Amana71

Readiness, not certification

COMPLIANCE READINESS REPORT

Demo Trading LLC

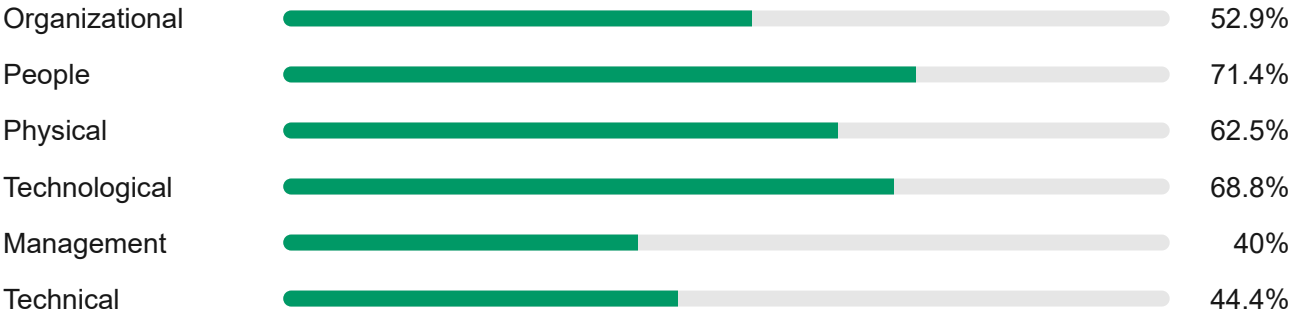
ISO/IEC 27001:2022 — Annex A reference controls · UAE Information Assurance Standard

23 September 2026 · Content library v0.5.0

51.6% Developing

At 51.6% readiness, Demo Trading LLC has solid foundations and is on a credible path. A focused push on the remaining gaps — especially the partly-implemented controls — would bring it close to audit-ready.

SCORE BY THEME



FRAMEWORK COMPARISON

Framework	Readiness	Controls	Met	Partial	Not met
ISO/IEC 27001:2022 — Annex A reference controls	60.3% (Developing)	34	12	16	6
UAE Information Assurance Standard	42.9% (Early stage)	14	0	12	2

TOP 10 GAPS TO CLOSE FIRST

1. Is it clear who is responsible for information security, and does that person have the authority to act? — Low effort

Partly in place · Fails A.5.2 (Defined security roles and who holds them), M1 (Security strategy and planning)

Evidence needed: Document naming the security owner and their responsibilities

2. Is information encrypted while travelling over the internet between you and customers or suppliers? — Low effort

Not in place · Fails A.8.24 (Use of encryption), T4 (Protecting information in transit)

Evidence needed: Evidence that external services use TLS/HTTPS; no plaintext transfer of sensitive data

3. Do staff know how to report a suspected security problem, and who to tell? — Low effort

Partly in place · Fails A.5.24 (Planning and preparing for incidents), A.6.8 (How staff report security events), M3 (Security awareness and training), T8 (Information security incident management)

Evidence needed: Reporting instructions communicated to staff (e.g. an email address, hotline, or intranet page)

4. Do you know who has been into the areas where sensitive information is handled? — Low effort

Partly in place · Fails A.7.2 (Controlling physical entry), A.7.4 (Monitoring premises for unauthorised access), T2 (Physical and environmental security)

Evidence needed: Visitor log, access-control report, or CCTV coverage of the sensitive area

5. Are staff expected to put sensitive papers away and lock their screens when they leave their desk? — Low effort

Not in place · Fails A.7.7 (Clear desk and clear screen), T2 (Physical and environmental security)

Evidence needed: Clear-desk and screen-lock rule, plus device settings showing automatic locking

6. Does every person have their own named login, with no shared or generic accounts for day-to-day work? — Medium effort

Partly in place · Fails A.5.15 (Rules for granting and controlling access), T5 (Access control)

Evidence needed: User list showing individual named accounts; confirmation that shared accounts are disabled or restricted

7. When someone joins, changes role, or leaves, is their system access granted or removed promptly through a defined process? — Medium effort

Not in place · Fails A.5.18 (Granting, reviewing and removing access rights), M4 (People security through the employment lifecycle)

Evidence needed: Joiner/mover/leaver checklist or ticket history showing access changes tied to HR events

8. Is stored data encrypted on laptops, servers, and mobile devices so it can't be read if a device is lost or stolen? Medium effort

Partly in place · Fails A.8.24 (Use of encryption), T6 (Protection of stored information)

Evidence needed: Configuration or policy showing disk/device encryption is enabled across company devices

