

Generic Security Standard

Generic Security Standard

Published 16 May 2009

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

This document defines a set of baseline generic information security controls applicable to any computerised information system. Additionally it provides guidance to administrators, developers and security personnel to assist in enhancing the security of implementations of applications and the technologies that underpin them.

This standard contains 87 baseline controls, and 5 above baseline controls, for a total of 92 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. User Administration	4
2.1.1. Each user must be given a unique account	4
2.1.2. A pre-defined naming convention should be used for user accounts	4
2.1.3. All requests for user account creation must be correctly authorised	5
2.1.4. Temporary or contract user accounts should have fixed period lifetimes	6
2.1.5. Account login time restrictions should be put in place to prevent access outside of required working hours	7
2.1.6. User accounts logged in after hours should be disconnected	8
2.2. Default Accounts	8
2.2.1. Delete all non-essential default accounts after installation	8
2.2.2. Generic accounts should not be created	9
2.2.3. Passwords of all default accounts must be changed from their initial value ..	10
2.3. Roles, Views, and Access Control	11
2.3.1. Access permissions on sensitive objects should be as restrictive as possible ..	11
2.3.2. Access to data, system and application software objects must be consistently enforced in line with access controls throughout the entire application architecture ...	11
2.3.3. Users should be provided with captive, menu driven accounts and prevented from accessing functions or data at the operating system level.	12
2.3.4. Application users must not be able to access the underlying operating system upon which their application is running.	13
2.3.5. Command line access should be denied except for administrative users.	14
2.3.6. Access or functionality provided to users at remote or untrusted locations should be kept to a minimum level.	14
2.3.7. Application privilege, functionality allocations and logical access controls at the operating system and database level must be able to support and implement any legal or regulatory control requirements for the application/system in question.	15
2.3.8. Enforce appropriate administrative segregation of duties	16
2.3.9. Access to the super user/administrator user account must be controlled	17
2.4. Privileges	18
2.4.1. User accounts must be created with least privilege	18
2.4.2. Software should run with minimum privilege	18
2.4.3. Non-administrative users must not be given administrative privileges or rights	19
2.5. Authentication/Password Configuration	20
2.5.1. Passwords must be stored in a one-way hashed format	20
2.5.2. The password minimum length for users must be 8 characters minimum.	21
2.5.3. Passwords must be transmitted across the internal network in encrypted form ..	21
2.5.4. Passwords must be at least 6 characters in length	22
2.5.5. A warning banner must be displayed prior to login	23
2.5.6. The repository used to store hashed passwords must not be accessible to non-privileged users	23

2.5.7. An idle timeout facility should be in place on desktop workstations/terminals	24
2.5.8. Date and time of last login must be displayed following successful login	25
2.5.9. User passwords must expire after a maximum of 60 days	26
2.5.10. Passwords must not be echoed on screen in plain text	26
2.5.11. Passwords must be expired following reset or account creation	27
2.5.12. Authentication failure must not indicate which authentication field is invalid	28
2.5.13. There should be a mechanism to prevent the selection of weak, easily guessed, passwords.	29
2.5.14. Strong authentication should be implemented	30
2.5.15. Users must provide a valid username and password to access an information asset	30
2.5.16. A software locking on demand facility should be available on the desktop	31
2.5.17. Administrative user passwords must have a maximum lifetime of 30 days	32
2.5.18. Admin user passwords must have a maximum lifetime of 7 days	32
2.5.19. The system must prevent password re-use for at least 12 changes	33
2.5.20. The user identifier and the password must be validated in a single operation	34
3. Security Compliance	36
3.1. Security Compliance Checking	36
3.1.1. Live data must not be supplied to 3rd parties for testing	36
3.1.2. Administrators must use analysis tools to detect account weaknesses	36
3.2. Security Management	37
3.2.1. Information owners must annually audit their user community	37
3.2.2. Physical output should be afforded appropriate physical protection	38
3.2.3. A recovery plan should be in place for every system within acceptable time	39
3.2.4. All user owned files must be reassigned 6 weeks after the user leaves or deleted	39
3.2.5. Contingency plans must be kept up to date.	40
3.2.6. Insurance arrangements should be adopted to provide additional protection	41
3.2.7. Contingency plans must be based upon risk analysis	41
3.2.8. Changes must not compromise security	42
3.2.9. Static data should be replicated where it is a single point of failure	43
3.2.10. User Administration must be clearly defined with documented procedures	43
3.2.11. Admin staff must be trained with clearly defined responsibilities	44
3.2.12. Live data for internal testing should be anonymised before use	45
3.2.13. When any individual leaves the organisation all access must be disabled.	46
3.2.14. Changes to all live systems must be under a change management process	46
3.2.15. All systems must have a nominated IT Custodian	47
3.2.16. Contingency plans must be subject to periodic tests.	47
3.2.17. Admin procedures must be documented, available and up to date	48
3.2.18. An undo function should be in the user interface for all atomic operations.	49
3.2.19. Emergency changes must include retrospective security authorisation	50
3.2.20. Old userids must not be re-issued to a new user.	50
3.2.21. Addition, modification and deletion of users must create an audit trail	51
3.2.22. Registers of users must be protected from loss and unauthorised access	52
4. Network Security Configuration	53
4.1. Network Interface Considerations	53
4.1.1. All phone lines within the company should be periodically swept for wire taps.	53
4.1.2. Switching based LANs should be implemented	53
4.1.3. Modem telephone numbers should be changed on a periodic basis where possible	54
4.2. Internet Considerations	55
4.2.1. Sensitive data must be encrypted in transit across an untrusted network	55
5. Configuration	56
5.1. Administration	56
5.1.1. All system administration should be performed using named accounts owned by the individual administrators	56

- 5.2. Backups 56
 - 5.2.1. Backup recovery timescales must be verified as acceptable 56
 - 5.2.2. Backup media must be stored securely at a remote location when not in use . 57
 - 5.2.3. Highly confidential data on backup media should be encrypted. 58
 - 5.2.4. Backup media must no be used more times than recommended maximum ... 58
- 6. Installation 60
 - 6.1. Setup Choices 60
 - 6.1.1. The latest version of the operating system should be installed wherever possible 60
 - 6.1.2. The RAID level selected should be appropriate to the criticality of the applications and the risks associated with disk failure 60
 - 6.1.3. All servers should be connected to an uninterruptible power supply 61
 - 6.1.4. The most secure implementation of the operating system should be selected at installation time 61
 - 6.1.5. All available patches for the operating system should be applied 62
- 7. Auditing and Monitoring 64
 - 7.1. Events to be alerted in real-time 64
 - 7.1.1. Systems must be able to detect/alert attempts to breach controls in real time . 64
 - 7.1.2. Systems must have a form of breakin evasion 64
 - 7.2. Audit log destination and format 65
 - 7.2.1. Audit log content must not be modifiable to non-privileged users or apps 65
 - 7.2.2. Audit log records must be retained for a minimum of thirteen months 66
 - 7.2.3. Audit logs must only be written to by the operating system or trusted apps ... 67
 - 7.2.4. Critical applications systems must maintain their own audit trails 67
 - 7.2.5. Audit log content must not be visible to non-privileged users 68
 - 7.3. Events to be audited 69
 - 7.3.1. Events captured must be sufficient to establish accountability for actions 69
 - 7.3.2. Audit logs must be reviewed periodically to identify suspicious event patterns 69
- 8. Other 71
 - 8.1. Cryptographic controls should be used to verify the integrity of transactions 71
 - 8.1.1. Standard 71
 - 8.1.2. Detailed Steps 71
 - 8.1.3. Risks Addressed 71
 - 8.2. Audit logs must be protected from deletion 71
 - 8.2.1. Standard 71
 - 8.2.2. Detailed Steps 71
 - 8.2.3. Risks Addressed 72
 - 8.3. Ensure keys and algorithms used to encrypt backups are correctly stored 72
 - 8.3.1. Standard 72
 - 8.3.2. Detailed Steps 72
 - 8.3.3. Risks Addressed 72
 - 8.4. Dialogues should include a commit function 73
 - 8.4.1. Standard 73
 - 8.4.2. Detailed Steps 73
 - 8.4.3. Risks Addressed 73
- 9. Checklist 74

Chapter 1. Introduction

1.1. Objectives

The objectives of this document are:

- To define a set of baseline generic information security controls applicable to any computerised information system.
- To provide guidance to administrators, developers and security personnel to assist in enhancing the security of implementations of applications and the technologies that underpin them.

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 your Information Security team consultancy function or other appropriate source of security skill.

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.

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](mailto:frankodwyer@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, an item of off the shelf software, hardware, media, a data item, a 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, except where a control relates to any “Information Asset”.

The use of “must” or “will” indicates what the author considers to be a mandatory control.

However, whether the controls listed here are mandatory for your organisation is entirely at your organisation's discretion and thus they should be interpreted as representing the strongest recommendation of the author.

The use of “should” or “recommended” or “ought” indicates that the author believes that the controls in question are worthwhile and should be implemented unless such an implementation is impossible, onerous or impractical. Again, the implementation of controls so recommended in this document is entirely at your organisation's discretion.

