



Security Assessment Report

Disclosure Scotland - Glasgow

Produced for British Telecommunications



Version: 1.0 DRAFT

Date: 29 March 2018 CHECK Team Leader:

CHECK Ref: 10591



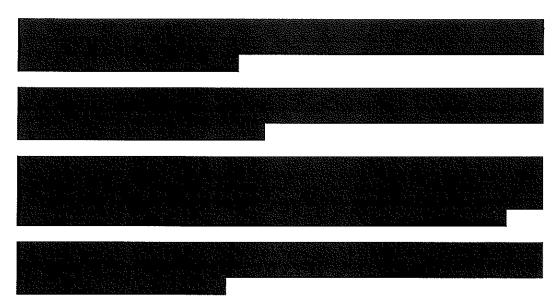
Meanagean can Respond

Introduction

This report details the findings and recommendations from an IT Security Assessment conducted by Digital Assurance (DA) for British Telecommunications (BT) in March 2018. The security assessment was conducted against the Disclosure Scotland - Glasgow systems under the terms of the NCSC CHECK scheme.

It is important to bear in mind that security assessment reports such as this are exception-based reports and as such generally document identified security flaws rather than identifying security controls that may have performed well.

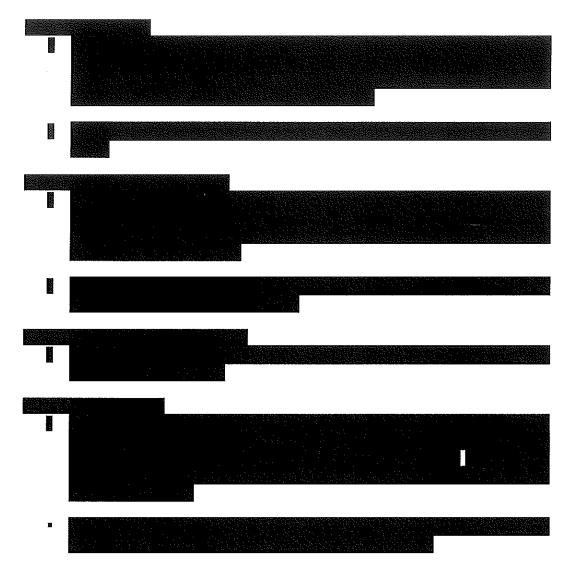
Summary



- Willing ability				REGRAME		
Rootscause	Trotal	Critical	High	Moderate	Low	Info
All Categories	44		8	16	19	1
Application Software	6				5	1
Database Configuration		S 2 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1				
Host Configuration	13		2	2	9	6 016 1 500
Firewall Configuration	3			1	2	-
Infrastructure Design =	-				- -	
Password Policy	1	a significant		1		Single Service
Patch Management	16		5	10	1	
Other	5	-	1	2	2	5 E 10 <u>.</u> 0015

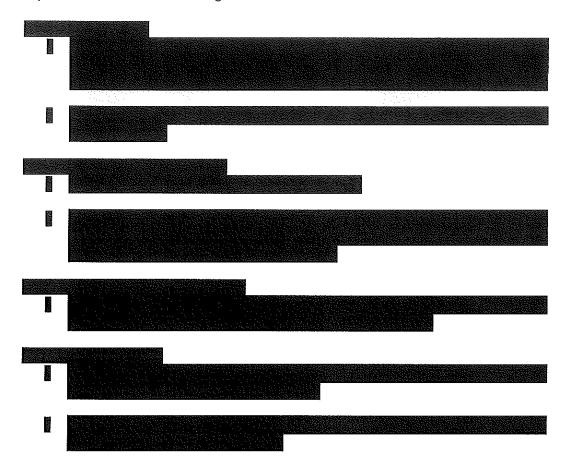
Key Findings

The most significant security issues identified during this assessment are summarised here, additional detail is provided in the 'Technical Summary' component of this management report and the 'Detailed Findings and Recommendations' section of this document.



Key Recommendations

Suggested remedial actions for the key security issues are summarised here, additional detail is provided in the 'Detailed Findings and Recommendations section of this document.



Summary of findings

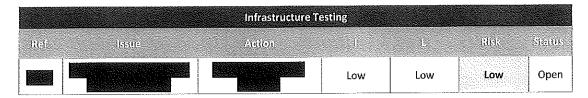
The findings of the assessment are summarised below alongside the current status of each finding at the time of report issue.