9. Before you take on a supplier who will handle your data, do you check how they protect it? Medium effort

Partly in place · Fails A.5.19 (Managing security risk from suppliers), A.5.21 (Security across the ICT supply chain), T7 (Third-party and supplier security)

Evidence needed: Completed supplier security assessment, certificate, or due-diligence record for at least the most important suppliers

10. Do your supplier contracts say what the supplier must do to keep your information safe? Medium effort

Not in place · Fails A.5.20 (Security requirements written into supplier agreements), T7 (Third-party and supplier security)

Evidence needed: Contract or terms containing security and confidentiality clauses

FULL GAP REGISTER

Access Control

Does every person have their own named login, with no shared or generic accounts for day-to-day work? — Medium effort

Partly in place · Fails A.5.15 (Rules for granting and controlling access), T5 (Access control)

Evidence needed: User list showing individual named accounts; confirmation that shared accounts are disabled or restricted

When someone joins, changes role, or leaves, is their system access granted or removed promptly through a defined process? — Medium effort

Not in place · Fails A.5.18 (Granting, reviewing and removing access rights), M4 (People security through the employment lifecycle)

Evidence needed: Joiner/mover/leaver checklist or ticket history showing access changes tied to HR events

Data Protection

Is information encrypted while travelling over the internet between you and customers or suppliers? — Low effort

Not in place · Fails A.8.24 (Use of encryption), T4 (Protecting information in transit)

Evidence needed: Evidence that external services use TLS/HTTPS; no plaintext transfer of sensitive data

Is stored data encrypted on laptops, servers, and mobile devices so it can't be read if a device is lost or stolen? — Medium effort

Partly in place · Fails A.8.24 (Use of encryption), T6 (Protection of stored information)

Evidence needed: Configuration or policy showing disk/device encryption is enabled across company devices

Governance

Is it clear who is responsible for information security, and does that person have the authority to act? — Low effort

Partly in place · Fails A.5.2 (Defined security roles and who holds them), M1 (Security strategy and planning)

Evidence needed: Document naming the security owner and their responsibilities

Are sensitive tasks split so that one person cannot carry out and hide a damaging action alone? — Medium effort

Not in place · Fails A.5.3 (Separating conflicting duties)

Evidence needed: Description of separated duties, or the compensating review where separation is not possible

Are your day-to-day IT and security procedures written down well enough that someone else could follow them? Medium effort

Partly in place · Fails A.5.37 (Documented operating procedures)

Evidence needed: Documented operating procedures for the main recurring IT and security tasks

Is security thought about at the start of new projects and system changes, rather than after they go live? Medium effort

Not in place · Fails A.5.8 (Security built into project management)

Evidence needed: Project process showing a security step, or completed security checks for a recent project

Incident Response

Do staff know how to report a suspected security problem, and who to tell? Low effort

Partly in place · Fails A.5.24 (Planning and preparing for incidents), A.6.8 (How staff report security events), M3 (Security awareness and training), T8 (Information security incident management)

Evidence needed: Reporting instructions communicated to staff (e.g. an email address, hotline, or intranet page)

After a security incident or near miss, do you review what happened and record any improvements? Low effort

Not in place · Fails T8 (Information security incident management)

Evidence needed: Post-incident review notes or lessons-learned record

People Security

When someone leaves, do they return all equipment and get reminded of the obligations that continue afterwards? Low effort

Not in place · Fails A.5.11 (Return of assets when people leave), A.6.5 (Obligations that continue after employment ends)

Evidence needed: Leaver checklist covering asset return and a record of the confidentiality reminder

Is there a disciplinary process that applies if someone deliberately breaks the security rules? Low effort

Partly in place · Fails A.6.4 (Disciplinary process for security breaches)

Evidence needed: Disciplinary procedure referencing information security breaches

Physical Security

Do you know who has been into the areas where sensitive information is handled? Low effort

Partly in place · Fails A.7.2 (Controlling physical entry), A.7.4 (Monitoring premises for unauthorised access), T2 (Physical and environmental security)

Evidence needed: Visitor log, access-control report, or CCTV coverage of the sensitive area

Are staff expected to put sensitive papers away and lock their screens when they leave their desk? Low effort

Not in place · Fails A.7.7 (Clear desk and clear screen), T2 (Physical and environmental security)

Evidence needed: Clear-desk and screen-lock rule, plus device settings showing automatic locking

Supplier Security

Before you take on a supplier who will handle your data, do you check how they protect it? Medium effort

Partly in place · Fails A.5.19 (Managing security risk from suppliers), A.5.21 (Security across the ICT supply chain), T7 (Third-party and supplier security)

Evidence needed: Completed supplier security assessment, certificate, or due-diligence record for at least the most important suppliers

Do your supplier contracts say what the supplier must do to keep your information safe? Medium effort

Not in place · Fails A.5.20 (Security requirements written into supplier agreements), T7 (Third-party and supplier security)

Evidence needed: Contract or terms containing security and confidentiality clauses

90-DAY ROADMAP

0–30 days

Is it clear who is responsible for information security, and does that person have the authority to act?