Chapter 2. User Configuration

2.1. User Administration

2.1.1. Each user must be given a unique account

ID	Version	Level	Enforcement
GSS-USER-1	1.0	baseline	mandatory

2.1.1.1. Standard

Each user must be given a unique account with which to access an information asset.

2.1.1.2. Detailed Steps

- Create a unique user account for all who access the information system.
- Identify shared accounts and replace with unique accounts for the sharing users

2.1.1.3. Risks Addressed

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

- Sharing accounts may result in a loss of availability during password change
- Sharing accounts results in password disclosure
- Sharing accounts may result in unauthorised access
- Sharing accounts may result in fraudulent misuse
- Sharing accounts may result in 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. A pre-defined naming convention should be used for user accounts

ID	Version	Level	Enforcement
GSS-USER-5	1.0	baseline	recommended

2.1.2.1. Standard

User accounts should be set up in accordance with a pre-defined naming convention.

2.1.2.2. Detailed Steps

- A recommended naming convention is first 3 letters of surname max, first letter of forename and next available two digit numeric counter. For example, "Calum Cooper" equates to COOC01. The use of such a convention caters for technologies that restrict username maximum length to 6 characters but will nonetheless render consistent, unique usernames across all technologies for all users.
- The application/system authentication subsystem should be designed to permit usernames of the length required by your convention to be supported

2.1.2.3. Risks Addressed

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

- Access may not be removed due to inconsistent user naming
- Unauthorised access to such accounts may then occur
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.1.3. All requests for user account creation must be correctly authorised

ID	Version	Level	Enforcement
GSS-USER-4	1.0	baseline	mandatory

2.1.3.1. Standard

All requests for user account creation must be correctly authorised.

2.1.3.2. Detailed Steps

- The creation of a user account must be approved by the business owner of the application in question

or their nominee.

- Where the account requested is for a non-application type system, the account request must be approved by the user's line manager

2.1.3.3. Risks Addressed

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

- Unauthorised access may be granted
- Unauthorised functionality may be granted
- 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.

2.1.4. Temporary or contract user accounts should have fixed period lifetimes

ID	Version	Level	Enforcement
GSS-USER-2	1.0	baseline	recommended

2.1.4.1. Standard

Temporary or contract users should be given accounts with fixed period lifetimes in accordance with the duration of their contracts/period of engagement.

2.1.4.2. Detailed Steps

- User account management should be used to set a user account lifetime
- Application logic should enable a user account lifetime to be set.
- Ensure that the system date and time are correctly set
- The process for getting access must obtain employment end dates.
- During account creation ensure that the employment end date is entered.

2.1.4.3. Risks Addressed

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

- Unauthorised access may occur
- 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.

2.1.5. Account login time restrictions should be put in place to prevent access outside of required working hours

ID	Version	Level	Enforcement
GSS-USER-9	1.0	baseline	recommended

2.1.5.1. Standard

Account login time restrictions should be put in place to prevent access outside of required working hours

2.1.5.2. Detailed Steps

- Determine required access times for users
- Implement login time restrictions outside of these working hours

2.1.5.3. Risks Addressed

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

- Unauthorised access may occur
- 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.

2.1.6. User accounts logged in after hours should be disconnected

ID	Version	Level	Enforcement
GSS-USER-10	1.0	baseline	recommended

2.1.6.1. Standard

User accounts logged in after hours should be disconnected

2.1.6.2. Detailed Steps

- Determine required access times for users
- Implement login time restrictions outside of these working hours
- Set the system to automatically disconnect users outside of these working hours

2.1.6.3. Risks Addressed

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

- Unauthorised access may occur
- 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.

2.2. Default Accounts

2.2.1. Delete all non-essential default accounts after installation

ID	Version	Level	Enforcement
GSS-USER-6	1.0	baseline	recommended

2.2.1.1. Standard

Guest accounts and all non-essential default accounts should be deleted from the system following initial installation

2.2.1.2. Detailed Steps

- If it is impossible or undesirable then default accounts must be disabled.
- Do not delete accounts absolutely required to run system processes
- Do not lock yourself out of the system by disabling all accounts
- Create the appropriate administrative accounts required for support

2.2.1.3. Risks Addressed

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

- Unauthorised unprivileged access may be obtained
- Unauthorised privileged 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.

2.2.2. Generic accounts should not be created

ID	Version	Level	Enforcement
GSS-USER-8	1.0	baseline	recommended

2.2.2.1. Standard

Wherever possible, generic accounts should be avoided

2.2.2.2. Detailed Steps

- Provide individual, non-shared accounts for all users.
- Generic accounts should only be created where it is unavoidable to do so
- Any generic accounts should not be capable of being logged into by users

2.2.2.3. Risks Addressed

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

- Unauthorised non-privileged access may occur
- Unauthorised privileged access may occur
- 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.

2.2.3. Passwords of all default accounts must be changed from their initial value

ID	Version	Level	Enforcement
GSS-USER-7	1.0	baseline	mandatory

2.2.3.1. Standard

The passwords of all accounts created during software installation must be changed from their default values immediately upon completion of the installation

2.2.3.2. Detailed Steps

- Identify accounts created during the installation of the software item in question.
- Change the passwords for each account created.

2.2.3.3. Risks Addressed

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

- Unauthorised non-privileged access may be obtained
- Unauthorised privileged 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.

2.3. Roles, Views, and Access Control

2.3.1. Access permissions on sensitive objects should be as restrictive as possible

ID	Version	Level	Enforcement
GSS-ACCE-5	1.0	baseline	recommended

2.3.1.1. Standard

Access permissions on sensitive objects should be as restrictive as possible

2.3.1.2. Detailed Steps

- Identify the sensitive objects
- Identify what the minimum access control permissions that are required for each object whilst ensuring normal functioning
- Set the minimum access control permissions against each object
- Monitor for changes to these permissions

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. Access to data, system and application software objects must be consistently enforced in line with access controls throughout the entire application architecture

ID	Version	Level	Enforcement
GSS-ACCE-1	1.0	baseline	mandatory

2.3.2.1. Standard

Access to data, system and application software objects must be consistently enforced in line with access controls throughout the entire application architecture

2.3.2.2. Detailed Steps

- if a user has access to functions x, y, z and data items a, b and c check that at the database level, the operating system level and at the network level that the user is unable to use these different view points to exceed these access restrictions.

2.3.2.3. Risks Addressed

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

- Subverting application access control through direct access to the database
- Subverting application access control by direct access to the operating system
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.3.3. Users should be provided with captive, menu driven accounts and prevented from accessing functions or data at the operating system level.

ID	Version	Level	Enforcement
GSS-ACCE-4	1.0	baseline	mandatory

2.3.3.1. Standard

Users should be provided with captive, menu driven accounts and prevented from accessing functions or data at the operating system level.

2.3.3.2. Detailed Steps

- Use OS access controls to prevent access to the command line.

- Develop the application such that the underlying OS is invisible to the user.

2.3.3.3. Risks Addressed

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

- Subverting application access control by direct access to the operating system
- Subverting DBMS access control by direct access to the operating system
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.3.4. Application users must not be able to access the underlying operating system upon which their application is running.

ID	Version	Level	Enforcement
GSS-ACCE-2	1.0	baseline	mandatory

2.3.4.1. Standard

Application users must not be able to access the underlying operating system upon which their application is running.

2.3.4.2. Detailed Steps

- Use OS access controls to prevent direct access by users.
- Ensure all user access is provided through the application interface.

2.3.4.3. Risks Addressed

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

- Subverting application access control by direct access to the operating system
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.3.5. Command line access should be denied except for administrative users.

ID	Version	Level	Enforcement
GSS-ACCE-3	1.0	baseline	mandatory

2.3.5.1. Standard

Command line access should be denied except for administrative users.

2.3.5.2. Detailed Steps

- Use OS access controls to prevent access to the command line.
- Use build tailoring to remove access to command line prompts

2.3.5.3. Risks Addressed

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

- Subverting application access control by direct access to the operating system
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.3.6. Access or functionality provided to users at remote or untrusted locations should be kept to a minimum level.

ID	Version	Level	Enforcement
GSS-ACCE-6	1.0	baseline	recommended

2.3.6.1. Standard

Access or functionality provided to users at remote or untrusted locations should be kept to a minimum level.

2.3.6.2. Detailed Steps

- Use OS access controls to prevent unnecessary access by remote non-privileged users
- Ensure that the access control permissions on the data objects available to remote users are the minimum required

2.3.6.3. 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.

2.3.7. Application privilege, functionality allocations and logical access controls at the operating system and database level must be able to support and implement any legal or regulatory control requirements for the application/system in question.

ID	Version	Level	Enforcement
GSS-ACCE-7	1.0	baseline	mandatory

2.3.7.1. Standard

Application privilege, functionality allocations and logical access controls at the operating system and database level must be able to support and implement any legal or regulatory control requirements for the application/system in question.