		Infrastructure	Testing			
1स्य	lesue	Action			Rick	Steller
			High	Moderate	High	Open
			High	Moderate	High	Open
			High	Moderate	High	Open
			High	Moderate	High	Open
			High	Moderate	High	Open
			High	Low	Moderate	Open
			High	Low	Moderate	Closed
			High	Low	Moderate	Open
			High	Low	Moderate	Open
			Moderate	Moderate	Moderate	Open
			Moderate	Moderate	Moderate	Open
			High	Low	Moderate	Open
			Moderate	Low	Low	Open
			Moderate	Low	Low	Open
			Moderate	Low	Low	Open
			Moderate	Low	Low	Open
			Moderate	Low	Low	Open

		Infrastr	ucture Testing			
Rel	ilgania erroria. T	Associa				Steine
			Moderate	Low	Low	Open
			Moderate	Low	Low	Open
			tion Security Review			
Ref	Estr:	Accion			flek	Sinns B
			High	Moderate	High	Open
			Moderate	Moderate	Moderate	Open
			High	Low	Moderate	Open
			High	Low	Moderate	Open
			High	Low	Moderate	Open
			High	Low	Moderate	Open
			Moderate	Moderate	Moderate	Open
			High	Low	Moderate	Open
			Moderate	Low	Low	Open
			Moderate	Low	Low	Open
		Firewall Configur	ation Security Review			
- Régi	lestre	A(q)(e) ₁			HILL	Sienes
			Moderate	Moderate	Moderate	Open
			High	Low	Moderate	Open
			Moderate	Moderate	Moderate	Open
			Low	Low	Low	Open
		AN THE SECOND	Moderate	Low	Low	Open

OFFICIAL SENSITIVE

British Telecommunications Disclosure Scotland - Glasgow



Web Application Testing						
Ref	lissue	Adim	T.	or more real series.	Risk	36106
			High	Moderate	High	Open
			High	Moderate	High	Open
			Moderate	Low	Low	Open
			Moderate	Low	Low	Open
			Low	Low	Low	Open
			Low	Low	Low	Open
			Low	Low	Low	Open
			Moderate	Low	Low	Open
			Information	Information	Information	Open

Diejaungenji (Sejajene)

Ratakane	DYAH631537/
Vielisla)	1.0 DRAFT
Complified Britis	29 March 2018
LapidUnings	13 April 2018
Buoteedire/Meddalle	OFFICIAL SENSITIVE
/Author	
Attilicordsaction	



CHECK	NCSC	03
	British Telecommunications	02
Electronic Copy	Digital Assurance	01
Name	Фиданівафон	Gopy Number

Table 2: Document distribution

Version History

Diglice	Алінов	V(eksijaja)	Reason for Update
29/03/2018		DRAFT v0.1	Document created
09/04/2018		DRAFT v0.2	Review and QA
11/04/2018		DRAFT v0.3	QA Amendments
13/03/2018		DRAFT v1.0	Release

