This first page shows the preparation for the videos in the course *Audit Reports that Land*.

The second page shows the report before the meeting. This is shared with the auditee at least one day in advance. That is, when I concluded the testing and found this problem, then straight away I booked the meeting with James Brown in room 301, prepared the Fact Sheet, and sent it to him.

The third page shows the report after the meeting, when the auditee's manager has reviewed it. The changed text is shown here in red, but ordinarily would be the same black text as the rest of the Fact Sheet.

Both the Cause and the Correction result from working with the auditee and management. The Cause is the "why" that identifies the root reason why the condition does not meet the criteria. You may or may not have time to investigate the root reason before you issue the Fact Sheet. Be aware that the easiest reason to attribute to the cause may in fact not be the root cause. It is important that management agrees with the root cause before the Correction can be developed.

Be sure to give the Fact Sheet to the auditee as soon as possible (within one or two business days) after the audit team has completed their tests of the gathered evidence. Ask for a quick response. This ensures the audit team has time to go back and re-examine the design and effectiveness of the controls, before they get involved in the next step of the fieldwork, and before the Fieldwork phase ends.

Audit	GCC Compliance		*Ref*	GCC-2018
Fact Sheet Issue	FS#	7	*WP*	3.13.15
Issue Found	2018-07-19	*Meeting*	2018-07-20	Rm 301
Auditor	Phil Irving	*Auditee*	James Brown	IT User Administr.

Criteria — *Accepted Y/N* — *Enforced Y/N*

Policy – IT User Administration (*internal use only*)

- User accounts should be created only with documented management authorization.
- Access should be unique per user and aligned with job responsibilities.
- Initial passwords must be changed upon first use.
- Periodic reviews should validate user access and account validity.

Policy – IT User Accounting (*internal use only*)

- The name of the user account should not reflect the role of the user

Condition — *Accepted Y/N*

- The organization maintains 1,754 AD accounts for 1,234 users, indicating duplicate or unnecessary accounts.
- In a sample of 200 accounts:
  a. 54 (27%) lacked evidence of management authorization.
  b. 61 (30.5%) retained their initial password.
- There is limited assurance that access permissions align with user roles.
- A predictable naming convention is used for local administrator accounts.

Consequence (Impact) — *Accepted Y/N*

- Increased risk of unauthorized access and privilege misuse.
- Elevated likelihood of account compromise due to unchanged passwords.
- Potential for privilege escalation through duplicate or unmanaged accounts.
- Reduced ability to demonstrate compliance with security and regulatory requirements.
- Predictable administrator account naming increases susceptibility to targeted attacks.

Management has reviewed this finding and: ☐ *Agrees* ☐ *Disagrees*

Date of review		*Manager*	Sheila Rainer	IT Operations

Management Response (in case of disagreement)

Cause (developed with auditee and management)

Recommendations (developed with auditee and management)

For Auditor Use Only

Finding Title:

Cause determined		*Peer Review*		
Finding Number		*Severity*		

Audit	GCC Compliance		*Ref*	GCC-2018
Fact Sheet Issue	FS#	7	*WP*	3.13.15
Issue Found	2018-07-19	*Meeting*	2018-07-20	Rm 301
Auditor	Phil Irving	*Auditee*	James Brown	IT User Administr.
Criteria			*Accepted Y/N* Y	*Enforced Y/N* Y

Policy – IT User Administration (*internal use only*)

- User accounts should be created only with documented management authorization.
- Access should be unique per user and aligned with job responsibilities.
- Initial passwords must be changed upon first use.
- Periodic reviews should validate user access and account validity.

Policy – IT User Accounting (*internal use only*)

- The name of the user account should not reflect the role of the user

Condition — *Accepted Y/N* Y

- The organization maintains 1,754 AD accounts for 1,234 users, indicating duplicate or unnecessary accounts.
- In a sample of 200 accounts:
    c. 54 (27%) lacked evidence of management authorization.
    d. 61 (30.5%) retained their initial password.
- There is limited assurance that access permissions align with user roles.
- A predictable naming convention is used for local administrator accounts.

Impact — *Accepted Y/N* Y

- Increased risk of unauthorized access and privilege misuse.
- Elevated likelihood of account compromise due to unchanged passwords.
- Potential for privilege escalation through duplicate or unmanaged accounts.
- Reduced ability to demonstrate compliance with security and regulatory requirements.
- Predictable administrator account naming increases susceptibility to targeted attacks.

Management has reviewed this finding and: ☑ *Agrees* ☐ *Disagrees*

Date of review	2018-07-23	*Manager*	Sheila Rainer	IT Operations

Management Response (in case of disagreement)

Cause (developed with auditee and management)

- Lack of enforced provisioning controls requiring documented approval.
- Absence of automated or centralized identity governance processes.
- Insufficient monitoring and periodic review of user accounts.
- Weak enforcement of password and administrative account standards

Recommendations (developed with auditee and management)

1. Account Provisioning Controls
    - Enforce mandatory, documented management approval for all new accounts.
    - Implement automated workflows to prevent account creation without approval.
2. Account Rationalization
    - Identify and remove or disable duplicate and unnecessary accounts.
    - Establish a single unique account per user unless formally justified.
3. Password and Authentication Controls
4. Privileged Access Controls
    - Eliminate predictable administrator account naming conventions.
    - Implement stronger controls for administrative accounts (e.g., separate credentials, monitoring).

For Auditor Use Only

Finding Title: Inadequate User Account Authorization and Control

Cause determined	2018-08-07	*Peer Review*	Larry Heinkel	2018-08-14
Finding Number	1	*Severity*	High	