2.3.7.2. Detailed Steps

- Ensure that any legal or regulatory controls required to be delivered by an application are well defined and well understood.
- For each of these regulatory/legal controls, constraints, requirements that the design or the actuality of the application is able to support them.
- For new applications, design the application to deliver against these regulatory/legal requirements.
- For existing applications determine through a gap analysis the components that need to be delivered or enhanced to deliver against these regulatory requirements,

2.3.7.3. Risks Addressed

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

- Regulatory non-compliance
- Legal non-compliance
- Legal action
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.3.8. Enforce appropriate administrative segregation of duties

ID	Version	Level	Enforcement
GSS-ACCE-8	1.0	baseline	recommended

2.3.8.1. Standard

System administration, operations, security administration and security monitoring should be defined as discrete groups and granted only those privileges required to perform their respective job functions.

2.3.8.2. Detailed Steps

- Use OS administrative controls to grant access and privileges only to those who require them based upon their job function.
- For an application under development ensure that the administrative functionality includes the ability to separate function and privilege and that the application supports the notion of the job functions.

2.3.8.3. Risks Addressed

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

- Regulatory non-compliance
- Legal non-compliance
- Legal action
- Subverting organisational control
- Subverting operational control
- Business information may be accidentally or maliciously altered.

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

2.3.9. Access to the super user/administrator user account must be controlled

ID	Version	Level	Enforcement
GSS-ACCE-9	1.0	baseline	mandatory

2.3.9.1. Standard

Processes and procedures should be developed to control access to the superuser/administrator account. In particular, the password for this account should be maintained under management control.

2.3.9.2. Detailed Steps

- Use OS administrative controls to grant access and privileges only to those who require them based upon their job function.
- Maintain the password for the superuser/administrator accounts in a physically secure manner with tamper evident packaging e.g. an envelope with edges and flaps sealed in pressure sensitive tape, such that any attempted access to the password value is detectable.
- Maintain records of the use made of the superuser password and change the password after it has been used to a new value.
- Store the password values using the tamper evident packaging described above in a fire proof safe.
- Place the keys to the safe under dual management control.

2.3.9.3. Risks Addressed

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

- Regulatory non-compliance
- Legal non-compliance
- Legal action
- Subverting organisational control
- Subverting operational control
- Compromise of the entire system
- Subversion of management control

- Subversion of organisational control
- Bypass of functional control
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.4. Privileges

2.4.1. User accounts must be created with least privilege

ID	Version	Level	Enforcement
GSS-PRIV-1	1.0	baseline	mandatory

2.4.1.1. Standard

User accounts should be created and maintained with the fewest privileges required to successfully execute the users job function.

2.4.1.2. Detailed Steps

- Determine the implications of each privilege within the Information Asset.
- Grant only privileges necessary for the user to perform their job function.

2.4.1.3. Risks Addressed

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

- Misuse of privilege can be accidental or malicious
- The less privilege held the less the potential impact misuse might have
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.4.2. Software should run with minimum privilege

ID	Version	Level	Enforcement
GSS-PRIV-2	1.0	baseline	mandatory

2.4.2.1. Standard

Programmes, utilities and application software should be developed to run with the minimum of privileges to successfully perform their function.

2.4.2.2. Detailed Steps

- Define the functions the software under development needs to perform.
- For each function, determine any requirement for an elevated privilege.
- Grant only those privileges specifically identified as required.

2.4.2.3. Risks Addressed

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

- Software always contains bugs which may allow privileges to be misused.
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.4.3. Non-administrative users must not be given administrative privileges or rights

ID	Version	Level	Enforcement
GSS-PRIV-3	1.0	baseline	mandatory

2.4.3.1. Standard

Non-administrative users must not be granted administrative privileges or rights

2.4.3.2. Detailed Steps

- Ensure that administrative privileges are only granted to identified administrative users

2.4.3.3. Risks Addressed

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

- Misuse of privilege, accidental or deliberate may result in system compromise
- Privileged accounts are the most prized target for attackers
- The fewer administrative privileged accounts the better
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.5. Authentication/Password Configuration

2.5.1. Passwords must be stored in a one-way hashed format

ID	Version	Level	Enforcement
GSS-AUTH-8	1.0	baseline	mandatory

2.5.1.1. Standard

Passwords must be stored in a one-way hashed format.

2.5.1.2. Detailed Steps

- A one way hashing algorithm such as SHA-1 must be used to transform the password entered by the user to its encrypted value.
- A salt-value must be used to reduce the ease with which dictionary based/known ciphertext attacks may be launched against the hashed values
- An iteration count may also be used to further complicate dictionary attacks
- The hash values must be accessible only to privileged users or the system

2.5.1.3. Risks Addressed

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

- Bulk cracking of passwords depends on access to the hashed values
- Business information may be accidentally or maliciously altered.

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

2.5.2. The password minimum length for users must be 8 characters minimum.

ID	Version	Level	Enforcement
GSS-AUTH-12	1.0	above baseline	mandatory

2.5.2.1. Standard

In higher risk environments or uses, the password minimum length for end users must be set to 8 characters.

2.5.2.2. Detailed Steps

- Configure the information asset to enforce a password min length of 8.
- If developing an authentication subsystem ensure it supports 8 char min length

2.5.2.3. Risks Addressed

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

- Shorter passwords are easier to guess or exhaustively search.
- Accounts may therefore be easily compromised.
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.5.3. Passwords must be transmitted across the internal network in encrypted form

ID	Version	Level	Enforcement
GSS-AUTH-9	1.0	baseline	mandatory

2.5.3.1. Standard

When a password is entered and transmitted across the internal network it should be done so in encrypted form.

2.5.3.2. Detailed Steps

- If the solution includes an encryption option, turn it on.
- Consider use of SSL or TLS for encryption of TCP connections.
- Consider use of IPSEC for network level encryption.

2.5.3.3. Risks Addressed

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

- Unencrypted passwords are subject to disclosure.
- Passwords discovered may be used for unauthorised access
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.5.4. Passwords must be at least 6 characters in length

ID	Version	Level	Enforcement
GSS-AUTH_11	1.0	baseline	mandatory

2.5.4.1. Standard

Password minimum length for non-privileged users must be 6 characters.

2.5.4.2. Detailed Steps

- Configure the information asset such that the password minimum length is 6.
- If developing an authentication subsystem ensure it supports this control.

2.5.4.3. Risks Addressed

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

- Passwords shorter than 6 characters may be easily guessed.

- Passwords shorter than 6 characters may be easy to exhaustively search.
- Unauthorised access may be obtained
- Malicious misuse may occur
- Fraudulent misuse may occur
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.5.5. A warning banner must be displayed prior to login

ID	Version	Level	Enforcement
GSS-AUTH-21	1.0	baseline	mandatory

2.5.5.1. Standard

Prior to logon, all systems must display a warning message advising of the consequences of misuse and that monitoring of usage may be performed.

2.5.5.2. Detailed Steps

- The banner text used must be approved in your legislative environment.
- The banner text used must be appropriate to the culture of your organisation.
- Setup the information asset to display the chosen messages prior to logon.
- If the OS cannot provide this facility it should be developed in the application.

2.5.5.3. Risks Addressed

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

- Warning against misuse makes it clear that access must be authorised
- Systems that "welcome" users before authentication may legitimise attacks
- Prosecution of abusers may be inhibited by a failure to warn
- Other legal infringements may occur if warnings are not given in advance

2.5.6. The repository used to store hashed passwords must not be accessible to non-privileged users

ID	Version	Level	Enforcement
GSS-AUTH-10	1.0	baseline	mandatory

2.5.6.1. Standard

Password files must not be accessible to non-privileged users.

2.5.6.2. Detailed Steps

- Use OS access controls to prevent access by local non-privileged users
- Use distributed access control to deny access to remote non-privileged users

2.5.6.3. Risks Addressed

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

- Access to password files may allow malicious users to subvert passwords
- Unauthorised access to business systems may occur as a result.
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.5.7. An idle timeout facility should be in place on desktop workstations/terminals

ID	Version	Level	Enforcement
GSS-AUTH-20	1.0	baseline	recommended

2.5.7.1. Standard

Desktop hardware systems such as workstations/terminals etc should have an idle timeout facility such that after a period of inactivity the workstation/terminal user must re-authenticate to resume access.

2.5.7.2. Detailed Steps

- Use OS access controls to enforce an idle timeout
- Where it is unavailable it must be developed as a component of the application

2.5.7.3. Risks Addressed

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

- Unattended logged in desktops are open to misuse by all with access to it
- 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.

2.5.8. Date and time of last login must be displayed following successful login

ID	Version	Level	Enforcement
GSS-AUTH-19	1.0	baseline	recommended

2.5.8.1. Standard

Successful log-ons should be followed immediately by a display of the date and time of the last log-on, together with details of any unsuccessful attempts since that time.

2.5.8.2. Detailed Steps

- Configure the asset to to display the last login and failed attempts after login
- Implement a product to provide this information if not available inherently
- If developing an authentication subsystem build these features in

2.5.8.3. Risks Addressed

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

- Last logins will indicate anomalous use
- Failures since last login also indicate attempts to gain access
- A failure to report on these things may permit ongoing breaches
- Business information may be accidentally or maliciously altered.

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

2.5.9. User passwords must expire after a maximum of 60 days

ID	Version	Level	Enforcement
GSS-AUTH-14	1.0	baseline	mandatory

2.5.9.1. Standard

User account passwords must expire after a maximum of 60 days.