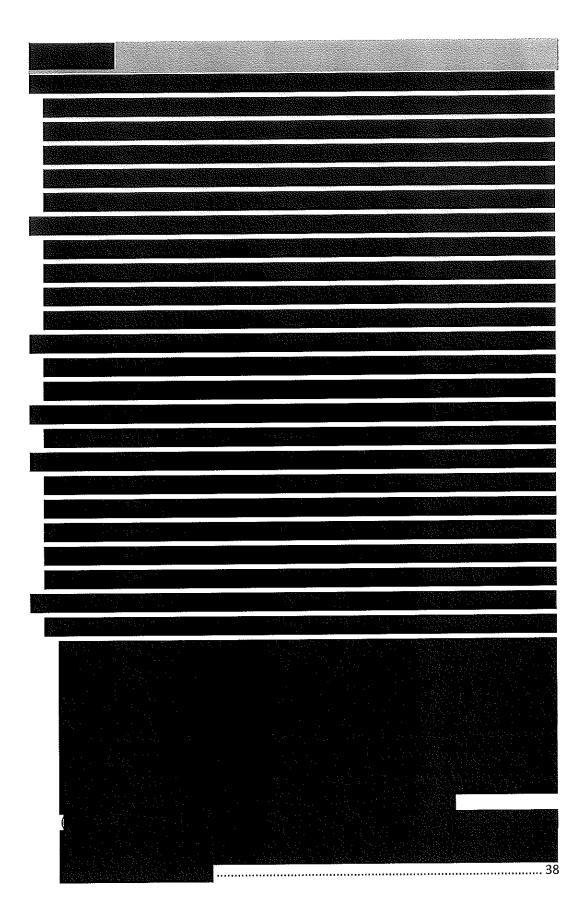
Table 3: Document version history

Confidentiality and Copyright

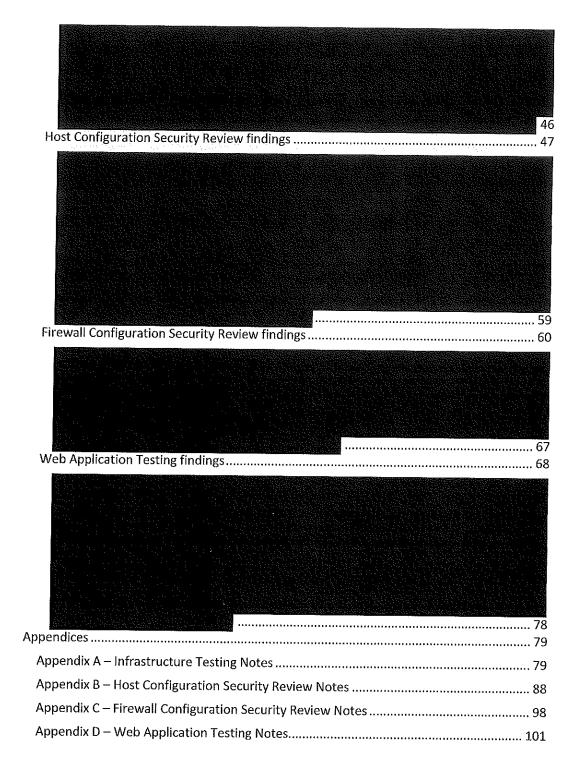
The information contained in this report is confidential and is submitted by Digital Assurance Consulting Ltd (Digital Assurance) on the understanding that it will be used only by the Staff and, where relevant, suppliers of British Telecommunications. In particular, the contents of this document may not be disclosed in whole or in part to any other party without the prior written consent of Digital Assurance.

Validity of Information

Digital Assurance has made every effort to ensure that all statements and information contained herein are accurate however it should be noted that the results of security testing reflect the systems as they were at the time of the testing and as such represent a 'snapshot' of the systems during the assessment.







Using This Report

This report is intended to provide details of the findings and recommendations arising from information security assessment activities (e.g. penetration testing, systems review or application security testing) conducted by Digital Assurance.

The report is designed to communicate important and sensitive information regarding security issues to both technical and non-technical staff with a requirement to know details or particular aspects of the security assessment findings.

Report Structure

The report is split into a number of sections to maintain structure and enhance readability as follows:

Introduction	This section contains background information regarding the parties, nature of the engagement as well as a brief overview of Digital Assurance security assessment services.
Scope	This section of the report details the objectives of the assessment with regard to type of testing performed and target systems/networks for the assessment. The scope section also documents any constraints and limitations in place during the testing.
Approach	This section outlines the overall approach taken to undertaking the security assessment
Detailed Findings and Recommendations	This section of the report provides detail on each individual issue identified during the assessment along with affected components, risk description, impact, likelihood and risk ratings along with a recommendation and estimated effort to implement recommendations. Often, detailed issues will reference appendices or external files especially where supplementary data is provided or where issues are broken down further into sub-issues.
Summary and Conclusion	This section summarises and consolidates the recommendations arising from the technical testing. Where appropriate, recommendations are provided that address the root cause of identified issues rather than to simply tackle each issue as a discrete fix. The aim is to provide recommendations that prevent re-occurrence of the issues.
Appendices	Appendices generally contain further technical details and often provide a level of detailed information on systems or

vulnerabilities identified that would be inappropriate for the main detailed findings section.

Presentation of Issues and Findings

Issues are presented in a common format to aid readability and assist the client in prioritising issues and, importantly, prioritising remedial action where necessary. The common issue presentation format contains a number of fields describing the nature of the issue, risk and recommendation as follows:

Reference	Unique identifier for the issue. Every issue in every Digital Assurance report you receive will be assigned this unique identifier which aids issue tracking.
Title	Short form title summarising the security issue
Testing phase	Documents from which phase of the testing the issue originated. This may be External testing, Internal testing, DMZ testing etc.
Impact rating	A rating of the likely impact resulting from a successful attack or exploitation of the issue. Ratings run Low, Moderate, High and Critical. An additional category of Info
Likelihood rating	A rating of the likelihood of a successful attack, this incorporates parameters such as availability of exploit code, complexity of attack and compensating controls/mitigating factors. Ratings run Low, Moderate and High.
Risk rating	An overall rating of the 'technical risk' posed by the issue. This is generally decided by both the impact and the likelihood although it is subject to modification based on other factors considered by the security assessor. Ratings run Low, Moderate, High and Critical. The rating of Information is used for informational issues.
Fix effort	A rating of the anticipated effort required to successfully perform remediation work, generally based on the recommendations made for a specific issue. This rating is highly subjective but is based on the security assessor's experience of similar issues and organisations. Ratings run Low, Moderate and High. This can loosely be translated to man-days as follows: 1. Low: up to 1 man-day of effort 2. Moderate: up to 5 man-days of effort 3. High: over 5 man-days of effort
Issue	A description of the security issue.