Is information encrypted while travelling over the internet between you and customers or suppliers?

Do staff know how to report a suspected security problem, and who to tell?

Do you know who has been into the areas where sensitive information is handled?

Are staff expected to put sensitive papers away and lock their screens when they leave their desk?

Does every person have their own named login, with no shared or generic accounts for day-to-day work?

31–60 days

When someone joins, changes role, or leaves, is their system access granted or removed promptly through a defined process?

Is stored data encrypted on laptops, servers, and mobile devices so it can't be read if a device is lost or stolen?

Before you take on a supplier who will handle your data, do you check how they protect it?

Do your supplier contracts say what the supplier must do to keep your information safe?

After a security incident or near miss, do you review what happened and record any improvements?

When someone leaves, do they return all equipment and get reminded of the obligations that continue afterwards?

61–90 days

Is there a disciplinary process that applies if someone deliberately breaks the security rules?

Are sensitive tasks split so that one person cannot carry out and hide a damaging action alone?

Are your day-to-day IT and security procedures written down well enough that someone else could follow them?

Is security thought about at the start of new projects and system changes, rather than after they go live?

EVIDENCE CHECKLIST

Have (16)

✓ Screenshot or policy showing multi-factor sign-in enabled for remote and admin access

✓ Dated access review record with reviewer sign-off

✓ Data inventory or information asset register listing personal/sensitive data and its location

✓ Backup schedule plus a record of at least one successful test restore

✓ Approved information security policy showing an approval date and evidence it was issued to staff

✓ Risk register or assessment showing identified risks, their rating, and the treatment decision

✓ Record of a compliance check or internal review, with findings and follow-up

✓ Incident response plan document listing roles and first-response steps

✓ Evidence of alerting rules or a record of periodic log review

✓ Record that pre-employment checks were completed, held on the personnel file

✓ Training records showing who was trained and when, plus the material covered

✓ Signed confidentiality or non-disclosure agreements on file

✓ Description of the secured area and how entry is controlled (key holders, badge list, or lock register)

✓ Written rule covering equipment taken off site, and a route for reporting loss

✓ Supplier or third-party register naming each provider and what data or access they have

✓ Dated supplier review records showing periodic reassessment

Missing (16)

○ User list showing individual named accounts; confirmation that shared accounts are disabled or restricted

○ Joiner/mover/leaver checklist or ticket history showing access changes tied to HR events

○ Configuration or policy showing disk/device encryption is enabled across company devices

○ Evidence that external services use TLS/HTTPS; no plaintext transfer of sensitive data

○ Document naming the security owner and their responsibilities

○ Description of separated duties, or the compensating review where separation is not possible

○ Documented operating procedures for the main recurring IT and security tasks

○ Project process showing a security step, or completed security checks for a recent project

○ Reporting instructions communicated to staff (e.g. an email address, hotline, or intranet page)

○ Post-incident review notes or lessons-learned record

○ Disciplinary procedure referencing information security breaches

○ Leaver checklist covering asset return and a record of the confidentiality reminder

○ Visitor log, access-control report, or CCTV coverage of the sensitive area

○ Clear-desk and screen-lock rule, plus device settings showing automatic locking

○ Completed supplier security assessment, certificate, or due-diligence record for at least the most important suppliers

○ Contract or terms containing security and confidentiality clauses

SCOPE AND LIMITATIONS

This report is based on self-reported answers and has not been audited or independently verified. It reflects readiness against ISO/IEC 27001:2022 — Annex A reference controls and UAE Information Assurance Standard, scored against content library v0.5.0. All 57 control mappings in this version are pending review by a certified assessor and should be treated as indicative until verified.

This assessment covers 43 of the 93 controls in ISO/IEC 27001:2022 — Annex A reference controls and 14 of the 15 controls in UAE Information Assurance Standard. Controls outside that set were not assessed and are not counted in the scores above.

Amana71 is a readiness and documentation tool. It is not an audit, certification, or accredited assessment service, and is not affiliated with any regulator or certification body. Responses are self-reported and unverified. The company remains solely accountable for its compliance obligations.

Amana71 is a readiness and documentation tool. It is not an audit, certification, or accredited assessment service, and is not affiliated with any regulator or certification body. Responses are self-reported and unverified. The company remains solely accountable for its compliance obligations.