2.5.9.2. Detailed Steps

- Configure the information asset to set password lifetimes to 60 days.
- Develop the authentication system of the asset to support variable lifetimes

2.5.9.3. Risks Addressed

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

- Infrequently changed passwords are more likely to be guessed.
- A guessed password is usable for longer than those more frequently changed
- Unauthorised non-privileged 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.

2.5.10. Passwords must not be echoed on screen in plain text

ID	Version	Level	Enforcement
GSS-AUTH-7	1.0	baseline	mandatory

2.5.10.1. Standard

A password must not be echoed on screen in plain text, whether entered by a user during logon or password change.

2.5.10.2. Detailed Steps

- Ensure that the password change function in the authentication subsystem is developed so as to mask the characters entered during the login dialogue or the password change dialogue.

2.5.10.3. Risks Addressed

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

- Disclosure of a password may result in unauthorised access
- Unauthorised access may result in fraudulent misuse
- Unauthorised access may result in malicious misuse
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.5.11. Passwords must be expired following reset or account creation

ID	Version	Level	Enforcement
GSS-AUTH-22	1.0	baseline	mandatory

2.5.11.1. Standard

To ensure that the period of time is minimised during which more than one user knows the password for the same account, passwords must be set in an expired form when accounts have been newly created or after a password is reset.

2.5.11.2. Detailed Steps

- Ensure new accounts are created with the password set expired.

- Ensure that reset account passwords are set to as expired.
- If developing an authentication system ensure it supports password expiry.

2.5.11.3. Risks Addressed

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

- When a new account is created the creator and the user know the password
- When a password is reset the restter and the user know the password
- New and reset passwords are often set to a well known default value
- A loss of accountability results from these problems
- Unauthorised access may ensue
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.5.12. Authentication failure must not indicate which authentication field is invalid

ID	Version	Level	Enforcement
GSS-AUTH-6	1.0	baseline	mandatory

2.5.12.1. Standard

Authentication failure messages must not indicate which of the authentication fields are invalid

2.5.12.2. Detailed Steps

- Ensure that the authentication subsystem provides no information during failure

2.5.12.3. Risks Addressed

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

- Providng knowledge of which component is wrong aids an attacker
- This allows a more focused attack
- Unauthorised access may occur as a result

- Malicious misuse may occur
- Fraudulent misuse may occur
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.5.13. There should be a mechanism to prevent the selection of weak, easily guessed, passwords.

ID	Version	Level	Enforcement
GSS-AUTH-18	1.0	baseline	recommended

2.5.13.1. Standard

There should be a mechanism to prevent the selection of weak, easily guessed, passwords.

2.5.13.2. Detailed Steps

- Use the information assets configuration controls to increase pwd complexity
- If developing an authentication system include password complexity controls
- Implement password complexity/filtering software additionally where required.
- Reject passwords that are present in a dictionary of common passwords
- Reject passwords derived from dictionary words (e.g. "word123")
- Reject passwords equal to or derived from user ID
- Reject passwords that are based on information about the user that may be guessed
- Require passwords to include punctuation and digits as well as letters
- Consider also requiring upper case characters in passwords

2.5.13.3. Risks Addressed

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

- Weak passwords may be easily guessed.
- An easily guessed password allows accounts to be subverted and access gained.
- Business information may be accidentally or maliciously altered.

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

2.5.14. Strong authentication should be implemented

ID	Version	Level	Enforcement
GSS-AUTH-4	1.0	above baseline	recommended

2.5.14.1. Standard

For above baseline applications/systems stronger forms of authentication are required than reusable passwords. Under such circumstances the use of tokens, smartcards, biometrics and zero knowledge proof authentication mechanisms are considered as potential solutions.

2.5.14.2. Detailed Steps

- Use available "strong" authentication where your organisation already has this
- Where no infrastructure is available, a deployment should be undertaken.

2.5.14.3. Risks Addressed

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

- Strong authentication provides greater assurance of identity
- 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.

2.5.15. Users must provide a valid username and password to access an information asset

ID	Version	Level	Enforcement
GSS-AUTH-3	1.0	baseline	mandatory

2.5.15.1. Standard

For baseline applications, users must provide a valid username and password to access an information asset.

2.5.15.2. Detailed Steps

- Use OS authentication to enforce username and password control
- Ensure the authentication mechanism supports usernames and passwords

2.5.15.3. Risks Addressed

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

- Unauthenticated access allows arbitrary access
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.5.16. A software locking on demand facility should be available on the desktop

ID	Version	Level	Enforcement
GSS-AUTH-23	1.0	baseline	recommended

2.5.16.1. Standard

Desktop hardware systems such as workstations/terminals etc should allow the user to lock their workstation without the need to logout of the underlying applications.

2.5.16.2. Detailed Steps

- Use OS functionality to permit localised locking of workstations.
- If no such facility exists applications should be locked where possible
- Applications without a lock facility should be logged out when unattended.

2.5.16.3. Risks Addressed

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

- Unattended logged in workstations or application terminals are vulnerable
- Physical access may allow unauthorised logical access to occur
- Unauthorised logical access may result in fraudulent misuse
- Unauthorised logical access may result in malicious misuse
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.5.17. Administrative user passwords must have a maximum lifetime of 30 days

ID	Version	Level	Enforcement
GSS-AUTH-15	1.0	baseline	mandatory

2.5.17.1. Standard

Administrative accounts must have a maximum password lifetime of 30 days

2.5.17.2. Detailed Steps

- Configure all admin accounts to have 30 day pass lifetimes
- If developing an authentication system ensure it supports variable pwd lifetimes

2.5.17.3. 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.

2.5.18. Admin user passwords must have a maximum lifetime of 7 days

ID	Version	Level	Enforcement
GSS-AUTH-16	1.0	baseline	mandatory

2.5.18.1. Standard

Admin user passwords must have a maximum lifetime of 7 days.

2.5.18.2. Detailed Steps

- Configure administration accounts to have a password lifetime of 7 days
- If developing an authentication system ensure it supports variable pwd lifetimes

2.5.18.3. Risks Addressed

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

- The longer a pwd goes unchanged the greater the chance of compromise
- Administrative users passwords are the most prized by attackers
- Unauthorised privileged 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.

2.5.19. The system must prevent password re-use for at least 12 changes

ID	Version	Level	Enforcement
GSS-AUTH-17	1.0	baseline	mandatory

2.5.19.1. Standard

The system should prevent password re-use for at least 12 changes. That is, the authentication subsystem must include a password history function that prevents a password being set that figures in the 12 previously used passwords for that user.

2.5.19.2. Detailed Steps

- Configure the pwd history function to prevent reuse of last 12 passwords.
- If developing an authentication system ensure it includes a history function.
- Ensure the function provides equal protection to historic pwds as to the current
- Ensure that historic passwords are stored in one way hashed form.
- Ensure that access to historic pwd values is not available non admin users

2.5.19.3. Risks Addressed

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

- Reusing the same passwords may lead to a password compromise
- A password compromise may lead to unauthorised access
- Unauthorised access may lead to fraudulent misuse
- Unauthorised access may lead to malicious misuse
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.5.20. The user identifier and the password must be validated in a single operation

ID	Version	Level	Enforcement
GSS-AUTH-5	1.0	baseline	mandatory

2.5.20.1. Standard

The user identifier and the password entered must be validated in a single operation and not as separate steps.

2.5.20.2. Detailed Steps

- Only authenticate when both the username and the password have been entered.

2.5.20.3. Risks Addressed

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

- Indicating the step that has failed during authentication aids an attacker
- Unauthorised access may result
- Fraudulent misuse may occur
- Legal or regulatory obligations may be breached
- Malicious misuse may occur
- 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. Live data must not be supplied to 3rd parties for testing

ID	Version	Level	Enforcement
GSS-TEST-1	1.0	baseline	mandatory

3.1.1.1. Standard

Live data must not be supplied to external organisations for the purpose of testing application changes or for the diagnosis/resolution of problems.

3.1.1.2. Detailed Steps

- The procedures for support by third parties must not permit live data disclosure

3.1.1.3. Risks Addressed

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

- Business information may be disclosed.
- Legal/regulatory rules may be breached
- Censure from regulatory bodies may occur as a result

3.1.2. Administrators must use analysis tools to detect account weaknesses

ID	Version	Level	Enforcement
GSS-MANA-9	1.0	baseline	mandatory

3.1.2.1. Standard

The administrators must have and make use of security administration tools which facilitate the identification of security weaknesses e.g. dead, unused or inappropriate accounts, accounts without password protection or accounts with weak passwords.

