

Generic Unix Security Standard

Generic Unix Security Standard

Published 16 May 2009

Copyright © 2001, 2002, 2003, 2009 Frank O'Dwyer

This document specifies generic technical security policy.

This standard contains 110 baseline controls, and 2 above baseline controls, for a total of 112 controls.

Important

All of these Security Standards and Security Policies are copyrighted. THEY ARE NOT IN THE PUBLIC DOMAIN. They are however distributed under a liberal open-source license, see Publishing these Security Standards and Policies.

Table of Contents

1. Introduction	1
1.1. Objectives	1
1.2. Scope	1
1.3. Not In Scope	1
1.4. Giving Feedback	1
1.5. Publishing these Security Standards and Policies	1
1.6. Related Documents	2
1.6.1. Generic Security Standards	2
1.6.2. Operating System Security Standards	2
1.6.3. Database Security Standards	3
1.7. Definitions	3
2. User Configuration	4
2.1. Default Accounts	4
2.1.1. Change default account passwords	4
2.1.2. The synch account must not be disabled or password protected	4
2.1.3. The nobody account should own no files on any of the systems filesystems	5
2.2. Roles, Views, and Access Control	6
2.2.1. Access to /dev/kmem must be restricted	6
2.2.2. Do not rely on access control lists on NFS file systems	6
2.2.3. Avoid changing permissions on objects with access control lists using a numeric chmod	7
2.2.4. Any filenames beginning with a period . must not be everyone or group writable/readable.	7
2.2.5. If a tape drive is used for backup ensure this device is not everyone readable ..	8
2.3. Privileges	9
2.3.1. at access should be restricted using at.allow	9
2.3.2. User UIDs must be greater than 20	9
2.3.3. Suid shell scripts should not be used	10
2.3.4. The use of the su command should be with the hyphen (-) qualifier	11
2.3.5. The alias file should be reviewed to ensure all redirection entries are users ..	12
2.3.6. root should only be logged into using su	12
2.3.7. Use the wheel group if possible	13
2.3.8. Users must have individual UIDs	14
2.3.9. Mount any foreign filesystems as NODEV	14
2.3.10. The write program should be set to SGID tty and not SUID root	15
2.3.11. cron access should be restricted using cron.allow	16
2.4. Authentication/Password Configuration	16
2.4.1. Implement a login failure retry interval of 3 seconds where possible	16
2.4.2. Autologout of idle users should occur after 1 hour	17
2.4.3. Do not permit the use of control characters in passwords	18
3. Security Compliance	19
3.1. Security Compliance Checking	19
3.1.1. Hidden files should be sought out and investigated	19
3.1.2. Reports should be produced and reviewed for access outside of normal hours ..	19
3.1.3. syslog.conf must be monitored for all alterations	20
3.1.4. All new su programs should be identified and validated	21
3.1.5. grpck should be run regularly	21
3.1.6. Reports should be produced and reviewed for multiple login failures from a single source	22
3.1.7. pwck should be run regularly	23
3.1.8. Security monitoring software should be installed and used	23
3.1.9. Reports should be produced and reviewed for multiple login failures	24
3.2. Security Management	25

3.2.1. Aliases should be created for all non-user accounts to redirect to the admin ..	25
4. Network Security Configuration	26
4.1. Network Interface Considerations	26
4.1.1. The ftp home directory should be owned by root	26
4.1.2. PPP must not be installed on the system	26
4.1.3. .rosts files must not be used	27
4.1.4. The systat service should be commented out of the inetd.conf file	28
4.1.5. SLIP must not be installed on the system	28
4.1.6. The ftp entry in the password file should contain an invalid password and refer to a non-existent shell	29
4.1.7. Disable anonymous ftp if possible	30
4.1.8. root must be used to run all crontab scripts as user UUCP. The scripts must be owned by root.	30
4.1.9. The /etc/inetd.conf should be owned by root.	31
4.1.10. rexecd daemon should be disabled	31
4.1.11. NFS Filesystems should be exported nosuid	32
4.1.12. Anonymous ftp should prevent overwrite by guests or anonymous users	33
4.1.13. Entries in an NFS exports file must be comprised of fully qualified hostnames	33
4.1.14. The ftp home directory should have permissions of 555	34
4.1.15. The fingerd daemon should be disabled by commenting out the finger entry in inetd.conf.	34
4.1.16. The permissions on the /etc/inetd.conf should be 644	35
4.1.17. The /etc/hosts.equiv should contain the fewest number of trusted hosts	36
4.1.18. Ensure /etc/ftputers contains default vendor and system accounts that should not require ftp access	36
4.1.19. Reverse lookup should be used for anonymous ftp connections	37
4.1.20. The /etc/hosts.equiv should be removed unless required	38
4.1.21. There should be a mail alias to redirect mail from the UUCP account using the aliases file	38
4.1.22. Anonymous ftp should prevent rename by guests or anonymous users	39
4.1.23. Inetd.conf must be monitored for all alterations	40
4.1.24. The tftp home directory should not permit write access	40
4.1.25. Ensure that the ftp daemon is the most recent	41
4.1.26. No SUID/SGID bits should be set on UUCP component programs.	42
4.1.27. The rcp daemon should be disabled unless required	42
4.1.28. Ensure /etc/ftputers is in place to deny users ftp access that do not require it	43
4.1.29. The ~ftp/etc/passwd file should be owned by root	43
4.1.30. UUCP if required should be configured to only allow remote file retrieval from particular directories	44
4.1.31. tftp should be disabled unless the system serves X-terminals	45
4.1.32. Anonymous ftp should prevent setting of umask by guests or anonymous users	45
4.1.33. UUCP Callback should be enabled	46
4.1.34. The /etc/hosts.equiv should contain no hyphens or plus signs	47
4.1.35. The /usr/lib/uucp/L.sys file must not allow group or everyone read access ..	47
4.1.36. rdist should be used as a more secure means of performing file transfers	48
4.1.37. Disable sendmail if it is not required	48
4.1.38. The /etc/hosts.equiv should be owned by root	49
4.1.39. UUCP account should be password protected if present	50
4.1.40. If NFS is used, all available patches should be applied.	50
4.1.41. The ~ftp/etc/passwd file permissions should be set to 444	51
4.1.42. The UUCP subsystem should be removed unless it is required	51
4.1.43. The /etc/hosts.equiv should contain no trusted users	52
4.1.44. The home directory of the ftp user account must not contain a .forward file ..	53
4.1.45. Ensure that the ftp daemon is started up with the -l qualifier	53
4.1.46. The home directory of the ftp user account must not contain a .rhosts file ..	54
4.1.47. The ~ftp/etc/passwd file must not contain the entries from the real password ..	54

file	55
4.1.48. The rsh daemon should be disabled unless required	55
4.1.49. NFS exports file must not contain an entry for localhosts	56
4.1.50. Users \$HOME directories must not contain any .netrc files	57
4.1.51. The ~ftp/usr/bin directory and its equivalents should not contain CLIs or other system commands	57
4.1.52. Telnet should be disabled unless required	58
4.1.53. The rlogin daemon should be disabled unless required	58
4.1.54. Ensure that the ftp server does not permit the execution of the site exec command	59
4.1.55. Do not export a system owned file system	60
4.1.56. No UUCP files or directories should permit everyone write access	60
4.1.57. Ensure that all patches available for sendmail have been applied	61
4.1.58. Anonymous ftp should prevent deletion by guests or anonymous users	61
4.1.59. The /etc/exports file should be owned by root	62
4.1.60. Anonymous ftp should prevent chmod by guests or anonymous users	63
4.1.61. The tftp daemon should be started up with the -s qualifier	63
4.1.62. The ftp daemon must deny access to user accounts whose shell is not found as a valid shell in /etc/shells	64
4.1.63. Export NFS filesystems read only wherever possible	65
5. Configuration	66
5.1. Files and File Permissions	66
5.1.1. .plan and .project files in users \$HOME directory should be kept empty	66
5.1.2. The wall command should be denied from non-administrative users	66
5.1.3. The permissions on the /etc/hosts.equiv should be 755	67
6. Installation	69
6.1. Setup Choices	69
6.1.1. Fsirand should be run once following commissioning	69
6.1.2. Do not install Unix as "Dual Universe"	69
7. Auditing and Monitoring	71
7.1. Events to be audited	71
7.1.1. The sulog should record both successful and unsuccessful su attempts	71
7.1.2. Lastlog should be enabled for all users	71
7.1.3. Events for logging to syslog should be enabled for auth, daemon and cron messages.	72
7.1.4. Events logged to the syslog should be written to a physically secure line printer as well.	73
7.1.5. The sulog contents should be recorded in both the sulog itself and written to a physically secure line printer	73
7.1.6. Loginlog should be used to identify potential breakin attempts	74
7.1.7. wtmp file should be regularly archived	75
8. Other	76
8.1. The file L.cmds should be empty	76
8.1.1. Standard	76
8.1.2. Detailed Steps	76
8.1.3. Risks Addressed	76
8.2. All UUCP accounts should be added to the /etc/ftpusers account.	76
8.2.1. Standard	76
8.2.2. Detailed Steps	76
8.2.3. Risks Addressed	77
8.3. If NFS is used, it should be ensured that the UUCP configuration, programs and data are never exported	77
8.3.1. Standard	77
8.3.2. Detailed Steps	77
8.3.3. Risks Addressed	77
8.4. .procmailrc and .forward should be reviewed for illicit entries	78
8.4.1. Standard	78
8.4.2. Detailed Steps	78

8.4.3. Risks Addressed	78
8.5. Any foreign filesystems should be mounted NOSUID	78
8.5.1. Standard	78
8.5.2. Detailed Steps	78
8.5.3. Risks Addressed	79
9. Checklist	80

Chapter 1. Introduction

1.1. Objectives

The objectives of this document are:

- To specify generic security standards applicable to all IT platforms.

