

REPORT

Gap Analysis - Results

Telecommunications company - Gap Analysis

Version Date: 18.7.2011
08:43:19

Version: 1

Gap Analysis - Results

Telecommunications company - Gap Analysis

Printed On: 18/07/2011

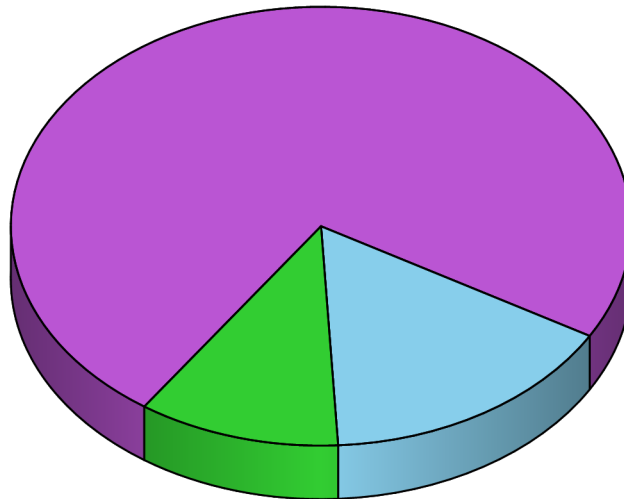
Gap Analysis - Results

Telecommunications company - Gap Analysis

According to the Standard	
ISO/IEC 27001:2005 Annex A with implementation guidance from ISO/IEC 27011	<i>Information technology – Security techniques - Information security management systems – Annex A – control objectives and controls</i> <i>Including implementation guidance from ISO/IEC 27011:2005 Information technology -- Security techniques -- Information security management guidelines for telecommunications organizations based on ISO/IEC 27002</i>

Period
18/07/2011 - 18/07/2011

Ratio of Control Implementation



15.79 % - Not Implemented 10.53 % - Partially Implemented 73.68 % - Implemented

ISO/IEC 27001:2005 Annex A with implementation guidance from ISO/IEC 27011

9 Physical and environmental security	
9.1 Secure areas	
9.1.1 Physical security perimeter	Implemented
<i>Physical barriers and controlled entry gates have been set up around areas that require maximum security.</i>	

Gap Analysis - Results

Telecommunications company - Gap Analysis

9.1.2 Physical entry controls	Partially Implemented
<i>Operation rooms and control centres to operate telecommunications facilities are protected by strong entry controls, but the visitor's information at the front desk is not protected.</i>	
9.1.3 Securing offices, rooms, and facilities	Implemented
<i>Offices, rooms and facilities have been physically secured.</i>	
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>	
9.1.7 Securing communication centres	Implemented
<i>Physical security of communication centres, where telecommunications facilities are housed have been designed, developed and applied.</i>	
9.1.8 Securing telecommunications equipment room	Implemented
<i>Physical security of equipment room, where telecommunications facilities are set for providing telecommunications business, has been designed, developed and applied.</i>	
9.1.9 Securing physically isolated operation areas	Implemented
<i>Physical security for physically isolated operating areas, where telecommunications facilities are located for providing telecommunications business, has been designed, developed and applied.</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>	

Gap Analysis - Results

Telecommunications company - Gap Analysis

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	Not Implemented
<i>All personnel are required to ask for authorization to take equipment, information or software off-site.</i>	
9.3 Security under the control of other party	
9.3.1 Equipment sited in other carrier's premises	Implemented
<i>When telecommunications organizations install equipment outside of their own premises, the equipment is sited in a protected area.</i>	
9.3.2 Equipment sited in user premises	Implemented
<i>When telecommunications organizations install equipment within the telecommunications service customer premises, the organizations' equipment is protected.</i>	
9.3.3 Interconnected telecommunications services	Implemented
<i>In the provision of interconnected telecommunications services, the telecommunications organizations specify a well-defined boundary and interface with other telecommunications organizations, so that each organization may be partitioned and isolated in a timely manner in order to evade an identified risk.</i>	