3.1.2.2. Detailed Steps

- Install a security analysis tool
- Use the analysis tool to identify account weaknesses
- Use the output to define an action plan for changes
- Implement the changes

3.1.2.3. Risks Addressed

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

- Analysing account security helps to implement controls compliance
- A failure to analyse account security may allow attackers to gain access
- 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. Information owners must annually audit their user community

ID	Version	Level	Enforcement
GSS-MAN-7	1.0	baseline	mandatory

3.2.1.1. Standard

Information Asset Owners must conduct an annual audit of their user community in order to ensure that each user has a continuingly valid need to access the information asset

3.2.1.2. Detailed Steps

- Produce a schedule of all information assets and their respective owners.
- Produce a list of users for the information asset concerned.
- Provide the information to the owner and action any account changes resulting

3.2.1.3. Risks Addressed

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

- Ongoing unauthorised access may result in a breach of controls
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

3.2.2. Physical output should be afforded appropriate physical protection

ID	Version	Level	Enforcement
GSS-PHYS-1	1.0	baseline	recommended

3.2.2.1. Standard

The control of physical output from an application, such as printouts, should be afforded consistent levels of physical control and protection that are logically in place within the application from which it originates

3.2.2.2. Detailed Steps

- Identify the physical outputs from the system.
- Identify how the electronic equivalents are controlled within the application
- Put in place physical security controls to ensure the protection over the outputs
- Shred sensitive documents

3.2.2.3. Risks Addressed

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

- There is no point having good logical controls if other output is poorly handled
- Dumpster diving often reveals sensitive information
- Unauthorised access may be obtained
- Unauthorised access may result in fraudulent or malicious misuse
- Business information may be disclosed.

- Business information and applications may be unavailable.

3.2.3. A recovery plan should be in place for every system within acceptable time

ID	Version	Level	Enforcement
GSS-DISA-1	1.0	baseline	mandatory

3.2.3.1. Standard

An appropriate recovery plan must be in place for each information asset to enable processing to resume within an acceptable time delay in the event of a disaster.

3.2.3.2. Detailed Steps

- Determine the business impact of a loss of service.
- Produce a resumption plan based upon the critical time scale
- Walk through the plan to test its likelihood of success.
- Revisit the plan with any changes arising from the testing.

3.2.3.3. Risks Addressed

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

- Business information and applications may be unavailable.
- Money may be lost.
- Service may be lost

3.2.4. All user owned files must be reassigned 6 weeks after the user leaves or deleted

ID	Version	Level	Enforcement
GSS-MANA-6	1.0	baseline	mandatory

3.2.4.1. Standard

Six weeks after a user leaves, with the approval of the appropriate line manager, all accounts that belong

to the leaver must be deleted. At which time any files owned by these accounts must be either deleted or reallocated.

3.2.4.2. Detailed Steps

- The leaver process should say user files are deleted or reassigned after 6 weeks

3.2.4.3. Risks Addressed

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

- Orphaned data objects may contain sensitive information
- These objects may become owned by newly created users
- Access to these objects may be unauthorised
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

3.2.5. Contingency plans must be kept up to date.

ID	Version	Level	Enforcement
GSS-DISA-3	1.0	baseline	mandatory

3.2.5.1. Standard

Contingency plans must be kept up to date.

3.2.5.2. Detailed Steps

- On an annual basis repeat the business impact assessment for the system
- If the analysis has changed check the plan is adequate.
- On an annual basis review the technical aspects of the restoration plan
- Determine if the technical plan are able to support the asset in its current state. Where it cannot, additional provisioning should be put in place.

3.2.5.3. Risks Addressed

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

- Requirements change and that should be reflected in the recovery plan
- A failure to reflect that in the plan may render it ineffective
- Business information and applications may be unavailable.
- Money may be lost
- Service may be denied
- Reputation of your organisation may be damaged

3.2.6. Insurance arrangements should be adopted to provide additional protection

ID	Version	Level	Enforcement
GSS-DISA-5	1.0	baseline	mandatory

3.2.6.1. Standard

Insurance arrangements should be adopted to provide additional protection against certain risks

3.2.6.2. Detailed Steps

- If a loss from a disaster can be well defined, an insurance policy is prudent

3.2.6.3. Risks Addressed

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

- The financial consequences of a breach or loss of service can be mitigated

3.2.7. Contingency plans must be based upon risk analysis

ID	Version	Level	Enforcement
GSS-DISA-2	1.0	baseline	mandatory

3.2.7.1. Standard

Contingency plans must be based upon risk analysis

3.2.7.2. Detailed Steps

- Perform an impact assessment to determine the impact of loss of service.
- Based upon the impact of the loss of service build an appropriate plan

3.2.7.3. Risks Addressed

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

- Failing to resource where really needed may lead to a crucial loss of service
- Loss of service for some systems may threaten the viability of the organisation
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

3.2.8. Changes must not compromise security

ID	Version	Level	Enforcement
GSS-MANA-12	1.0	baseline	mandatory

3.2.8.1. Standard

The change management function must ensure that changes do not compromise security controls.

3.2.8.2. Detailed Steps

- Ensure any change control committees are attended by information security.
- Ensure all changes include authorisation from the information security dept.

3.2.8.3. Risks Addressed

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

- Unauthorised changes may result in unauthorised access
- Unauthorised changes may lead to a loss of service
- 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.

3.2.9. Static data should be replicated where it is a single point of failure

ID	Version	Level	Enforcement
GSS-AVAI-1	1.0	baseline	recommended

3.2.9.1. Standard

Where a high impact application is reliant upon static data, this data should be replicated so as to avoid a single point of failure

3.2.9.2. Detailed Steps

- Perform an impact assessment to determine if it is a high impact application
- Determine from the application data model the repositories of static data
- Decide whether the loss of the static data is likely to severely impact the app
- Where the loss of the static data is of high impact ensure that this is replicated.

3.2.9.3. Risks Addressed

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

- Fault tolerance is crucial to ensure continuity of service for high impact systems
- Business information and applications may be unavailable.

3.2.10. User Administration must be clearly defined with documented procedures

ID	Version	Level	Enforcement
GSS-MANA-1	1.0	baseline	mandatory

3.2.10.1. Standard

User administration must be a clearly defined function with documented procedures

3.2.10.2. Detailed Steps

- Identify the parties responsible for the administration of users for the system
- Identify the information owner for the information asset under consideration.
- Write procedures for the creation, modification and deletion of user accounts.
- Ensure these procedures include stages for authorisation for all access

3.2.10.3. Risks Addressed

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

- Ensuring access granted is correct and authorised is crucial
- A failure to grant access appropriately may result in misuse
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

3.2.11. Admin staff must be trained with clearly defined responsibilities

ID	Version	Level	Enforcement
GSS-MANA-14	1.0	baseline	mandatory

3.2.11.1. Standard

The ongoing administration of platforms must be performed by trained staff with clearly defined responsibilities.

3.2.11.2. Detailed Steps

- Ensure that all administrative jobs are well defined.
- Ensure all administrators are trained in order to execute their job functions

3.2.11.3. Risks Addressed

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

- Training helps to prevent mal administration taking place

- Maladministration may result in unauthorised access
- Maladministration may result in a loss of service
- Maladministration may result in a loss of data integrity
- 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.

3.2.12. Live data for internal testing should be anonymised before use

ID	Version	Level	Enforcement
GSS-TEST-2	1.0	baseline	recommended

3.2.12.1. Standard

The use of live data internally for testing should only be performed when the data has been desensitised i.e. all sensitive data overwritten

3.2.12.2. Detailed Steps

- Ensure testing procedures include live data anonymisation
- Ageing the data may be the only requirement.

3.2.12.3. Risks Addressed

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

- Testing users are not usually the same as the live users
- Data may therefore be disclosed without authorisation
- Legal/regulatory rules may be breached
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

3.2.13. When any individual leaves the organisation all

access must be disabled.

ID	Version	Level	Enforcement
GSS-MANA-5	1.0	baseline	mandatory

3.2.13.1. Standard

When any individual leaves the organisation all access must be disabled immediately.

3.2.13.2. Detailed Steps

- Ensure that when someone leaves the security admin function is notified

3.2.13.3. Risks Addressed

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

- Removing access when no longer required protects against misuse
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

3.2.14. Changes to all live systems must be under a change management process

ID	Version	Level	Enforcement
GSS-MANA-11	1.0	baseline	mandatory

3.2.14.1. Standard

Changes to all production systems must be controlled by a change management process

3.2.14.2. Detailed Steps

- Ensure change processes are developed and in place for live systems.
- Ensure that changes are subject to comment and approval prior to committing Ensure the process has the objective of ensuring continuity and quality of service.

3.2.14.3. Risks Addressed

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

- Change management forces inspection of planned changes
- This inspection provides the opportunity to identify errors and pitfalls
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

3.2.15. All systems must have a nominated IT Custodian

ID	Version	Level	Enforcement
GSS-MANA-10	1.0	baseline	mandatory

3.2.15.1. Standard

All systems must have a nominated IT Custodian

3.2.15.2. Detailed Steps

- Ensure someone from IT is nominated as the contact for the information asset

3.2.15.3. Risks Addressed

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

- An individual with responsibility for a system will ensure proper support
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

3.2.16. Contingency plans must be subject to periodic tests.

ID	Version	Level	Enforcement
GSS-DISA-4	1.0	baseline	mandatory

3.2.16.1. Standard

Contingency plans must be subject to periodic tests.

3.2.16.2. Detailed Steps

- Following a change to the plan, the plan should be re-tested.
- Following changes in the staff, the plan should be re-tested.
- Following the elapse of one year the plan should be re-tested.

3.2.16.3. Risks Addressed

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

- Testing a plan helps to ensure it will serve the purpose
- A failure to test it means that any failings will only be found when in use for real
- Business information and applications may be unavailable.
- Money may be lost
- Reputation of the organisation may be damaged

3.2.17. Admin procedures must be documented, available and up to date

ID	Version	Level	Enforcement
GSS-MANA-15	1.0	baseline	mandatory

3.2.17.1. Standard

Administrative procedures must be documented, comprehensive, up-to-date, accessible to authorised staff and protected from unauthorised access or loss.