1.2. Scope

Controls specified in this document apply to all IT platforms.

All of the organisation's information systems will be subject to the policies specified within this generic security standard. The policies will be applied to new and existing installations.

1.3. Not In Scope

Compliance with this standard will not provide “in depth” security architecture or intelligent security design guidance to projects. As a consequence, for high impact or safety-critical business applications, additional guidance will still need to be sought from the Information Security team consultancy function.

This is a generic standard. Controls specific to particular technologies are not defined here but will be the subject of additional standards.

Compliance with this standard does not negate the need for an overall security review of a proposed application. Contact the Information Security team if you are in doubt.

1.4. Giving Feedback

Your feedback to improve this document is welcome. Please let me know of your experiences in applying the controls and guidance in this standard. Are the controls effective, easy to implement, too onerous, clear, unclear, something missing? Does an exceptional case need to be covered? Let me know. Please send your comments to frankodwyer AT netscape.net. Your comments will be used to produce better free security standards for the IT community.

I also request that you give feedback where you think the controls and guidance is correct. This will let us gauge whether or not specific controls are controversial or broadly acceptable to the community, and will help us to resolve cases where we have conflicting feedback on particular content.

1.5. Publishing these Security Standards and Policies

This document may be reproduced and distributed in whole or in part, free of charge, subject to the following conditions:

- All copyright and trademark notices, and this permission notice must be preserved complete on all complete or partial copies.

- Any translation or derivative work of this document must be approved by Frank O'Dwyer in writing before distribution.
- If you distribute this guide in part, instructions for obtaining the complete version of this manual must be included, and a means for obtaining a complete version provided.
- Small portions may be reproduced as illustrations for reviews or quotes in other works without this permission notice if proper citation is given.
- Neither Frank O'Dwyer's name nor the names of any contributors may be used to endorse or promote products derived from this document without specific prior written permission.

THIS DOCUMENT IS PROVIDED BY FRANK O'DWYER AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL FRANK O'DWYER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

I would like to be informed of any plans to publish or distribute these documents, just so I know how they're being used and where they are becoming available. If you are publishing or distributing or planning to publish or distribute any of these documents, please send mail to frankodwyer AT netscape.net

1.6. Related Documents

This document should be read and applied in conjunction with the technology specific security standards that are available from the frankodwyer.com web site. Please note that some of the documents below are currently under development and as such may not as yet be available. Check back frequently for updates to this document and those documents listed below.

1.6.1. Generic Security Standards

Generic Security Standards

<http://www.frankodwyer.com/standards/index.html#generic>

Data Protection European Union Security Standard

<http://www.frankodwyer.com/standards/index.html#generic>

Application Service Provider Security Standards

<http://www.frankodwyer.com/standards/index.html#generic>

1.6.2. Operating System Security Standards

Generic Unix Security Standards

<http://www.frankodwyer.com/standards/index.html#os>

Windows NT4.0 Generic Security Standards

<http://www.frankodwyer.com/standards/index.html#os>

Windows NT4.0 Workstation Security Standards

<http://www.frankodwyer.com/standards/index.html#os>

Windows NT4.0 Server Security Standards

<http://www.frankodwyer.com/standards/index.html#os>

Windows NT4.0 Domain Security Standards

<http://www.frankodwyer.com/standards/index.html#os>

1.6.3. Database Security Standards

Oracle Security Standards

<http://www.frankodwyer.com/standards/index.html#db>

1.7. Definitions

An “Information Asset” equates to any computerised information system or component thereof and thus includes an application, off the shelf software, hardware, media, data item, data item repository and associated communications networks. The specification of the Information Asset in question will usually be given so that this document is unambiguous.

Chapter 2. User Configuration

2.1. Default Accounts

2.1.1. Change default account passwords

ID	Version	Level	Enforcement
GUS-USER-02	1.0	baseline	mandatory

2.1.1.1. Standard

The default passwords of the following accounts must be changed following installation; open, uucp, toor, mount, guest, manager, ingres, mail, help, visitor, system, bin, demo, telnet, lp, who, finger, games

2.1.1.2. Detailed Steps

- For all accounts above the following accounts should have their passwords changed; open, uucp, toor, mount, guest, manager, ingres, uucp, mail, help, visitor, system, bin, demo, telnet, lp, who, finger, games

2.1.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised access may be obtained
- Unauthorised access may be used for fraudulent or malicious misuse
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.1.2. The synch account must not be disabled or password protected

ID	Version	Level	Enforcement
GUS-DA-2	1.0	baseline	mandatory

2.1.2.1. Standard

The synch account must not be disabled or password protected

2.1.2.2. Detailed Steps

- Ensure the synch account is enabled
- Ensure the synch account has no password

2.1.2.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Emergency shutdown can be performed
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.1.3. The nobody account should own no files on any of the systems filesystems

ID	Version	Level	Enforcement
GUS-DA-1	1.0	baseline	recommended

2.1.3.1. Standard

The nobody account should own no files on any of the systems filesystems

2.1.3.2. Detailed Steps

- Scan the filesystems for objects owned by nobody
- Reassign the ownership of any objects identified belonging to nobody

2.1.3.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.2. Roles, Views, and Access Control

2.2.1. Access to /dev/kmem must be restricted

ID	Version	Level	Enforcement
GUS-ACCESS-1	1.0	baseline	mandatory

2.2.1.1. Standard

Access to the device file /dev/kmem must be restricted

2.2.1.2. Detailed Steps

- Ensure that access to the device file /dev/kmem has the most restrictive access permissions

2.2.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Users may be able to change their UID to root
- Root access may lead to complete compromise of the system
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.2.2. Do not rely on access control lists on NFS file systems

ID	Version	Level	Enforcement
GUS-ACCESS-2	1.0	baseline	recommended

2.2.2.1. Standard

Do not rely on access control lists on NFS file systems

2.2.2.2. Detailed Steps

- Be aware that access control lists often do not work on NFS file systems

- Do not therefore rely on access control lists to mediate access to objects on NFS file systems

2.2.2.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Access to objects may not be restricted as expected
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.2.3. Avoid changing permissions on objects with access control lists using a numeric chmod

ID	Version	Level	Enforcement
GUS-ACCESS-3	1.0	baseline	recommended

2.2.3.1. Standard

Avoid changing permissions on objects with access control lists using a numeric chmod

2.2.3.2. Detailed Steps

- Be aware that numeric chmod commands may disable the ACL
- Use the symbolic chmod command to modify the permissions of files with ACLs

2.2.3.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Access to objects may not be restricted as expected
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.2.4. Any filenames beginning with a period . must not be everyone or group writable/readable.

ID	Version	Level	Enforcement
GUS-ACCESS-4	1.0	baseline	recommended

2.2.4.1. Standard

Any filenames beginning with a period . must not be everyone or group writable/readable.

2.2.4.2. Detailed Steps

- Identify all files beginning with a period .
- Check for each file whether it has everyone or group read/write
- Remove these permissions wherever possible

2.2.4.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Access to objects may not be restricted as expected
- Unauthorised access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.2.5. If a tape drive is used for backup ensure this device is not everyone readable

ID	Version	Level	Enforcement
GUS-ACCESS-5	1.0	baseline	recommended

2.2.5.1. Standard

If a tape drive is used for backup ensure this device is not everyone readable

2.2.5.2. Detailed Steps

- Identify the backup tape drives
- Check the permissions for this device

- Remove world read access where this permission has been enabled

2.2.5.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Access to data may not be restricted as expected
- Unauthorised access to data may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.3. Privileges

2.3.1. at access should be restricted using at.allow

ID	Version	Level	Enforcement
GUS-PRIV-2	1.0	baseline	recommended

2.3.1.1. Standard

at access should be restricted using at.allow

2.3.1.2. Detailed Steps

- Edit the at.allow file
- Add the users names who need to be able to submit at jobs

2.3.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.3.2. User UIDs must be greater than 20

ID	Version	Level	Enforcement
GUS-USER-01	1.0	baseline	mandatory

2.3.2.1. Standard

User UIDs must be greater than 20

2.3.2.2. Detailed Steps

- List each user account entry in the /etc/passwd file
- Check the UID value of each and highlight those that are not greater than 20
- Change the UID values to greater than 20 if possible
- Ensure that any new user accounts are set up with UIDs greater than 20

2.3.2.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised privileged access may be obtained
- Unauthorised access may be used for fraudulent or malicious misuse
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.3.3. Suid shell scripts should not be used

ID	Version	Level	Enforcement
GUS-PRIV-02	1.0	baseline	recommended

2.3.3.1. Standard

Suid shell scripts should not be used

2.3.3.2. Detailed Steps

- Identify all suid shell scripts on the system
- Replace these scripts with a different language such as perl

2.3.3.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised privileged access may be obtained
- Unauthorised access may lead to malicious or fraudulent misuse
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.3.4. The use of the su command should be with the hyphen (-) qualifier

ID	Version	Level	Enforcement
GUS-PRIV-01	1.0	baseline	recommended

2.3.4.1. Standard

The use of the su command should always be used with the hyphen (-) qualifier

2.3.4.2. Detailed Steps

- Educate all users to ensure that the(-) hyphen qualifier is used with su.
- Check scripts or executables running on the system that call su also use hyphen

2.3.4.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Account login script controls may be bypassed
- Unauthorised access may be obtained
- Unauthorised access may lead to fraudulent or malicious misuse
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.3.5. The alias file should be reviewed to ensure all redirection entries are users

ID	Version	Level	Enforcement
GUS-MAIL-03	1.0	baseline	recommended

2.3.5.1. Standard

The mail aliases file should be reviewed to ensure that all entries for mail redirection are valid users and not a program or a script for execution

2.3.5.2. Detailed Steps

- Review the aliases file
- Identify all redirection target accounts
- Check each of these targets is a user and not a script or program
- Investigate any entries that are inconsistent with this
- Delete inconsistent entries

2.3.5.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised program execution may occur
- Unauthorised access may be obtained
- Unauthorised access may lead to fraudulent or malicious misuse
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.3.6. root should only be logged into using su

ID	Version	Level	Enforcement
GUS-PRIV-05	1.0	above baseline	recommended

2.3.6.1. Standard

root should only be logged into using su

2.3.6.2. Detailed Steps

- Set all terminals to restricted to force root login via su

2.3.6.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Direct compromise of the root password will still result in no access
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.3.7. Use the wheel group if possible

ID	Version	Level	Enforcement
GUS-PRIV-06	1.0	baseline	mandatory

2.3.7.1. Standard

Where it is available use the wheel group

2.3.7.2. Detailed Steps

- Create the wheel group
- Add all users who are permitted to su root to the group
- Exclude all others

2.3.7.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised privileged access may be obtained
- Unauthorised access may be used for malicious or fraudulent misuse
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.

