

Audit Program – Remote Access Security

The remote access security audit will consists of the following 3 phases:

DESCRIPTION	
<p>Phase 1</p> <p>□ Internet Scanner</p> <ul style="list-style-type: none"> • Obtain a clear understanding of the capabilities of Internet Scanner and its application within the XYZ environment with particular reference to remote access security and the identification of modem lines. • Identify the subnet and IP address range that can be found on the XYZNet. • Identify some order of priority or importance for the various IP address ranges resident on the XYZNet (e.g. all hosts on the XYZ backbone or within the DMZ). • Start by performing a Level 1 Inventory scan of these critical IP address ranges in order to identify any unauthorised hosts residing thereon. • Analyse the results generated by a Level 1 Inventory scan in terms of the following: <ul style="list-style-type: none"> • Unauthorised hosts, • Operating system of hosts, • Abnormalities, • Standard vulnerabilities. • Report on the results of the Level 1 Inventory scan. 	<p>P1 WP1</p> <p>P1 WP2</p> <p>P1 WP2</p> <p>P1 WP3</p> <p>P1 WP3</p> <p>P1 WP3</p>

Phase 2

□ REMOTE ACCESS

DIAL-UP REMOTE ACCESS

IMPLEMENTATION

Identification

- Perform an inventory of the dial-up remote access devices and components that are connected to the XYZ network infrastructure (XYZNet):
 - Dialup client software,
 - Access servers (NAS/RAS),
 - Authentication software,
 - Centralised single remote access database.
- Identify the following properties for each of the dial-up remote access devices located within the XYZNet:
 - Functional operation, (device/operating system),
 - Platform – Windows NT/Unix,
 - Risk versus Cost,
 - Physical and logical location.

**P2
WP1-2**

**P2
WP1-2**

Dial-up remote access Technology and Architecture

- Identify the following dial-up remote access security features:
 - Firewall technologies,
 - Authentication,
 - Authorisation,
 - Accounting,
 - Encryption.
- Identified the protocol used to connect remote users to the XYZNet.
- If a Point-to-Point Protocol is being used, evaluate the authentication method being supported e.g. PAP (Password Authentication Protocol) vs CHAP (Challenge Handshake Authentication Protocol).
- Evaluate the dial-up remote access process in terms of dial-in and dial-out services.
 - Single dial-in point (single large modem pool or access server),
 - Identify the set of modems used for dial-in and dial-out services,
 - Identify whether or not dial-in and dial-out servers are authenticated,
 - Identify whether the call-back is supported within the dial-up remote access environment,
 - If call-back is applied within the dial-up remote access infrastructure, assess and evaluate the call-back controls currently in place.

**P2
WP3-4**

P2 WP5

P2 WP6

**P2
WP7-8**

<p>Organisation and management policies</p> <ul style="list-style-type: none"> • Ascertain the effectiveness and adequacy of physical security for the dial-up remote access infrastructure. • Ascertain the effectiveness and adequacy of logical access control measures for the dial-up remote access infrastructure: <ul style="list-style-type: none"> • Password controls, • Changes in employment and job responsibilities. • Monitoring, recording and reporting controls for security violations. • Evaluate and assess the adequacy as well as compliance with XYZ's Remote Access Security policy. • Identify the effective utilisation of the Shiva architecture used for managing the security policy applied in ensuring: <ul style="list-style-type: none"> • High performance, • Scalability, • Centralised control. • Evaluate the adequacy and efficiency of the controls currently in place to prevent the bypassing of the Shiva authentication mechanisms when accessing the XYZNet by means of: 	<p>P2 WP9-10</p> <p>P2 WP11-14</p> <p>WP11-12 WP13 WP14</p> <p>P2 WP15-17</p> <p>P2 WP 18</p> <p>P2 WP 19</p>
<p>□ Wardialling</p> <p>The process of identifying all remote access to the XYZNet via modem. Initially this process would be confined to the MegaWatt Park environment however a review of the modem connections in the other areas will be carried out at a later stage or may be incorporated within the current audit as an extension of the scope.</p> <ul style="list-style-type: none"> • Select appropriate software or techniques used to identify modem lines by performing wardialling. • Install and perform initial tests to assess the viability and adequacy of the software. • Apply the software within the XYZNet environment to identify all modem lines. • Obtain an authorised and approved list of modem lines within the XYZNet. • Compare the identified list of modem lines through wardialling with an authorised list of lines. 	<p>P2 WP19</p>
<p>MANAGEMENT</p> <p>Business continuity</p> <p>Identify and evaluate the following:</p> <ul style="list-style-type: none"> • Regular and effective reviews of the dial-up remote access capacity and the availability of adequate technical support to ensure the uninterrupted reliable operation of the dial-up remote access. • The establishment of appropriate policies and procedures to ensure the effective handling and protection of dial-up access configuration data. • The establishment of procedures in ensuring the secured continuity of operations in the event of a disaster or failure (DRP) to the dial-up remote accesses infrastructure. • Identify whether some or other type of intruder detection software has been implemented within the dial-up remote access infrastructure. 	<p>P2 WP20</p> <p>P2 WP21</p> <p>P2 WP22</p> <p>P2 WP23</p>