OFFICIAL SENSITIVE

British Telecommunications
Disclosure Scotland - Glasgow

Affected Components	Where applicable this will detail the systems, applications or other components affected by the issue. Where an issue is prevalent throughout a large population of components this may simply state that the issue is widespread.
Risk	A description of the risk posed generally detailing the attacker type, attacker pre-requisites and the likely impact on information assets.
Recommendation	A recommendation or set of recommendations for remediation or otherwise mitigating the risks posed by the issue.
Notes	Any additional observations or other notes relating to the issue.
References	Any vendor, CVE and other references relating to the issue.

lindikordierakom.

Digital Assurance was engaged by British Telecommunications to undertake a security assessment of the Disclosure Scotland - Glasgow systems and associated infrastructure. The assessment was performed in March 2018 and consisted of 4 phases of technical assessments as summarised below:

- Infrastructure Testing
- Host Configuration Security Review
- Firewall Configuration Security Review
- Web Application Testing

All security testing was performed at BT Disclosure Scotland Newcastle (CTE) and Glasgow (PQ) by

of Digital Assurance between Monday 05

March and Wednesday 28 March 2018.

About Digital Assurance

Digital Assurance is a London based security consultancy delivering a range of security assessment, secure design and security training services. Digital Assurance was founded in 2006 by experienced and well-respected security consultants who have been delivering information security and assurance services to UK and international clients for over a decade.

Our security assessments are generally highly tailored to customer requirements and are designed to provide the greatest level of assurance for a given amount of time and budget.

Digital Assurance is a UKAS accredited ISO9001:2008 organisation. Digital Assurance is an NCSC CHECK scheme subscriber and authorised to conduct testing on government systems under the terms of the CHECK scheme.





Statelete

The scope of work is documented in this section of the report for each stage of the assessment and where relevant will reference external scope documents.

The scope of work was agreed between Digital Assurance and British Telecommunications and is detailed in the Terms of Reference (ToR) document associated with this security assessment.

BT Disclosure Scotland - Glasgow

Infrastructure Testing

PQ Ops	VLANS
VIAN ID Network Range	Network Label
	Log Collect Production
	Log Collect Management
	HP Openview
	VPN1
	VPN2
	VPN3
	VPN4
	Mail
	IL4 Management
	Infrastructure Services
	Infrastructure Services Management
	Infrastructure Services SAN
	Nokia Firewall Management
	Infrastructure Services Private
	Terminal Services
	Hyper-V SAN
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Hyper-V Infrastructure Services
	Internet Data
	Network Management
PQ Suppo	
VLANID Network Range	Network Label
	Database
	RAC Cluster 1 Private
	RAC Cluster 2 Private
A Shaka a	Internet Presentation Back
	Internet Presentation Management
	Database Management
	Application
	Application Private
	Application Management

		MIS
100000000000000000000000000000000000000		MIS Private
		MIS Management
		Intranet Proxy
		Intranet Presentation Front
		Intranet Presentation Back
		Internet Proxy
		Internet Presentation Front
		Intranet Presentation Management
		MPX SAN
		IL3 iLO
		IL4 ILO
		PQ Live VLANS
WIVA	Malen	ork Ronge Network Label
		IL3 ILO
		IL4 ILO
	****	MIS
		MIS Private
100 V S	200	MIS Management
		MIS SAN
	and a manager of a conference of the conference	HPOV RAC Cluster Private
		Database Management
		Database
		Application Management
		Application SAN
		Application
		Mail Gateway Management
		Mail Gateway
		Terminal Services - Live
		RAC Cluster 1 Private - De-scoped
		RAC Cluster 2 Private - De-scoped
		Application Private
		Internet Presentation Back
		Print and Scan DMZ
named and the second		Intranet Proxy
		Intranet Presentation Front
**************************************		Intranet Presentation Back
		Hyper-V Infrastructure Services
		Pacific Quay Standalone Management
		Pacific Quay Standalone IL4
		Pacific Quay Standalone terminals
		Internet Proxy
		Internet Presentation Front
		Internet Mail Gateway Management
		Internet Mail Gateway