- Business information and applications may be unavailable.

2.3.8. Users must have individual UIDs

ID	Version	Level	Enforcement
GUS-USER-03	1.0	baseline	mandatory

2.3.8.1. Standard

Every user must have a unique UID.

2.3.8.2. Detailed Steps

- List all users sorted by UID.
- Identify all those with shared UIDs.
- Modify the users such that they have a unique UID.
- Ensure the files and directories these users own are appropriately owned.
- Ensure the files and directories these users own remain accessible.

2.3.8.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised access to data and software objects
- Unauthorised access may lead to fraudulent or malicious misuse
- Loss of accountability
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.3.9. Mount any foreign filesystems as NODEV

ID	Version	Level	Enforcement
GUS-PRIV-04	1.0	baseline	mandatory

2.3.9.1. Standard

Ensure that any foreign file systems are mounted NODEV

2.3.9.2. Detailed Steps

- Locate all instances where a foreign filesystem is mounted.
- For each instance ensure that the mount is qualified with NODEV

2.3.9.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Malicious device files can be used to subvert system controls
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.3.10. The write program should be set to SGID tty and not SUID root

ID	Version	Level	Enforcement
GUS-PRIV-03	1.0	above baseline	recommended

2.3.10.1. Standard

The write program should be set to SGID tty and not SUID root

2.3.10.2. Detailed Steps

- Locate the write program
- Check its permissions
- If the permissions are SUID root set them to SGID tty

2.3.10.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised privileged commands may be executed

- Unauthorised privileged access may be obtained
- Unauthorised access may result in malicious or fraudulent misuse
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.3.11. cron access should be restricted using cron.allow

ID	Version	Level	Enforcement
GUS-PRIV-1	1.0	baseline	recommended

2.3.11.1. Standard

cron access should be restricted using cron.allow

2.3.11.2. Detailed Steps

- Edit the cron.allow file
- Add the users names who need to be able to submit cron jobs

2.3.11.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.4. Authentication/Password Configuration

2.4.1. Implement a login failure retry interval of 3 seconds where possible

ID	Version	Level	Enforcement
GUS-AUTH-03	1.0	baseline	recommended

2.4.1.1. Standard

Implement a login failure retry interval of 3 seconds where possible

2.4.1.2. Detailed Steps

- If the variant of Unix supports a login failure retry interval set this interval to 3 seconds

2.4.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Automated password guessing routines will be hampered
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.4.2. Autologout of idle users should occur after 1 hour

ID	Version	Level	Enforcement
GUS-AUTH-02	1.0	baseline	recommended

2.4.2.1. Standard

Autologout of idle users should be set after 1 hour

2.4.2.2. Detailed Steps

- set autologout in .cshrc script to 1 hour

2.4.2.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised access may be obtained
- Unauthorised access may result in fraudulent or malicious misuse
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.4.3. Do not permit the use of control characters in passwords

ID	Version	Level	Enforcement
GUS-AUTH-01	1.0	baseline	recommended

2.4.3.1. Standard

The use of control characters should be prevented from being used within user passwords.

2.4.3.2. Detailed Steps

- Use filtering software that rejects passwords containing control characters.

2.4.3.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Control characters within passwords can be interpreted and lead to a breach
- Unauthorised privileged access may be obtained
- Unauthorised privileged commands may be executed
- Unauthorised access may lead to fraudulent or malicious misuse
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

Chapter 3. Security Compliance

3.1. Security Compliance Checking

3.1.1. Hidden files should be sought out and investigated

ID	Version	Level	Enforcement
GUS-MON-05	1.0	baseline	recommended

3.1.1.1. Standard

Hidden files should be sought out and investigated. Certain control characters in file names can make it difficult to see or access such files.

3.1.1.2. Detailed Steps

- Use the ls -q command to list files with control characters in their name.
- For each file identified review its contents for any malicious code or commands.
- Remove any files which are clearly intended to breach the security of the system.

3.1.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Malicious scripts and programs may be used to gain unauthorised access
- Unauthorised access may be used for malicious or fraudulent misuse
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

3.1.2. Reports should be produced and reviewed for access outside of normal hours

ID	Version	Level	Enforcement
GUS-AUD-02	1.0	baseline	recommended

3.1.2.1. Standard

Reports should be produced and reviewed for access outside of normal hours

3.1.2.2. Detailed Steps

- Log times of user logins
- Determine the normal access times for the system
- Report on logons that fall outside of those access times
- Reconcile the use with the account owner to ensure legitimacy

3.1.2.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Misuse may go unnoticed
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

3.1.3. syslog.conf must be monitored for all alterations

ID	Version	Level	Enforcement
GUS-AUD-01	1.0	baseline	mandatory

3.1.3.1. Standard

syslog.conf must be monitored for alterations

3.1.3.2. Detailed Steps

- Establish a baseline syslog.conf
- Identify any changes to the file from the baseline
- Reconcile the changes to ensure they are legitimate

3.1.3.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Misuse may go unnoticed
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

3.1.4. All new su programs should be identified and validated

ID	Version	Level	Enforcement
GUS-MON-01	1.0	baseline	recommended

3.1.4.1. Standard

All new su programs should be identified and validated to ensure that they are legitimate.

3.1.4.2. Detailed Steps

- Instigate a means of identifying the addition of new su programs to the system.
- Investigate the new su programs to ensure they are valid.
- Investigate any that are not and remove them from the system.

3.1.4.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Privileged unauthorised access may be obtained
- Unauthorised access may result in malicious or fraudulent misuse
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

3.1.5. grpck should be run regularly

ID	Version	Level	Enforcement
GUS-MON-03	1.0	baseline	recommended

3.1.5.1. Standard

grpck should be run regularly to check for inconsistencies in the /etc/groups file

3.1.5.2. Detailed Steps

- Run grpck to check for any inconsistencies in the groups file
- Any inconsistencies reported should be investigated and rectified

3.1.5.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Incorrect group membership may permit unauthorised access
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

3.1.6. Reports should be produced and reviewed for multiple login failures from a single source

ID	Version	Level	Enforcement
GUS-AUD-07	1.0	baseline	recommended

3.1.6.1. Standard

Reports should be produced and reviewed for multiple login failures from a single source

3.1.6.2. Detailed Steps

- Record login failures against user accounts
- Extract the source address/terminal id for each failure
- Report on login failures based upon source address
- Investigate any source terminal with a login failure against more than one target user account.

3.1.6.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Misuse may go unnoticed
- Unauthorised access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

3.1.7. pwck should be run regularly

ID	Version	Level	Enforcement
GUS-MON-02	1.0	baseline	recommended

3.1.7.1. Standard

pwck should be run regularly to identify inconsistencies in the password file.

3.1.7.2. Detailed Steps

- Run pwck on a regular basis to identify any inconsistencies in the passwd file.
- Any inconsistencies identified should be investigated and rectified.

3.1.7.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised access may be obtained
- Unauthorised access may lead to malicious or fraudulent misuse
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

3.1.8. Security monitoring software should be installed and used

ID	Version	Level	Enforcement
GUS-MON-04	1.0	baseline	recommended

3.1.8.1. Standard

Security monitoring software, for example Tripwire, Cops, Tiger, TCPWrapper etc should be installed and used for monitor for security critical changes, to harden the operating system and to provide security reporting.

3.1.8.2. Detailed Steps

- Identify security monitoring products appropriate to your environment.
- Install these tools.
- Use them to protect and monitor your system

3.1.8.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Security significant changes may go unnoticed
- Attempts to breach security may go unnoticed
- Unauthorised access may be obtained
- Unauthorised access may result in malicious or fraudulent misuse
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

3.1.9. Reports should be produced and reviewed for multiple login failures

ID	Version	Level	Enforcement
GUS-AUD-06	1.0	baseline	recommended

3.1.9.1. Standard

Reports should be produced and reviewed for multiple login failures

3.1.9.2. Detailed Steps

- Record login failures against user accounts
- Produce a daily report of login failures for user accounts

- Reconcile the login failures with the owners of the accounts.