<ul style="list-style-type: none"> • The effectiveness of change management in ensuring that all changes to dial-up remote access security mechanisms is valid, authorised, approved and planned. 	<p>P2 WP24</p>
<p>OPERATIONS</p> <ul style="list-style-type: none"> • Evaluating whether dial-up remote access device/component logs are recorded and consolidated into statistics that is analysed, generated and printed utilising reporting and event-analysis applications. • Establish users with dial-up remote access. • Establish the frequency of utilisation of the dial-up remote access accounts. • Identify duplicates on the dial-up remote access database in terms of: <ul style="list-style-type: none"> • Duplicate accounts, • Duplicate unique numbers. 	<p>P2 WP25 26</p> <p>“</p> <p>“</p> <p>“</p> <p>“</p> <p>“</p>

<p>THIRD PARTY REMOTE ACCESS</p>	
<p>IMPLEMENTATION</p>	
<p><i>Identification</i></p>	
<ul style="list-style-type: none"> • Perform an inventory of the third party remote access devices and components that are connected to the XYZ network infrastructure (XYZNet): <ul style="list-style-type: none"> • Dialup client software, • Access servers (NAS/RAS), • Authentication software, • Centralised single remote access database. 	<p>P2 WP27</p>
<ul style="list-style-type: none"> • Identify the following properties for each of the third party remote access devices located within the XYZNet: <ul style="list-style-type: none"> • Functional operation, (device/operating system), • Platform – Windows NT/Unix, • Risk versus Cost, • Physical and logical location. 	<p>P2 WP27</p>
<p><i>Technology and Architecture</i></p>	
<ul style="list-style-type: none"> • Identify the following critical third party remote access security features: <ul style="list-style-type: none"> • Firewall technologies, • Authentication, • Authorisation, • Accounting, • Encryption. 	<p>P2 WP28</p>
<ul style="list-style-type: none"> • Evaluate the third party remote access process in terms of dial-in and dial-out services. <ul style="list-style-type: none"> • Single dial-in point (single large modem pool or access server), • Identify whether or not dial-in servers are authenticated, • Identify whether the call-back is supported within the third party remote access environment, • If call-back is supported, assess and evaluate the call-back controls currently in place. 	<p>P2 WP29</p>
<p><i>Organisation and management policies</i></p>	
<ul style="list-style-type: none"> • Ascertain the effectiveness and adequacy of physical security for the third party remote access infrastructure. 	<p>P2 WP30-31</p>
<ul style="list-style-type: none"> • Ascertain the effectiveness and adequacy of access control measures for the third party remote access infrastructure: <ul style="list-style-type: none"> • Computer access controls, • Changes in employment and job responsibilities, • Monitoring, recording and reporting controls for security violations. 	<p>P2 WP32-35</p> <p>P2 WP32-33</p> <p>P2 WP34</p> <p>P2 WP35</p>
<ul style="list-style-type: none"> • Evaluate and assess the adequacy as well as compliance with the XYZ's Third Party Security Access policies. 	<p>P2 WP36-39</p>

<ul style="list-style-type: none"> Identify the effective utilisation of the Firewall / Shiva architecture used for managing the security policy applied and ensuring: <ul style="list-style-type: none"> High performance, Scalability, Centralised control. 	<p>P2 WP40</p>
<p>MANAGEMENT</p>	
<p><i>Business continuity</i></p>	
<p>Identify and evaluate the following:</p>	
<ul style="list-style-type: none"> Regular and effective reviews of the third party remote access capacity and the availability of adequate technical support to ensure the uninterrupted reliable operation of the third party remote access. 	<p>P2 WP41</p>
<ul style="list-style-type: none"> The establishment of appropriate policies and procedures to ensure the handling and protection of third party remote access configuration data. 	<p>P2 WP42</p>
<ul style="list-style-type: none"> The establishment of procedures in ensuring the secured continuity of operations in the event of a disaster or failure (DRP) to the third party remote accesses infrastructure. 	<p>P2 WP43</p>
<ul style="list-style-type: none"> Identify whether some or other type of intruder detection software has been implemented within the third party remote access infrastructure. 	<p>P2 WP44</p>
<ul style="list-style-type: none"> The effectiveness of change management in ensuring that all changes to third party remote access security mechanisms is valid, authorised, approved and planned. 	<p>P2 WP45</p>
<p>OPERATIONS</p>	
<ul style="list-style-type: none"> Evaluated whether the third party remote access logs are recorded and consolidated into statistics that are analysed, generated and printed utilising reporting and event-analysis applications. 	<p>P2 WP46</p>
<ul style="list-style-type: none"> Established the users with third party remote access. 	<p>“</p>
<ul style="list-style-type: none"> Established the utilisation frequency of third party remote access. 	<p>“</p>