3.2.17.2. Detailed Steps

- Ensure that routine administrative tasks are documented.
- Ensure that administration documents are maintained up to date.
- Ensure that administration documents are tested.
- Ensure that admin documentation is protected from unauthorised access

3.2.17.3. Risks Addressed

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

- A failure to maintain admin procedures may result in maladministration
- A failure to perform administration correctly may result in a loss of service
- A failure to perform administration correctly may result in a loss of integrity
- A failure to perform administration correctly may result in disclosure
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

3.2.18. An undo function should be in the user interface for all atomic operations.

ID	Version	Level	Enforcement
GSS-INTE-1	1.0	baseline	recommended

3.2.18.1. Standard

An undo function should be available in the user interface for all atomic operations.

3.2.18.2. Detailed Steps

- Design the app so that atomic operations can be undone via the user interface

3.2.18.3. Risks Addressed

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

- People make mistakes and an undo function provides rectification
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

3.2.19. Emergency changes must include retrospective

security authorisation

ID	Version	Level	Enforcement
GSS-MANA-13	1.0	baseline	mandatory

3.2.19.1. Standard

Ensure that emergency changes are subject to retrospective approval from the organisations information security function

3.2.19.2. Detailed Steps

- Ensure emergency change procedures include retrospective security approval

3.2.19.3. Risks Addressed

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

- Emergency changes may be used to mask unauthorised activity
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

3.2.20. Old userids must not be re-issued to a new user.

ID	Version	Level	Enforcement
GSS-MANA-3	1.0	baseline	mandatory

3.2.20.1. Standard

Old user ids must not be re-issued to a new user

3.2.20.2. Detailed Steps

- In conjunction with the information owner define templates for the various roles
- Ensure the process for creating/modifying accounts refers to the templates
- Create a blank disabled template for each of the roles to use during the process

3.2.20.3. Risks Addressed

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

- Re-issuing old ids may allow access to objects that was not expected
- Access to these objects may be unauthorised
- Such access may lead to fraudulent or accidental misuse of the system
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

3.2.21. Addition, modification and deletion of users must create an audit trail

ID	Version	Level	Enforcement
GSS-MANA-2	1.0	baseline	mandatory

3.2.21.1. Standard

The addition, modification and deletion of users must create an appropriate audit trail which identifies when change was actioned, the actioning party and the authorising party.

3.2.21.2. Detailed Steps

- Use OS access controls to prevent access by local non-privileged users
- Use distributed access control to prevent access by remote users

3.2.21.3. Risks Addressed

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

- A failure to create an audit trail may mask malicious behaviour
- A failure to follow appropriate procedures may result in unauthorised access
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

3.2.22. Registers of users must be protected from loss and unauthorised access

ID	Version	Level	Enforcement
GSS-MANA-8	1.0	baseline	mandatory

3.2.22.1. Standard

Registers of users must be protected from loss and unauthorised access

3.2.22.2. Detailed Steps

- Use access controls to prevent access by local non-privileged users
- Use safes or secure filing cabinets to protect registers of user accounts

3.2.22.3. Risks Addressed

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

- Unauthorised access to registers provides attackers with intelligence
- This information may be used to gain unauthorised access
- 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.

Chapter 4. Network Security Configuration

4.1. Network Interface Considerations

4.1.1. All phone lines within the company should be periodically swept for wire taps.

ID	Version	Level	Enforcement
GSS-NET-3	1.0	baseline	recommended

4.1.1.1. Standard

All phone lines within the company should be periodically swept for wire taps.

4.1.1.2. Detailed Steps

- Obtain a reflectometer
- Use the reflectometer to detect any unauthorised attachments to the lines

4.1.1.3. Risks Addressed

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

- The risk of eavesdropping
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.2. Switching based LANs should be implemented

ID	Version	Level	Enforcement
GSS-NET-1	1.0	baseline	recommended

4.1.2.1. Standard

Switching based LANs should be implemented

4.1.2.2. Detailed Steps

- For new LANs implement switches
- For existing LANs implement a migration plan to move to switching

4.1.2.3. Risks Addressed

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

- The risk of eavesdropping on the LAN is reduced
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.1.3. Modem telephone numbers should be changed on a periodic basis where possible

ID	Version	Level	Enforcement
GSS-NET-2	1.0	baseline	recommended

4.1.3.1. Standard

Modem telephone numbers should be changed on a periodic basis where possible

4.1.3.2. Detailed Steps

- On an annual basis get new numbers for your modem phone lines

4.1.3.3. Risks Addressed

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

- The risk of eavesdropping on the LAN is reduced
- Hacking
- Identification of illicit usage
- Business information may be accidentally or maliciously altered.

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

4.2. Internet Considerations

4.2.1. Sensitive data must be encrypted in transit across an untrusted network

ID	Version	Level	Enforcement
GSS-NETW-1	1.0	baseline	mandatory

4.2.1.1. Standard

Encryption should be used to prevent disclosure of sensitive data whilst in transmission across an untrusted network

4.2.1.2. Detailed Steps

- If the solution includes an encryption option, turn it on.
- Consider use of SSL or TLS for encryption of TCP connections.
- Consider use of IPSEC for network level encryption.

4.2.1.3. Risks Addressed

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

- Unencrypted data can be read and altered on an unencrypted network.
- Unencrypted data can be replayed on an unencrypted network.
- Sensitive data items such as passwords can be disclosed
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

Chapter 5. Configuration

5.1. Administration

5.1.1. All system administration should be performed using named accounts owned by the individual administrators

ID	Version	Level	Enforcement
GSS-ADMIN-1	1.0	baseline	recommended

5.1.1.1. Standard

All system administration should be performed using named accounts owned by the individual administrators

5.1.1.2. Detailed Steps

- Create administrative accounts for each administrator on the system
- Disable the default administrator account if possible

5.1.1.3. Risks Addressed

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

- Loss of administrative accountability.
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

5.2. Backups

5.2.1. Backup recovery timescales must be verified as acceptable

ID	Version	Level	Enforcement
GSS-BACK-3	1.0	baseline	mandatory

5.2.1.1. Standard

The ability to recover data from backup media within timescales acceptable to the organisation must be verified.

5.2.1.2. Detailed Steps

- Determine the data recovery times required for the application in question.
- Determine the length of time it takes to perform a restore
- Where these two times conflict adjust the recovery process accordingly.

5.2.1.3. Risks Addressed

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

- Recovering data from backups within certain timescales may be critical
- A failure to recover in a timely manner may cause financial loss
- A failure to recover in a timely manner may cause a loss of business
- A failure to recover in a timely manner may cause a loss of reputation
- A failure to recover in a timely manne may cause censure
- Business information and applications may be unavailable.

5.2.2. Backup media must be stored securely at a remote location when not in use

ID	Version	Level	Enforcement
GSS-BACK-2	1.0	baseline	mandatory

5.2.2.1. Standard

Backup media, except when in use, must be stored at a secure location, remote from the originating information asset to which it relates.

5.2.2.2. Detailed Steps

- Develop a backup cycle that demands storage of media at a secure remote site.

5.2.2.3. Risks Addressed

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

- Should the information asset be destroyed ensure the backup does not go with it
- Business information and applications may be unavailable.

5.2.3. Highly confidential data on backup media should be encrypted.

ID	Version	Level	Enforcement
GSS-BACK-4	1.0	above baseline	mandatory

5.2.3.1. Standard

Highly confidential data on backup media should be encrypted to prevent disclosure.

5.2.3.2. Detailed Steps

- Ensure that the backup solution includes an encryption option.
- Use the encryption option to protect the backups.

5.2.3.3. Risks Addressed

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

- Legal proceedings may result
- The organisation may be subject to censure
- The reputation of the organisation may be damaged
- Business information may be disclosed.
- Business information and applications may be unavailable.

5.2.4. Backup media must no be used more times than recommended maximum

ID	Version	Level	Enforcement
GSS-BACK-1	1.0	baseline	mandatory

5.2.4.1. Standard

Backup media must not be used more times than the number recommended by the media manufacturer.

5.2.4.2. Detailed Steps

- Identify the number of times the media can be used.
- Develop a backup cycle that includes a procedure for checking media ageing.
- Destroy the media securely at the end of its useful life

5.2.4.3. Risks Addressed

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

- Recovering data is dependent upon the ability to successfully read the media
- Business information and applications may be unavailable.

Chapter 6. Installation

6.1. Setup Choices

6.1.1. The latest version of the operating system should be installed wherever possible

ID	Version	Level	Enforcement
GSS-INST-1	1.0	baseline	recommended

6.1.1.1. Standard

The latest version of the operating system should be installed wherever possible

6.1.1.2. Detailed Steps

- Obtain the latest version of the operating system
- Install the latest version of the operating system

6.1.1.3. Risks Addressed

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

- Later versions of software often contain security fixes
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

6.1.2. The RAID level selected should be appropriate to the criticality of the applications and the risks associated with disk failure

ID	Version	Level	Enforcement
GSS-HARD-2	1.0	baseline	recommended

6.1.2.1. Standard

The RAID level selected should be appropriate to the criticality of the applications and the risks associated with disk failure

6.1.2.2. Detailed Steps

- Identify the raid levels available
- Identify the availability requirements of the system
- Implement the most appropriate raid level according to the availability requirements

6.1.2.3. Risks Addressed

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

- Business information and applications may be unavailable.