3.1.9.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Misuse may go unnoticed
- Unauthorised access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

3.2. Security Management

3.2.1. Aliases should be created for all non-user accounts to redirect to the admin

ID	Version	Level	Enforcement
GUS-MAIL-02	1.0	baseline	recommended

3.2.1.1. Standard

Aliases should be created for all non-user accounts to redirect inbound mail to an administrator account where it will be read

3.2.1.2. Detailed Steps

- Identify all non-user accounts
- Identify an administrator to receive mail for these accounts
- Set up a mail alias to direct inbound mail to these accounts to the administrator

3.2.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

Chapter 4. Network Security Configuration

4.1. Network Interface Considerations

4.1.1. The ftp home directory should be owned by root

ID	Version	Level	Enforcement
GUS-NET-54	1.0	baseline	recommended

4.1.1.1. Standard

The ftp home directory should be owned by root

4.1.1.2. Detailed Steps

- Set the ownership of the ftp home directory to root

4.1.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised write access may be obtained
- Business information and data may be maliciously or accidentally altered
- Business information and applications may be unavailable.

4.1.2. PPP must not be installed on the system

ID	Version	Level	Enforcement
GUS-NET-29	1.0	baseline	mandatory

4.1.2.1. Standard

PPP must not be installed on the system

4.1.2.2. Detailed Steps

- Remove the PPP executable from the system
- Remove any reference to PPP from network configuration files

4.1.2.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Remote unauthorised access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.3. .rhosts files must not be used

ID	Version	Level	Enforcement
GUS-NET-16	1.0	baseline	mandatory

4.1.3.1. Standard

.rhosts files must not be used as they can provide arbitrary remote access to local users accounts and are subject to spoofing.

4.1.3.2. Detailed Steps

- Search users home directories for the presence of .rhosts files
- For those identified replace the access with another more secure method.
- Delete the .rhosts file

4.1.3.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- .rhosts file entries can permit successful spoofing
- Unauthorised access may be obtained
- Fraudulent misuse may occur
- Malicious misuse may occur
- Business information may be accidentally or maliciously altered.

- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.4. The systat service should be commented out of the inetd.conf file

ID	Version	Level	Enforcement
GUS-NET-15	1.0	baseline	recommended

4.1.4.1. Standard

The systat service should be commented out of the inetd.conf file as this provides very useful information to attackers

4.1.4.2. Detailed Steps

- Edit the inetd.conf file
- Identify the entry that initiates the systat daemon
- Comment out the entry so identified

4.1.4.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unnecessary intelligence may be given to system attackers
- Unauthorised access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.5. SLIP must not be installed on the system

ID	Version	Level	Enforcement
GUS-NET-28	1.0	baseline	mandatory

4.1.5.1. Standard

SLIP must not be installed on the system

4.1.5.2. Detailed Steps

- Remove the SLIP executable from the system
- Remove any reference to SLIP from network configuration files

4.1.5.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Remote unauthorised access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.6. The ftp entry in the password file should contain an invalid password and refer to a non-existent shell

ID	Version	Level	Enforcement
GUS-NET-53	1.0	baseline	recommended

4.1.6.1. Standard

The ftp entry in the password file should contain an invalid password and refer to a non-existent shell

4.1.6.2. Detailed Steps

- Edit the password file and set an invalid password value and a non-existent shell

4.1.6.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised access may be obtained
- Business information and data may be maliciously or accidentally altered
- Business information and data may be accidentally or maliciously disclosed
- Business information and applications may be unavailable.

4.1.7. Disable anonymous ftp if possible

ID	Version	Level	Enforcement
GUS-NET-45	1.0	baseline	recommended

4.1.7.1. Standard

Disable anonymous ftp if possible

4.1.7.2. Detailed Steps

- Edit the configuration and/or services file and comment out anonymous ftp service
- Restart the inet daemon and other appropriate system services/daemons to make the change take effect

4.1.7.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised non-privileged remote access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be accidentally or maliciously disclosed.
- Business information and applications may be unavailable.

4.1.8. root must be used to run all crontab scripts as user UUCP. The scripts must be owned by root.

ID	Version	Level	Enforcement
GUS-NET-11	1.0	baseline	mandatory

4.1.8.1. Standard

root must be used to run all crontab scripts as user UUCP. The scripts must be owned by root.

4.1.8.2. Detailed Steps

- Identify all crontab scripts required to be run by UUCP.
- Take ownership of these scripts by root.

- Ensure that when they are run they are executed by root as crontab.

4.1.8.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Protects crontab scripts from malicious alteration or substitution
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.9. The /etc/inetd.conf should be owned by root.

ID	Version	Level	Enforcement
GUS-NET-26	1.0	baseline	recommended

4.1.9.1. Standard

The /etc/inetd.conf should be owned by root.

4.1.9.2. Detailed Steps

- View the ownership of the inetd.conf file
- If this is not owned by root set it to be owned by root

4.1.9.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised changes to the file may be made
- Unauthorised access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.10. rexecd daemon should be disabled

ID	Version	Level	Enforcement
GUS-NET-14	1.0	baseline	recommended

4.1.10.1. Standard

The rexecd daemon should be disabled by commenting out the rexec entry in inetd.conf.

4.1.10.2. Detailed Steps

- Edit inetd.conf and locate the entry for rexecd
- Comment out the entry that initiates this daemon.

4.1.10.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Remote execution can be used to attempt to subvert system controls
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.11. NFS Filesystems should be exported nosuid

ID	Version	Level	Enforcement
GUS-NET-36	1.0	baseline	recommended

4.1.11.1. Standard

NFS Filesystems should be exported nosuid

4.1.11.2. Detailed Steps

- Exam the contents of the NFS exports file
- Ensure that the file systems are exported nosuid

4.1.11.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be accidentally or maliciously disclosed.
- Business information and applications may be unavailable.

4.1.12. Anonymous ftp should prevent overwrite by guests or anonymous users

ID	Version	Level	Enforcement
GUS-NET-47	1.0	baseline	recommended

4.1.12.1. Standard

Anonymous ftp should be configured to prevent overwrite by guests or anonymous users

4.1.12.2. Detailed Steps

- Configure the ftp daemon to prevent overwrite by anonymous or guest users

4.1.12.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised data deletions may take place
- Unauthorised data alteration may take place
- Business information and applications may be unavailable.

4.1.13. Entries in an NFS exports file must be comprised of fully qualified hostnames

ID	Version	Level	Enforcement
GUS-NET-33	1.0	baseline	mandatory

4.1.13.1. Standard

Entries in an NFS exports file must be comprised of fully qualified hostnames

4.1.13.2. Detailed Steps

- Exam the contents of the NFS exports file
- Ensure that the entries are fully qualified hostnames

4.1.13.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Data may be exported to incorrect hosts
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.14. The ftp home directory should have permissions of 555

ID	Version	Level	Enforcement
GUS-NET-55	1.0	baseline	recommended

4.1.14.1. Standard

The ftp home directory should have permissions of 555

4.1.14.2. Detailed Steps

- Set the file permissions of the ftp home directory to 555

4.1.14.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised write access may be obtained
- Business information and data may be maliciously or accidentally altered
- Business information and applications may be unavailable.

4.1.15. The fingerd daemon should be disabled by commenting out the finger entry in inetd.conf.

ID	Version	Level	Enforcement
GUS-NET-13	1.0	baseline	recommended

4.1.15.1. Standard

The fingerd daemon should be disabled by commenting out the finger entry in inetd.conf.

4.1.15.2. Detailed Steps

- Edit the inetd.conf file in order to delete the fingerd daemon entry.

4.1.15.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- The unnecessary provision of intelligence to attackers
- Unauthorised access may be obtained
- Unauthorised access may lead to fraudulent or malicious misuse
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.16. The permissions on the /etc/inetd.conf should be 644

ID	Version	Level	Enforcement
GUS-NET-27	1.0	baseline	recommended

4.1.16.1. Standard

The permissions on the /etc/inetd.conf should be 644

4.1.16.2. Detailed Steps

- View the permissions on the inetd.conf file
- If this is not set to 644 set the permissions to 644

4.1.16.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised changes to the file may be made
- Unauthorised access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.17. The /etc/hosts.equiv should contain the fewest number of trusted hosts

ID	Version	Level	Enforcement
GUS-NET-21	1.0	baseline	recommended

4.1.17.1. Standard

The /etc/hosts.equiv should contain the fewest number of trusted hosts

4.1.17.2. Detailed Steps

- View the contents of the /etc/hosts.equiv file and validate all entries
- Remove all of the entries that are not required

4.1.17.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.18. Ensure /etc/ftpusers contains default vendor and system accounts that should not require ftp access

ID	Version	Level	Enforcement
GUS-NET-44	1.0	baseline	recommended

4.1.18.1. Standard

Ensure /etc/ftpusers contains default vendor and system accounts that should not require ftp access

4.1.18.2. Detailed Steps

- Edit the /etc/ftpusers account
- Add the following accounts to the list where they are not already included, news, nobody, lp, uucp, bin, guest.
- Add all other default vendor accounts that have no ftp requirement
- Add all other default system accounts that have no ftp requirement

4.1.18.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised non-privileged remote access may be obtained
- Unauthorised privileged remote access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be accidentally or maliciously disclosed.
- Business information and applications may be unavailable.

4.1.19. Reverse lookup should be used for anonymous ftp connections

ID	Version	Level	Enforcement
GUS-NET-51	1.0	baseline	recommended

4.1.19.1. Standard

Reverse lookup should be used for anonymous ftp connections

4.1.19.2. Detailed Steps

- Configure the ftp daemon to use reverse lookup of anonymous ftp connections

4.1.19.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- IP address spoofing can be prevented
- Business information and data may be maliciously or accidentally altered
- Business information and data may be accidentally or maliciously disclosed
- Business information and applications may be unavailable.

