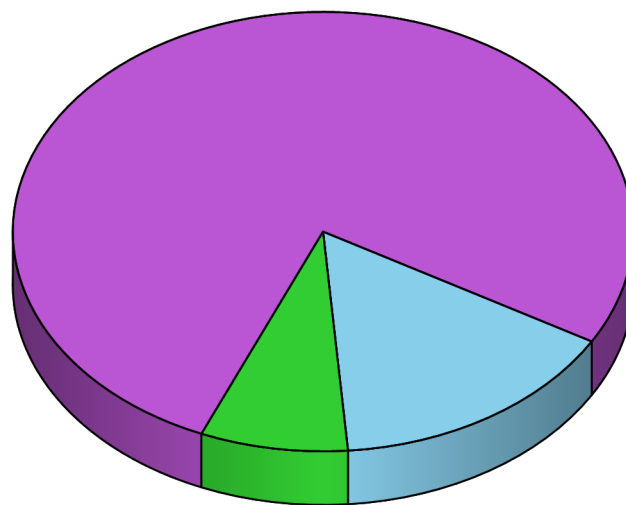
Gap Analysis - Results

Bank - Gap Analysis

According to the Standard	
ISO/IEC 27001:2005	Information Technology - Security Techniques - Information Security

Period
12/07/2011 - 12/07/2011

Ratio of Control Implementation



15.38 % - Not Implemented 7.69 % - Partially Implemented 76.92 % - Implemented

ISO/IEC 27001:2005

9 Physical and environmental security	
9.1 Secure areas	
9.1.1 Physical security perimeter	Implemented
<i>Physical obstacles and controlled entry gates have been set up around areas that require maximum security.</i>	
9.1.2 Physical entry controls	Implemented
<i>Physical entry controls have been set up around areas that require maximum security.</i>	
9.1.3 Securing offices, rooms, and facilities	Implemented
<i>Offices, rooms and facilities have been physically secured.</i>	

Gap Analysis - Results

Bank - Gap Analysis

9.1.4 Protecting against external and environmental threats	Partially Implemented
<i>There is physical protection against some threats (e.g. fire and flood) but it can be improved.</i>	
9.1.5 Working in secure areas	Implemented
<i>Physical protection and guidelines for working in secure areas have been designed and applied.</i>	
9.1.6 Public access, delivery, and loading areas	Not Implemented
<i>No actions have been taken to secure access point such as delivery and loading areas.</i>	
9.2 Equipment security	
9.2.1 Equipment siting and protection	Implemented
<i>The equipment is protected.</i>	
9.2.2 Supporting utilities	Implemented
<i>The equipment is protected from power failures.</i>	
9.2.3 Cabling security	Implemented
<i>Power and telecommunications cabling carrying data or supporting information services are protected.</i>	
9.2.4 Equipment maintenance	Implemented
<i>The equipment is correctly maintained.</i>	
9.2.5 Security of equipment off-premises	Not Implemented
<i>Off-site equipment is not sufficiently protected.</i>	
9.2.6 Secure disposal or re-use of equipment	Implemented
<i>All items of equipment containing storage media are checked prior to disposal.</i>	
9.2.7 Removal of property	Implemented
<i>All personnel are required to ask for authorization to take equipment, information or software off-site.</i>	