6.1.3. All servers should be connected to an uninterruptible power supply

ID	Version	Level	Enforcement
GSS-HARD-1	1.0	baseline	recommended

6.1.3.1. Standard

All servers should be connected to an uninterruptible power supply

6.1.3.2. Detailed Steps

- Ensure that machine rooms are served with UPS capability
- Connect the servers to the UPS

6.1.3.3. Risks Addressed

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

- Business information and applications may be unavailable.

6.1.4. The most secure implementation of the operating system should be selected at installation time

ID	Version	Level	Enforcement
GSS-INST-2	1.0	baseline	recommended

6.1.4.1. Standard

The most secure implementation of the operating system should be selected at installation time

6.1.4.2. Detailed Steps

- Security related choices at installation time should be selected on the basis of the most secure option.

6.1.4.3. Risks Addressed

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

- Extended security functionality is often only available if selected as an installation option.
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

6.1.5. All available patches for the operating system should be applied

ID	Version	Level	Enforcement
GSS-INST-3	1.0	baseline	recommended

6.1.5.1. Standard

All available patches for the operating system should be applied

6.1.5.2. Detailed Steps

- Identify available patches for the operating system
- Test the patches
- Implement the patches

6.1.5.3. Risks Addressed

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

- Security vulnerabilities may go unfixed
- 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 alerted in real-time

7.1.1. Systems must be able to detect/alert attempts to breach controls in real time

ID	Version	Level	Enforcement
GSS-ALER-1	1.0	baseline	recommended

7.1.1.1. Standard

Information Assets must be able to detect attempts to circumvent security controls and to provide alerts in real time of such attempts. For example repeated unsuccessful login attempts above a certain threshold should raise an automatic alarm to the security monitoring function or system administration team.

7.1.1.2. Detailed Steps

- Use the native real time security alerting system to provide alerts
- Where an asset is under development ensure it includes an alert mechanism
- Consider the deployment of event monitoring software to interpret events

7.1.1.3. Risks Addressed

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

- A failure to identify attempted breaches allows attempts to continue
- Ongoing attempts to gain access will eventually succeed if left unchecked
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

7.1.2. Systems must have a form of breakin evasion

ID	Version	Level	Enforcement
GSS-RESP-1	1.0	baseline	mandatory

7.1.2.1. Standard

Systems must be able to measure the number of consecutive log-on attempts irrespective of time span, and no more than six such failures must be allowed before automatic protective action occurs.

7.1.2.2. Detailed Steps

- Use the native O/S and authentication subsystem to identify breakin attempts
- Employ breakin evasion techniques when the threshold is breached, such as;
- Not permitting any further login attempts from that source
- Hanging up the line if it is a dial connection
- Not permitting login regardless of authentication of the userid and password
- Disabling the user account that is subject to the login failures.
- Where an app is under development it should include breakin evasion ability

7.1.2.3. Risks Addressed

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

- The ability to take positive action during attack safeguards the system.
- A failure to take action may result in a successful breach of the system
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

7.2. Audit log destination and format

7.2.1. Audit log content must not be modifiable to non-privileged users or apps

ID	Version	Level	Enforcement
GSS-ELOG-4	1.0	baseline	mandatory

7.2.1.1. Standard

Audit log content must not be writable or modifiable to non-privileged users and applications

7.2.1.2. Detailed Steps

- Use access control to prevent write access by non-privileged users and apps

7.2.1.3. Risks Addressed

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

- The ability to modify the content of the event log may mask malicious actions
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

7.2.2. Audit log records must be retained for a minimum of thirteen months

ID	Version	Level	Enforcement
GSS-ELOG-5	1.0	baseline	mandatory

7.2.2.1. Standard

Audit log records must be retained for a minimum of thirteen months

7.2.2.2. Detailed Steps

- Ensure the backup procedure ensures audit log data is retained for 13 months

7.2.2.3. Risks Addressed

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

- You may need to reconstruct events over the course of a financial year
- A failure to keep this data may mask malicious events
- A failure to keep this data may make reconstruction of events impossible
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

7.2.3. Audit logs must only be written to by the operating system or trusted apps

ID	Version	Level	Enforcement
GSS-ELOG-1	1.0	baseline	mandatory

7.2.3.1. Standard

Audit/event logs must only be written to by trusted operating system and application software

7.2.3.2. Detailed Steps

- Use access control to prevent writes from non-privileged users and software.
- Use distributed access control to prevent access by remote non-privileged users

7.2.3.3. Risks Addressed

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

- The ability to write to the event log may be used to right misleading events
- The ability to delete events from the event log may mask malicious behaviour
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

7.2.4. Critical applications systems must maintain their own audit trails

ID	Version	Level	Enforcement
GSS-ELOG-6	1.0	above baseline	mandatory

7.2.4.1. Standard

Critical application systems must maintain their own audit trails

7.2.4.2. Detailed Steps

- Use the inbuilt auditing subsystem of the system to create an audit log.

- If developing, ensure the app includes support for writing to its own audit log

7.2.4.3. Risks Addressed

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

- Critical apps must keep a record of events that are not subject to interference
- Failing to maintain an event log may make reconstruction of events impossible
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

7.2.5. Audit log content must not be visible to non-privileged users

ID	Version	Level	Enforcement
GSS-ELOG-3	1.0	baseline	mandatory

7.2.5.1. Standard

Audit log content must not be visible to non-privileged users

7.2.5.2. Detailed Steps

- Use OS access controls to prevent read access by non-privileged users
- Use distributed access control to prevent access by remote non-privileged users

7.2.5.3. Risks Addressed

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

- Audit logs often contain information and events useful to attackers
- Providing access to this information may lead to unauthorised access
- 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.

7.3. Events to be audited

7.3.1. Events captured must be sufficient to establish accountability for actions

ID	Version	Level	Enforcement
GSS-EVEN-1	1.0	baseline	mandatory

7.3.1.1. Standard

The security events recorded within the log of an Information Asset must be sufficient to establish individual accountability for actions performed and be able to support the investigation and resolution of suspected violations.

7.3.1.2. Detailed Steps

- Define the set of events to be recorded within the auditing subsystem
- If an app is in development ensure that business events are captured
- If an app is in development ensure that technical events are captured

7.3.1.3. Risks Addressed

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

- Capturing events allows an audit trail of activity to be created
- A failure to capture events prevents abnormal activity from being identified
- This allows an attackers behaviour to unnoticed.
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

7.3.2. Audit logs must be reviewed periodically to identify suspicious event patterns

ID	Version	Level	Enforcement
GSS-RESP-2	1.0	baseline	mandatory

7.3.2.1. Standard

Audit logs must be reviewed periodically to identify security incidents or suspicious patterns of events.

7.3.2.2. Detailed Steps

- Define patterns of events that are normal for the system in question
- Investigate patterns of events that fall outside these normal patterns
- If the pattern proves to be valid add it to the normal pattern knowledge base.
- If the pattern remains anomalous analyse it on the basis that it is an attack

7.3.2.3. Risks Addressed

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

- Attacks may go unidentified
- Fraudulent activity may go unidentified
- Breaches of business rules may go unidentified
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

Chapter 8. Other

8.1. Cryptographic controls should be used to verify the integrity of transactions

ID	Version	Level	Enforcement
GSS-INTE-4	1.0	baseline	recommended

8.1.1. Standard

Cryptographic controls such as message authentication codes, digital signatures etc should be used to verify the integrity of critical transactions

8.1.2. Detailed Steps

- Identify the critical transactions within the application
- Use cryptographic integrity checks to validate the data within these functions

8.1.3. Risks Addressed

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

- Business information may be accidentally or maliciously altered.

8.2. Audit logs must be protected from deletion

ID	Version	Level	Enforcement
GSS-ELOG-2	1.0	baseline	mandatory

8.2.1. Standard

Audit logs must be protected from deletion

8.2.2. Detailed Steps

- Use OS access controls to prevent delete access by non-privileged users

8.2.3. Risks Addressed

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

- Deletion of the event log may be used to mask malicious actions
- Deletion of the event log may mask fraudulent misuse
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

8.3. Ensure keys and algorithms used to encrypt backups are correctly stored

ID	Version	Level	Enforcement
GSS-BACK-5	1.0	above baseline	mandatory

8.3.1. Standard

The protection of encryption keys and algorithms used in encrypting backups needs to be ensured to reduce the risk of the keys and algorithms being disclosed, altered or destroyed

8.3.2. Detailed Steps

- The backup solution must include key management to prevents key disclosure
- The backup solution must include key management to prevents key alteration
- The backup solution must include key management to prevents key destruction

8.3.3. Risks Addressed

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

- Key and algorithm information may be accidentally or deliberately altered
- Business information may be disclosed.
- Business information and applications may be unavailable.