4.1.20. The /etc/hosts.equiv should be removed unless required

ID	Version	Level	Enforcement
GUS-NET-20	1.0	baseline	recommended

4.1.20.1. Standard

The /etc/hosts.equiv should be removed unless required

4.1.20.2. Detailed Steps

- View the contents of the /etc/hosts.equiv file and validate any entries
- Where the file is empty delete the file altogether

4.1.20.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.21. There should be a mail alias to redirect mail from the UUCP account using the aliases file

ID	Version	Level	Enforcement
GUS-MAIL-04	1.0	baseline	mandatory

4.1.21.1. Standard

There should be a mail alias to redirect mail from the UUCP account using the aliases file. The .forward file should not be used to achieve this.

4.1.21.2. Detailed Steps

- Add an entry in the aliases file forwarding mail to an alternate account
- Ensure that there are no entries in the UUCP account's .forward file.

4.1.21.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be disclosed.

4.1.22. Anonymous ftp should prevent rename by guests or anonymous users

ID	Version	Level	Enforcement
GUS-NET-48	1.0	baseline	recommended

4.1.22.1. Standard

Anonymous ftp should be configured to prevent rename by guests or anonymous users

4.1.22.2. Detailed Steps

- Configure the ftp daemon to prevent rename by anonymous or guest users

4.1.22.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised object renames may take place
- Business information and data may be maliciously or accidentally altered

- Business information and applications may be unavailable.

4.1.23. Inetd.conf must be monitored for all alterations

ID	Version	Level	Enforcement
GUS-NET-03	1.0	baseline	mandatory

4.1.23.1. Standard

Inetd.conf must be monitored for alterations

4.1.23.2. Detailed Steps

- Establish a baseline inetd.conf
- Identify any changes to the file from the baseline
- Reconcile the changes to ensure they are legitimate

4.1.23.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- inetd.conf changes may result in the execution of unauthorised services
- Privileged unauthorised access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.24. The tftp home directory should not permit write access

ID	Version	Level	Enforcement
GUS-NET-62	1.0	baseline	recommended

4.1.24.1. Standard

The tftp home directory should not permit write access

4.1.24.2. Detailed Steps

- Check the permissions on the tftp home directory
- Set the permissions on the directory to exclude write access

4.1.24.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information and data may be maliciously or accidentally altered
- Business information and data may be maliciously or accidentally disclosed
- Business information and applications may be unavailable.

4.1.25. Ensure that the ftp daemon is the most recent

ID	Version	Level	Enforcement
GUS-NET-40	1.0	baseline	recommended

4.1.25.1. Standard

Ensure that the ftp daemon is the most recent

4.1.25.2. Detailed Steps

- Determine the currently installed ftp daemon
- Determine the most current ftp daemon
- If they differ install the most current ftp daemon

4.1.25.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised privileged access may be obtained
- Unauthorised non-privileged access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be accidentally or maliciously disclosed.
- Business information and applications may be unavailable.

4.1.26. No SUID/SGID bits should be set on UUCP component programs.

ID	Version	Level	Enforcement
GUS-NET-05	1.0	baseline	recommended

4.1.26.1. Standard

Where the UUCP subsystem is required all SUID and SGID bits should be removed from its component programs

4.1.26.2. Detailed Steps

- Determine if the UUCP subsystem is required.
- If it is required, identify all of the components with SGID and SUID bits set.
- For all components so identified strip these bits.

4.1.26.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised privileged access may be obtained remotely
- Access may lead to to fraudulent or malicious misuse
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.27. The rcp daemon should be disabled unless required

ID	Version	Level	Enforcement
GUS-NET-19	1.0	baseline	recommended

4.1.27.1. Standard

The rcp daemon should be disabled unless required

4.1.27.2. Detailed Steps

- Edit inetd.conf and locate the entry for rcpd
- Comment out the entry that initiates this daemon.

4.1.27.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.28. Ensure /etc/ftpusers is in place to deny users ftp access that do not require it

ID	Version	Level	Enforcement
GUS-NET-43	1.0	baseline	recommended

4.1.28.1. Standard

Ensure /etc/ftpusers is in place to deny users ftp access that do not require it

4.1.28.2. Detailed Steps

- Create an /etc/ftpusers file
- Populate the file with the users who should not have ftp access
- Ensure that the list is single entry per line

4.1.28.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised remote access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be accidentally or maliciously disclosed.
- Business information and applications may be unavailable.

4.1.29. The ~ftp/etc/passwd file should be owned by root

ID	Version	Level	Enforcement
GUS-NET-59	1.0	baseline	recommended

4.1.29.1. Standard

The ~ftp/etc/passwd file should be owned by root

4.1.29.2. Detailed Steps

- Check the file ownership of ~ftp/etc/passwd
- Where the owner is not root set the ownership to be root

4.1.29.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information and data may be maliciously or accidentally altered
- Business information and data may be maliciously or accidentally disclosed
- Business information and applications may be unavailable.

4.1.30. UUCP if required should be configured to only allow remote file retrieval from particular directories

ID	Version	Level	Enforcement
GUS-NET-07	1.0	baseline	recommended

4.1.30.1. Standard

UUCP if required should be configured to only allow remote file retrieval from particular directories.

4.1.30.2. Detailed Steps

- Configure UUCP access to permit access to specifically required directories.

4.1.30.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised access to data objects may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.31. tftp should be disabled unless the system serves X-terminals

ID	Version	Level	Enforcement
GUS-NET-61	1.0	baseline	recommended

4.1.31.1. Standard

tftp should be disabled unless the system serves X-terminals

4.1.31.2. Detailed Steps

- Determine if tftp is required
- Where it is not required comment the tftp entry out of the inetd.conf file

4.1.31.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information and data may be maliciously or accidentally altered
- Business information and data may be maliciously or accidentally disclosed
- Business information and applications may be unavailable.

4.1.32. Anonymous ftp should prevent setting of umask by guests or anonymous users

ID	Version	Level	Enforcement
GUS-NET-50	1.0	baseline	recommended

4.1.32.1. Standard

Anonymous ftp should be configured to prevent setting of umask by guests or anonymous users

4.1.32.2. Detailed Steps

- Configure the ftp daemon to prevent setting of umask by anonymous or guest users

4.1.32.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised object access permissioning may take place
- Business information and data may be maliciously or accidentally altered
- Business information and data may be accidentally or maliciously disclosed
- Business information and applications may be unavailable.

4.1.33. UUCP Callback should be enabled

ID	Version	Level	Enforcement
GUS-NET-08	1.0	baseline	recommended

4.1.33.1. Standard

UUCP callback should be enabled to reduce the risk of simple spoofing attacks

4.1.33.2. Detailed Steps

- If UUCP is required set up UUCP callback to deny simple spoofing attacks.

4.1.33.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Simple spoofing attacks
- Unauthorised access may be obtained
- Unauthorised access may lead to fraudulent or malicious misuse
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.34. The /etc/hosts.equiv should contain no hyphens or plus signs

ID	Version	Level	Enforcement
GUS-NET-22	1.0	baseline	recommended

4.1.34.1. Standard

The /etc/hosts.equiv should contain no hyphens or plus signs

4.1.34.2. Detailed Steps

- View the contents of the /etc/hosts.equiv file and identify any (-) or (+)
- Remove all entries containing a - or a + symbol

4.1.34.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.35. The /usr/lib/uucp/L.sys file must not allow group or everyone read access

ID	Version	Level	Enforcement
GUS-NET-66	1.0	baseline	mandatory

4.1.35.1. Standard

The /usr/lib/uucp/L.sys file must not allow group or everyone read access

4.1.35.2. Detailed Steps

- Check the permissions on the /usr/lib/uucp/L.sys file
- Remove group or everyone read access where it is granted

4.1.35.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- A password may be disclosed
- Unauthorised access to data objects may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.36. rdist should be used as a more secure means of performing file transfers

ID	Version	Level	Enforcement
GUS-NET-01	1.0	baseline	mandatory

4.1.36.1. Standard

rdist should be used as a more secure means of performing file transfers and should be used in preference to ftp.

4.1.36.2. Detailed Steps

- Use rdist for file transfers in preference to ftp

4.1.36.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.37. Disable sendmail if it is not required

ID	Version	Level	Enforcement
GUS-NET-38	1.0	baseline	recommended

4.1.37.1. Standard

Disable sendmail if it is not required

4.1.37.2. Detailed Steps

- Remove it as a service

4.1.37.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised privileged access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be accidentally or maliciously disclosed.
- Business information and applications may be unavailable.

4.1.38. The /etc/hosts.equiv should be owned by root

ID	Version	Level	Enforcement
GUS-NET-23	1.0	baseline	recommended

4.1.38.1. Standard

The /etc/hosts.equiv should be owned by root

4.1.38.2. Detailed Steps

- Check the ownership of the /etc/hosts.equiv file
- Where it is not owned by root change the ownership to root

4.1.38.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.39. UUCP account should be password protected if present

ID	Version	Level	Enforcement
GUS-NET-06	1.0	baseline	recommended

4.1.39.1. Standard

Where the UUCP account is present it should be password protected.

4.1.39.2. Detailed Steps

- If the UUCP account is present ensure that it is password protected.

4.1.39.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised remote access may be obtained
- Unauthorised access may be used for fraudulent misuse
- Unauthorised access may be used for malicious misuse
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.40. If NFS is used, all available patches should be applied.

ID	Version	Level	Enforcement
GUS-NET-31	1.0	baseline	recommended

4.1.40.1. Standard

If NFS is used, all available patches should be applied.

4.1.40.2. Detailed Steps

- Ensure that the release of software updates are monitored.

- Ensure that the patches identified are applied.

4.1.40.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.41. The ~ftp/etc/passwd file permissions should be set to 444

ID	Version	Level	Enforcement
GUS-NET-60	1.0	baseline	recommended

4.1.41.1. Standard

The ~ftp/etc/passwd file permissions should be set to 444

4.1.41.2. Detailed Steps

- Check the file permissions of ~ftp/etc/passwd
- Where the permissions are not set to 444 set the permissions to 444

4.1.41.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information and data may be maliciously or accidentally altered
- Business information and data may be maliciously or accidentally disclosed
- Business information and applications may be unavailable.

4.1.42. The UUCP subsystem should be removed unless it is required

ID	Version	Level	Enforcement
GUS-NET-04	1.0	baseline	mandatory

4.1.42.1. Standard

The UUCP subsystem must be removed unless it is required.

4.1.42.2. Detailed Steps

- Check to see whether the UUCP subsystem is actually required.
- If it is not required, remove it.

4.1.42.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- UUCP can be a source of multiple security vulnerabilities
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.43. The /etc/hosts.equiv should contain no trusted users

ID	Version	Level	Enforcement
GUS-NET-25	1.0	baseline	recommended

4.1.43.1. Standard

The /etc/hosts.equiv should contain no trusted users

4.1.43.2. Detailed Steps

- View the contents of the /etc/hosts.equiv file and identify any specific users
- Remove all entries relating to specific users

4.1.43.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.44. The home directory of the ftp user account must not contain a .forward file

ID	Version	Level	Enforcement
GUS-NET-58	1.0	baseline	mandatory

4.1.44.1. Standard

The home directory of the ftp user account must not contain a .forward file

4.1.44.2. Detailed Steps

- Delete any .forward file from the ftp user home directory

4.1.44.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information and data may be maliciously or accidentally altered
- Business information and data may be maliciously or accidentally disclosed
- Business information and applications may be unavailable.

4.1.45. Ensure that the ftp daemon is started up with the -l qualifier

ID	Version	Level	Enforcement
GUS-NET-41	1.0	baseline	recommended

4.1.45.1. Standard

Ensure that the ftp daemon is started up with the -l qualifier to log connections

4.1.45.2. Detailed Steps

- Edit the configuration or services file referenced during the startup of the ftp daemon
- Modify the entry for the ftp daemon to include the -l qualifier

4.1.45.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised use may go unrecorded
- Unauthorised use may go undetected
- Business information may be accidentally or maliciously altered.
- Business information may be accidentally or maliciously disclosed.
- Business information and applications may be unavailable.

4.1.46. The home directory of the ftp user account must not contain a .rhosts file

ID	Version	Level	Enforcement
GUS-NET-57	1.0	baseline	mandatory

4.1.46.1. Standard

The home directory of the ftp user account must not contain a .rhosts file

4.1.46.2. Detailed Steps

- Delete any .rhosts file from the ~ftp directory

4.1.46.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised remote access may be obtained
- Business information and data may be maliciously or accidentally altered
- Business information and data may be maliciously or accidentally disclosed

- Business information and applications may be unavailable.

4.1.47. The `~ftp/etc/passwd` file must not contain the entries from the real password file

ID	Version	Level	Enforcement
GUS-NET-56	1.0	baseline	mandatory

4.1.47.1. Standard

The `~ftp/etc/passwd` file must not contain the entries from the real password file

4.1.47.2. Detailed Steps

- Do not copy the real `passwd` file
- Do not copy entries from the real `passwd` file
- Create a new `passwd` file for the `~ftp/etc/passwd`

4.1.47.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised access to the system may be obtained
- Business information and data may be maliciously or accidentally altered
- Business information and data may be maliciously or accidentally disclosed
- Business information and applications may be unavailable.

4.1.48. The `rsh` daemon should be disabled unless required

ID	Version	Level	Enforcement
GUS-NET-18	1.0	baseline	recommended

4.1.48.1. Standard

The `rsh` daemon should be disabled unless required

4.1.48.2. Detailed Steps

- Edit inetd.conf and locate the entry for rshd
- Comment out the entry that initiates this daemon.

4.1.48.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.49. NFS exports file must not contain an entry for localhost

ID	Version	Level	Enforcement
GUS-NET-32	1.0	baseline	recommended

4.1.49.1. Standard

The NFS exports file must not contain an entry for localhost

4.1.49.2. Detailed Steps

- Exam the contents of the NFS exports file
- Ensure that no entries exist for localhost

4.1.49.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.50. Users \$HOME directories must not contain any

.netrc files

ID	Version	Level	Enforcement
GUS-NET-65	1.0	baseline	mandatory

4.1.50.1. Standard

Users \$HOME directories must not contain any .netrc files

4.1.50.2. Detailed Steps

- List all users \$HOME directories and identify those with .netrc files
- Delete all .netrc files found

4.1.50.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Passwords may be disclosed
- Unauthorised access to data objects may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.51. The ~ftp/usr/bin directory and its equivalents should not contain CLIs or other system commands

ID	Version	Level	Enforcement
GUS-NET-52	1.0	baseline	recommended

4.1.51.1. Standard

The ~ftp/usr/bin directory and its equivalents should not contain CLIs or other system commands

4.1.51.2. Detailed Steps

- Ensure that the contents of the ~ftp/usr/bin directory contains no unnecessary system commands or CLIs

4.1.51.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unintended commands may be executed
- Business information and data may be maliciously or accidentally altered
- Business information and data may be accidentally or maliciously disclosed
- Business information and applications may be unavailable.

4.1.52. Telnet should be disabled unless required

ID	Version	Level	Enforcement
GUS-NET-30	1.0	baseline	recommended

4.1.52.1. Standard

Telnet should be disabled unless required

4.1.52.2. Detailed Steps

- Comment the telnet daemon out of the inetd.conf file

4.1.52.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Remote unauthorised access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.53. The rlogin daemon should be disabled unless required

ID	Version	Level	Enforcement
GUS-NET-17	1.0	baseline	recommended

4.1.53.1. Standard

The rlogin daemon should be disabled unless required

4.1.53.2. Detailed Steps

- Edit inetd.conf and locate the entry for rlogind
- Comment out the entry that initiates this daemon.

4.1.53.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.54. Ensure that the ftp server does not permit the execution of the site exec command

ID	Version	Level	Enforcement
GUS-NET-42	1.0	baseline	recommended

4.1.54.1. Standard

Ensure that the ftp server does not permit the execution of the site exec command

4.1.54.2. Detailed Steps

- Check the ftp daemon default configuration
- Test the ftp server to see if the site exec command is accepted

4.1.54.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be accidentally or maliciously disclosed.

- Business information and applications may be unavailable.

4.1.55. Do not export a system owned file system

ID	Version	Level	Enforcement
GUS-NET-37	1.0	baseline	mandatory

4.1.55.1. Standard

Do not export a system owned file system

4.1.55.2. Detailed Steps

- Examine the contents of the NFS exports file
- Ensure that no system owned file systems are exported.

4.1.55.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised privileged access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be accidentally or maliciously disclosed.
- Business information and applications may be unavailable.

4.1.56. No UUCP files or directories should permit everyone write access

ID	Version	Level	Enforcement
GUS-NET-64	1.0	baseline	recommended

4.1.56.1. Standard

No UUCP files or directories should permit everyone write access

4.1.56.2. Detailed Steps

- Check the permissions on the UUCP files and directories

- Set the permissions to exclude everyone write access where it is currently permitted.

4.1.56.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised access to data objects may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.57. Ensure that all patches available for sendmail have been applied

ID	Version	Level	Enforcement
GUS-NET-39	1.0	baseline	recommended

4.1.57.1. Standard

Ensure that all patches available for sendmail have been applied

4.1.57.2. Detailed Steps

- Maintain notification for sendmail patch release
- Apply these patches as they become available.

4.1.57.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised privileged access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be accidentally or maliciously disclosed.
- Business information and applications may be unavailable.

4.1.58. Anonymous ftp should prevent deletion by guests or anonymous users

ID	Version	Level	Enforcement
GUS-NET-46	1.0	baseline	recommended

4.1.58.1. Standard

Anonymous ftp should be configured to prevent deletions by guests or anonymous users

4.1.58.2. Detailed Steps

- Configure the ftp daemon to prevent deletion by anonymous or guest users

4.1.58.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised object deletions may take place
- Business information and applications may be unavailable.

4.1.59. The /etc/exports file should be owned by root

ID	Version	Level	Enforcement
GUS-NET-35	1.0	baseline	recommended

4.1.59.1. Standard

The /etc/exports file should be owned by root

4.1.59.2. Detailed Steps

- Exam the ownership of the NFS exports file
- Set the ownership to root

4.1.59.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be accidentally or maliciously disclosed.

- Business information and applications may be unavailable.

4.1.60. Anonymous ftp should prevent chmod by guests or anonymous users

ID	Version	Level	Enforcement
GUS-NET-49	1.0	baseline	recommended

4.1.60.1. Standard

Anonymous ftp should be configured to prevent chmod by guests or anonymous users

4.1.60.2. Detailed Steps

- Configure the ftp daemon to prevent chmod by anonymous or guest users

4.1.60.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised object access permissioning may take place
- Business information and data may be maliciously or accidentally altered
- Business information and data may be accidentally or maliciously disclosed
- Business information and applications may be unavailable.

4.1.61. The tftp daemon should be started up with the -s qualifier

ID	Version	Level	Enforcement
GUS-NET-63	1.0	baseline	recommended

4.1.61.1. Standard

The tftp daemon should be started up with the -s qualifier

4.1.61.2. Detailed Steps

- Edit the inetd.conf file

- Add the -s qualifier to the tftp daemon entry in the file

4.1.61.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information and data may be maliciously or accidentally altered
- Business information and data may be maliciously or accidentally disclosed
- Business information and applications may be unavailable.