8.4. Dialogues should include a commit func-

tion

ID	Version	Level	Enforcement
GSS-INTE-2	1.0	baseline	recommended

8.4.1. Standard

Dialogues should be developed in the application interface that seek confirmation prior to committing a sensitive transaction within the application

8.4.2. Detailed Steps

- Identify the sensitive functions that will be in the application.
- Ensure that for these functions include confirmation dialogues are developed

8.4.3. 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 9. Checklist

<i>User Configuration</i>		
<i>User Administration</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
GSS-USER-1	Has each user been given a unique account?	
GSS-USER-5	Are user accounts set up in accordance with a pre-defined naming convention?	
GSS-USER-4	Does a business process exist to ensure that all requests for user account creation are correctly authorised?	
GSS-USER-2	Have temporary or contract users been given accounts with fixed period lifetimes?	
GSS-USER-9	Are account login time restrictions in place to prevent access outside of required working hours?	
GSS-USER-10	Are user accounts logged in after hours should be disconnected?	
<i>Default Accounts</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
GSS-USER-6	Have guest accounts and all non-essential default accounts been deleted from the system following initial installation?	
GSS-USER-8	Have all generic accounts been removed or disabled?	
GSS-USER-7	Have the passwords of all accounts created during software installation been changed from their default values?	
<i>Roles, Views, and Access Control</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
GSS-ACCE-5	Are the access permissions on sensitive objects as restrictive as possible?	
GSS-ACCE-1	Is access to data, system and application software objects consistently enforced, in line with access controls throughout the entire application architecture?	
GSS-ACCE-4	Are users provided with captive, menu driven accounts and prevented from accessing functions or data at the operating system level?	
GSS-ACCE-2	Can application users access the underlying operating system upon which their application is running?	
GSS-ACCE-3	Is command line access denied except for administrative users?	
GSS-ACCE-6	Is access or functionality provided to users at remote or untrusted locations kept to a minimum level.	
GSS-ACCE-7	Are any legal or regulatory control requirements supported and implemented by the application/system implementation?	
GSS-	Are system administration, operations, security administration and secur-	

Checklist

ACCE-8	ity monitoring defined as discrete functional groups and granted only those privileges required to perform their respective job functions.	
GSS-ACCE-9	Is access to the superuser/administrator account maintained under management control?	
<i>Privileges</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
GSS-PRIV-1	Are user accounts created and maintained with the fewest privileges required to successfully execute the users job functions?	
GSS-PRIV-2	Is software installed and run with the minimum privileges required to successfully execute its function.	
GSS-PRIV-3	Are non-administrative users granted administrative privileges or rights?	
<i>Authentication/Password Configuration</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
GSS-AUTH-8	Are passwords stored in a one-way hashed format?	
GSS-AUTH-12	Is the password minimum length 8 characters?	
GSS-AUTH-9	Are passwords transmitted across the internal network in encrypted form?	
GSS-AUTH_11	Is the password minimum length for non-privileged users 6 characters?	
GSS-AUTH-21	Is a warning banner displayed prior to login?	
GSS-AUTH-10	Are password files/password repositories accessible to non-privileged users?	
GSS-AUTH-20	Is an idle timeout facility in use on the desktop?	
GSS-AUTH-19	After a successful log-ons is the date and time of the last log-on, together with details of any unsuccessful attempts since that time, displayed?	
GSS-AUTH-14	Do user account passwords expire ater 60 days?	
GSS-AUTH-7	Are passwords echoed on screen using asterisk characters or similar, rather than plain text?	
GSS-AUTH-22	Are passwords set to be expired following password or account creation?	
GSS-AUTH-6	Do authentication failure messages hide which of the authentication fields are invalid?	
GSS-AUTH-18	Is there a method of preventing the selection of weak, easily guessed passwords?	
GSS-AUTH-4	For above baseline applications, has a strong authentication mechanism been implemented?	
GSS-AUTH-3	For baseline applications, are users required to provide a valid username and password?	
GSS-AUTH-23	Is a desktop software locking facility available to users?	

Checklist

GSS-AU-TH-15	Do administrative accounts have a maximum password lifetime 30 days?	
GSS-AU-TH-16	Do admin user passwords have a maximum lifetime of 7 days?	
GSS-AU-TH-17	Is a password history function enabled preventing the 12 previous passwords being reused?	
GSS-AU-TH-5	Is the user identifier and password validated in a single operation?	
<i>Security Compliance</i>		
<i>Security Compliance Checking</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
GSS-TEST-1	Is it ensured that live data is not supplied to 3rd parties for testing?	
GSS-MANA-9	Do the administrators use analysis tools to detect account weaknesses?	
<i>Security Management</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
GSS-MAN-7	Do the information owners annually audit their user community?	
GSS-PHYS-1	Is physical output afforded appropriate physical protection?	
GSS-DISA-1	Is a recovery plan in place for every system within an acceptable time?	
GSS-MANA-6	Are all files reassigned 6 weeks after a user leaves or deleted?	
GSS-DISA-3	Are the contingency plans kept up to date?	
GSS-DISA-5	Have insurance arrangements been adopted to provide additional protection?	
GSS-DISA-2	Are contingency plans based upon risk analysis?	
GSS-MANA-12	Is it ensured that the change management function ensure that changes do not compromise security controls.	
GSS-AVAI-1	Is static data replicated so as to avoid a single point of failure?	
GSS-MANA-1	Is user administration a clearly defined function with documented procedures	
GSS-MANA-14	Are admin staff trained with clearly defined responsibilities?	
GSS-TEST-2	Is live data for internal testing anonymised before use?	
GSS-MANA-5	Is it ensured that when any individual leaves the organisation all access is disabled immediately?	
GSS-MANA-11	Are all changes to production systems controlled by a change management process?	
GSS-MANA-10	Do all systems have a nominated IT Custodian?	
GSS-DISA-4	Are the contingency plans subject to periodic tests.	
GSS-MANA-15	Are the admin procedures documented, up to date and available to those who need them?	
GSS-INTE-1	Is an undo function available in the user interface for all atomic opera-	

Checklist

	tions?	
GSS-MANA-13	Are emergency changes subject to retrospective approval from the organisations information security function?	
GSS-MANA-3	Is it ensured that old user ids are not re-issued to a new user?	
GSS-MANA-2	Does the addition, modification and deletion of users create an audit trail?	
GSS-MANA-8	Are the registers of users protected from loss and unauthorised access	
<i>Network Security Configuration</i>		
<i>Network Interface Considerations</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
GSS-NET-3	Are all phone lines within the company should periodically swept for wire taps?	
GSS-NET-1	Is switching used on LANs?	
GSS-NET-2	Are modem telephone numbers changed on a periodic basis?	
<i>Internet Considerations</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
GSS-NETW-1	Is encryption used to prevent disclosure of sensitive data whilst in transmission across an untrusted network?	
<i>Configuration</i>		
<i>Administration</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
GSS-AD-MIN-1	iS system administration performed using named accounts owned by the individual administrators?	
<i>Backups</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
GSS-BACK-3	Have the backup recovery timescales between verified as acceptable to the organisation?	
GSS-BACK-2	Are backup media stored securely at a remote location when not in use	
GSS-BACK-4	Ar backups encrypted where it has been identified that highly confidential data is being written?	
GSS-BACK-1	Is the number of times backup media are used recorded and prevented from being used more times than the manufacturers recommended maximum?	
<i>Installation</i>		
<i>Setup Choices</i>		

Checklist

<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
GSS-INST-1	Is the latest version of the operating system installed wherever possible?	
GSS-HARD-2	Is the RAID level selected appropriate to the criticality of the applications and the risks associated with disk failure?	
GSS-HARD-1	Are all servers connected to an uninterruptible power supply?	
GSS-INST-2	Is the most secure implementation of the operating system selected at installation time?	
GSS-INST-3	Are all available patches for the operating system applied?	
<i>Auditing and Monitoring</i>		
<i>Events to be alerted in real-time</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
GSS-ALER-1	Is the system able to detect/alert attempts to breach controls in real time?	
GSS-RESP-1	Does the system have a form of breakin evasion?	
<i>Audit log destination and format</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
GSS-ELOG-4	Has it been ensured that the audit log content is not writable or modifiable by non-privileged users and applications?	
GSS-ELOG-5	Are the audit log records retained for a minimum of thirteen months?	
GSS-ELOG-1	Is the audit/event log only written to by the operating system or trusted apps?	
GSS-ELOG-6	Does the application maintain its own audit trail?	
GSS-ELOG-3	Is the audit log content prevented from access by non-privileged users	
<i>Events to be audited</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
GSS-EVEN-1	Are the events captured must be sufficient to establish accountability for actions?	
GSS-RESP-2	Are audit logs reviewed periodically to identify security incidents or suspicious patterns of events?	
<i>Other</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
GSS-INTE-4	Are cryptographic controls used to verify the integrity of transactions?	
GSS-ELOG-2	Is the audit/event log protected from deletion	
GSS-	Are the encryption keys and algorithms used in encrypting backups pro-	

Checklist

BACK-5	tected against disclosure, alteration or destruction?	
GSS-INTE-2	Are dialogues included in the application interface that seek confirmation prior to committing a sensitive transaction within the application?	