4.1.62. The ftp daemon must deny access to user accounts whose shell is not found as a valid shell in /etc/shells

ID	Version	Level	Enforcement
GUS-NET-02	1.0	baseline	mandatory

4.1.62.1. Standard

the ftp daemon should deny access to user accounts whose shell is not found as a valid shell in /etc/shells

4.1.62.2. Detailed Steps

- Ensure that /etc/shells includes only those shells valid for your system

4.1.62.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- The execution of illicit user shells by ftp may provide unauthorised access
- Unauthorised access may be used for malicious or fraudulent misuse
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.63. Export NFS filesystems read only wherever pos-

sible

ID	Version	Level	Enforcement
GUS-NET-34	1.0	baseline	recommended

4.1.63.1. Standard

Export NFS filesystems read only wherever possible

4.1.63.2. Detailed Steps

- Exam the contents of the NFS exports file
- Ensure that the file systems are exported read only where possible

4.1.63.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information and applications may be unavailable.

Chapter 5. Configuration

5.1. Files and File Permissions

5.1.1. .plan and .project files in users \$HOME directory should be kept empty

ID	Version	Level	Enforcement
GUS-USER-04	1.0	baseline	recommended

5.1.1.1. Standard

The files .plan and .project held in user \$HOME directories should be kept empty so that if the account is fingered no unnecessary information is released about the individual.

5.1.1.2. Detailed Steps

- The .plan and .project files held in the users \$HOME should be identified.
- Each of these files should be checked for any contents.
- For any with content these should be cleared out.

5.1.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unnecessary intelligence may be provided to system attackers
- Unauthorised access may be obtained
- Unauthorised access may result in fraudulent or malicious misuse
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

5.1.2. The wall command should be denied from non-administrative users

ID	Version	Level	Enforcement
GUS-FP-1	1.0	baseline	recommended

5.1.2.1. Standard

The wall command should be denied from non-administrative users

5.1.2.2. Detailed Steps

- Set permissions on the wall command to prevent execution by non-administrative users

5.1.2.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unwanted broadcast messages may be generated
- Business information may be disclosed.
- Business information and applications may be unavailable.

5.1.3. The permissions on the /etc/hosts.equiv should be 755

ID	Version	Level	Enforcement
GUS-NET-24	1.0	baseline	recommended

5.1.3.1. Standard

The permissions on the /etc/hosts.equiv should be 755

5.1.3.2. Detailed Steps

- Check the permissions of the /etc/hosts.equiv file
- Where the permissions are greater than 755 set the permissions to 755

5.1.3.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised access to the file may be obtained
- Entries may be added to the file to provide unauthorised access
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

Chapter 6. Installation

6.1. Setup Choices

6.1.1. Fsirand should be run once following commissioning

ID	Version	Level	Enforcement
GUS-SETUP-1	1.0	baseline	recommended

6.1.1.1. Standard

Fsirand should be run once following commissioning to generate random inode numbers for the files on the system

6.1.1.2. Detailed Steps

- Following commissioning of the system run fsirand

6.1.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

6.1.2. Do not install Unix as "Dual Universe"

ID	Version	Level	Enforcement
GUS-INST-01	1.0	baseline	mandatory

6.1.2.1. Standard

Do not install Unix in dual universe form as this can introduce significant security vulnerabilities.

6.1.2.2. Detailed Steps

- During installation install either Berkeley or System V.

6.1.2.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Multiple weaknesses may ensue from a dual universe installation
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

Chapter 7. Auditing and Monitoring

7.1. Events to be audited

7.1.1. The sulog should record both successful and unsuccessful su attempts

ID	Version	Level	Enforcement
GUS-EVEN-03	1.0	baseline	recommended

7.1.1.1. Standard

The sulog should record both successful and unsuccessful su attempts

7.1.1.2. Detailed Steps

- Configure auditing to record both successful and unsuccessful su attempts

7.1.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Attempts to breach security can be identified and avoided
- Unauthorised access may be obtained
- Unauthorised access may lead to fraudulent or malicious misuse
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

7.1.2. Lastlog should be enabled for all users

ID	Version	Level	Enforcement
GUS-AUD-03	1.0	baseline	recommended

7.1.2.1. Standard

Lastlog should be enabled for all users

7.1.2.2. Detailed Steps

- Ensure that all users have a lastlog file and that it is written to

7.1.2.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised account usage may go unnoticed
- Business information may be accidentally or maliciously altered.
- Business information may be accidentally or maliciously disclosed.
- Business information and applications may be unavailable.

7.1.3. Events for logging to syslog should be enabled for auth, daemon and cron messages.

ID	Version	Level	Enforcement
GUS-AUD-04	1.0	baseline	recommended

7.1.3.1. Standard

Events for logging to syslog should be enabled for auth, daemon and cron messages.

7.1.3.2. Detailed Steps

- Configure auditing to log auth, daemon and cron messages to the syslog

7.1.3.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised activity may go unrecorded
- Business information may be accidentally or maliciously altered.
- Business information may be accidentally or maliciously disclosed.
- Business information and applications may be unavailable.

7.1.4. Events logged to the syslog should be written to a

physically secure line printer as well.

ID	Version	Level	Enforcement
GUS-AUD-05	1.0	baseline	recommended

7.1.4.1. Standard

Events logged to the syslog should be written to a physically secure line printer as well.

7.1.4.2. Detailed Steps

- Configure auditing to write the syslog events to a physically secure line printer as well.

7.1.4.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised activity may go unrecorded
- Business information may be accidentally or maliciously altered.
- Business information may be accidentally or maliciously disclosed.
- Business information and applications may be unavailable.

7.1.5. The sulog contents should be recorded in both the sulog itself and written to a physically secure line printer

ID	Version	Level	Enforcement
GUS-EVEN-04	1.0	baseline	recommended

7.1.5.1. Standard

The sulog contents should be recorded in both the sulog itself and written to a physically secure line printer

7.1.5.2. Detailed Steps

- Configure auditing to write the sulog events to both the sulog and to a line printer

7.1.5.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Primary audit data is retained in a tamper proof manner allowing the identification of privileged unauthorised access
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

7.1.6. Loginlog should be used to identify potential breakin attempts

ID	Version	Level	Enforcement
GUS-EVEN-02	1.0	baseline	recommended

7.1.6.1. Standard

The loginlog file should be created and every entry should be considered as a potential breakin attempt and should therefore be regularly reviewed.

7.1.6.2. Detailed Steps

- Create the loginlog file
- Review the loginlog file on a periodic basis and identify new entries
- Each entry represents 5 login failures which should be investigated
- Any irreconcilable entries should be treated as a breakin attempt

7.1.6.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Attempts to breach security can be identified and avoided
- Unauthorised access may be obtained
- Unauthorised access may lead to fraudulent or malicious misuse
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

7.1.7. wtmp file should be regularly archived

ID	Version	Level	Enforcement
GUS-EVEN-01	1.0	baseline	recommended

7.1.7.1. Standard

The wtmp should be regularly archived to protect its contents from loss

7.1.7.2. Detailed Steps

- Ensure that the wtmp file is backed up at intervals which precede its erasure

7.1.7.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Loss of security significant event information may be lost
- Loss of accountability may occur
- Business information and applications may be unavailable.

Chapter 8. Other

8.1. The file L.cmds should be empty

ID	Version	Level	Enforcement
GUS-NET-10	1.0	baseline	recommended

8.1.1. Standard

The file L.cmds should be empty thereby making it impossible to remotely execute commands by using UUX.

8.1.2. Detailed Steps

- Delete any entries from the L.cmds file

8.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

8.2. All UUCP accounts should be added to the /etc/ftpusers account.

ID	Version	Level	Enforcement
GUS-NET-12	1.0	baseline	recommended

8.2.1. Standard

All UUCP accounts should be added to the /etc/ftpusers account.

8.2.2. Detailed Steps

- Edit the /etc/ftpusers to include all UUCP accounts.

8.2.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

8.3. If NFS is used, it should be ensured that the UUCP configuration, programs and data are never exported

ID	Version	Level	Enforcement
GUS-NET-09	1.0	baseline	mandatory

8.3.1. Standard

If NFS is used, it should be ensured that the UUCP configuration, programs and data are never exported as these are owned by UUCP and not root.

8.3.2. Detailed Steps

- Determine if NFS is in use.
- Determine if UUCP is in use.
- If both are in use check that the UUCP configuration, programs and data are not on the export volume.

8.3.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

8.4. .procmailrc and .forward should be re-

viewed for illicit entries

ID	Version	Level	Enforcement
GUS-MAIL-01	1.0	baseline	recommended

8.4.1. Standard

.procmailrc and .forward should be reviewed for illicit entries for example, the execution of a script in the /tmp directory.

8.4.2. Detailed Steps

- list the contents of each file
- validate the entries in each file
- remove any illicit entries in each file
- investigate the source of any illicit entries

8.4.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be disclosed.
- Business information and applications may be unavailable.

8.5. Any foreign filesystems should be mounted NOSUID

ID	Version	Level	Enforcement
GUS-PRIV-07	1.0	baseline	recommended

8.5.1. Standard

Any foreign filesystems including floppy disks should be mounted NOSUID

8.5.2. Detailed Steps

- When mounting a foreign filesystem ensure it is qualified with NOSUID

8.5.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Unauthorised root access may be obtained
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

Chapter 9. Checklist

<i>User Configuration</i>		
<i>Default Accounts</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
GUS-USER-02	Have the default passwords of the default accounts open, uucp, toor, mount, guest, manager, ingres, mail, help, visitor, system, bin, demo, telnet, lp, who, finger, games	
GUS-DA-2	Is the synch account disabled or password protected?	
GUS-DA-1	Is it ensured that the nobody account owns no files on any of the systems filesystems?	
<i>Roles, Views, and Access Control</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
GUS-ACCESS-1	Is access to /dev/kmem restricted?	
GUS-ACCESS-2	Is reliance placed on access control lists on NFS file systems	
GUS-ACCESS-3	Is it ensured that changing permissions on objects with access control lists is avoided?	
GUS-ACCESS-4	Is it ensured that any filenames beginning with a period . everyone or group writable/readable	
GUS-ACCESS-5	Are tape drives used for backups everyone readable?	
<i>Privileges</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
GUS-PRIV-2	Is at access restricted using at.allow?	
GUS-USER-01	Are all user UIDs greater than 20?	
GUS-PRIV-02	Are suid shell scripts in use on the system?	
GUS-PRIV-01	Is the hyphen qualifier always used with the su command?	
GUS-MAIL-03	Has the mail aliases file been reviewed to ensure that all entries for mail redirection are valid users and not a program or a script for execution?	
GUS-PRIV-05	Is root access only available via su?	
GUS-PRIV-06	If the wheel group is available is it in use?	
GUS-USER-03	Do all users on the system have unique UIDs?	
GUS-	Are all foreign filesystems mounted NODEV?	

Checklist

PRIV-04		
GUS-PRIV-03	Is the write program set to SGID tty and not SUID root?	
GUS-PRIV-1	Is cron access restricted using cron.allow?	
<i>Authentication/Password Configuration</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
GUS-AU-TH-03	Has a login failure retry interval of 3 seconds been implemented?	
GUS-AU-TH-02	Has autologout been set to 1 hour for idle users?	
GUS-AU-TH-01	Has the use of control characters in user passwords been prevented?	
<i>Security Compliance</i>		
<i>Security Compliance Checking</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
GUS-MON-05	Are hidden files or files with control characters in their names identified and investigated on a regular basis?	
GUS-AUD-02	Are reports produced and reviewed for access outside of normal hours?	
GUS-AUD-01	Is syslog.conf monitored for any changes?	
GUS-MON-01	Are new SU programs identified and validated?	
GUS-MON-03	Is grpck run regularly on the system?	
GUS-AUD-07	Are reports produced and reviewed for multiple login failures from a single source?	
GUS-MON-02	Is pwck run regularly to check for inconsistencies in the password file?	
GUS-MON-04	Are security tools installed and in use on the system?	
GUS-AUD-06	Are reports produced and reviewed for multiple login failures?	
<i>Security Management</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
GUS-MAIL-02	Are aliases in place for all non-user accounts?	
<i>Network Security Configuration</i>		
<i>Network Interface Considerations</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>

Checklist

GUS- NET-54	Is the ftp home directory owned by root?	
GUS- NET-29	Is it ensured that PPP is not installed on the system?	
GUS- NET-16	Are .rhosts files in use on users accounts on the system?	
GUS- NET-15	Has the systat service been commented out of the inetd.conf file?	
GUS- NET-28	Is it ensured that SLIP is not installed on the system?	
GUS- NET-53	Does the ftp entry in the password file contain an invalid password and refer to a non-existent shell?	
GUS- NET-45	If anonymous ftp is not required is it disabled?	
GUS- NET-11	Does root run all UUCP crontab scripts as user UUCP and own all of the scripts?	
GUS- NET-26	Is the /etc/inetd.conf owned by root?	
GUS- NET-14	Has the rexecd daemon been commented out in the inetd.conf?	
GUS- NET-36	Are NFS Filesystems exported nosuid?	
GUS- NET-47	Is anonymous ftp configured to prevent overwrite by guests or anonymous users?	
GUS- NET-33	Are the entries in the NFS exports file comprised of fully qualified hostnames?	
GUS- NET-55	Does the ftp home directory have permissions of 555?	
GUS- NET-13	Has the fingerd daemon been commented out of the inetd.conf file?	
GUS- NET-27	Are the permissions on the /etc/inetd.conf set to 644?	
GUS- NET-21	Does the /etc/hosts.equiv file contain the fewest number of trusted hosts?	
GUS- NET-44	Is it ensured that /etc/ftpusers contains default vendor and system accounts that should not require ftp access?	
GUS- NET-51	Is reverse lookup used for anonymous ftp connections	
GUS- NET-20	Has the /etc/hosts.equiv been removed where it is not required?	
GUS- MAIL-04	Does the UUCP account have a mail alias in the aliases file and no entries in the .forward file?	
GUS- NET-48	Is anonymous ftp configured to prevent rename by guests or anonymous users?	
GUS- NET-03	Is inetd.conf monitored for any changes?	
GUS- NET-62	Does the tftp home directory permit write access?	
GUS-	Is the ftp daemon the most recent?	

Checklist

NET-40		
GUS- NET-05	If the UUCP subsystem is required have the SGID/SUID bits been stripped from the UUCP?	
GUS- NET-19	Has the rcp daemon been commented out of the inetd.conf?	
GUS- NET-43	Are users who do not require ftp access denied it's use?	
GUS- NET-59	Is the ~ftp/etc/passwd file owned by root?	
GUS- NET-07	Has UUCP been set up to permit file retrieval from only certain pre-defined directories?	
GUS- NET-61	Is tftp disabled where it is not required?	
GUS- NET-50	Is anonymous ftp configured to prevent setting of umask by guests or anonymous users?	
GUS- NET-08	Is UUCP callback enabled?	
GUS- NET-22	Has it been ensured that the /etc/hosts.equiv contains no hyphens or plus signs?	
GUS- NET-66	Does the /usr/lib/uucp/L.sys file allow group or everyone read access?	
GUS- NET-01	Is rdist used for secure file transfer?	
GUS- NET-38	Is sendmail disabled where it is not required?	
GUS- NET-23	Is the /etc/hosts.equiv owned by root?	
GUS- NET-06	Is the UUCP account password protected where present?	
GUS- NET-31	Have all available NFS been applied?	
GUS- NET-60	Are the ~ftp/etc/passwd file permissions set to 444?	
GUS- NET-04	Has the UUCP subsystem been removed? If not, is it required?	
GUS- NET-25	Has it been ensured that the /etc/hosts.equiv contains no trusted users	
GUS- NET-58	Does the home directory of the ftp user account contain a .forward file?	
GUS- NET-41	Is it ensured that the ftp daemon is started up with the -l qualifier to log connections?	
GUS- NET-57	Does the home directory of the ftp user account contain a .rhosts file?	
GUS- NET-56	Does the ~ftp/etc/passwd file contain entries from the real password file?	
GUS- NET-18	Has the rsh daemon been commented out of the inetd.conf?	
GUS- NET-32	Does the NFS exports file contain an entry for localhost	

Checklist

GUS-NET-65	Do users \$HOME directories contain any .netrc files?	
GUS-NET-52	Is it ensured that the ~ftp/usr/bin directory and its equivalents do not contain CLIs or other system commands	
GUS-NET-30	Is Telnet disabled unless required?	
GUS-NET-17	Has the rlogin daemon been commented out of the inetd.conf?	
GUS-NET-42	Is it ensured that the ftp server does not permit the execution of the site exec command?	
GUS-NET-37	Are any system owned file systems exported?	
GUS-NET-64	Do UUCP files or directories permit everyone write access?	
GUS-NET-39	Have all patches available for sendmail been applied?	
GUS-NET-46	Is anonymous ftp configured to prevent deletions by guests or anonymous users?	
GUS-NET-35	Is the /etc/exports file owned by root?	
GUS-NET-49	Is anonymous ftp configured to prevent chmod by guests or anonymous users?	
GUS-NET-63	Is the tftp daemon started up with the -s qualifier?	
GUS-NET-02	Does the ftp daemon deny access to user accounts whose shell is not found to be a valid shell in /etc/shells?	
GUS-NET-34	Are NFS filesystems exported read only where possible?	
<i>Configuration</i>		
<i>Files and File Permissions</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
GUS-USER-04	Are the .plan and .project files held in the users \$HOME directories kept empty?	
GUS-FP-1	Is the wall command denied from non-administrative users?	
GUS-NET-24	Are the permissions on the /etc/hosts.equiv set to 755	
<i>Installation</i>		
<i>Setup Choices</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
GUS-SETUP-1	Is Fsirand run once on the system following commissioning?	
GUS-INST-01	Is the installation dual universe i.e. accepts both Berkeley and System V commands.	

Checklist

<i>Auditing and Monitoring</i>		
<i>Events to be audited</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
GUS-EVEN-03	Does the sulog record both successful and unsuccessful su attempts	
GUS-AUD-03	Is lastlog enabled for all users?	
GUS-AUD-04	Are the following events logged to syslog - auth, daemon and cron messages?	
GUS-AUD-05	Are the events logged to the syslog also written to a physically secure line printer as well?	
GUS-EVEN-04	Are the sulog contents recorded in both the sulog itself and written to a physically secure line printer?	
GUS-EVEN-02	Does the loginlog file exist and are its contents regularly reviewed?	
GUS-EVEN-01	Is the wtmp file regularly archived?	
<i>Other</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
GUS-NET-10	Is the L.cmds file empty?	
GUS-NET-12	Are all UUCP accounts added to the /etc/ftpusers account?	
GUS-NET-09	If NFS is in use has it been ensured that the UUCP configuration, programs and data are never exported?	
GUS-MAIL-01	Are the .procmailrc and .forward files reviewed for illicit entries?	
GUS-PRIV-07	Are all foreign filesystems mounted NOSUID?	