ANSI Technologies
Executive Downloadable Asset

CYBERSECURITY READINESS ASSET

UAE Cybersecurity Readiness Checklist for SMEs

A leadership-ready checklist for identity, email, endpoints, backup, data sharing, vendors and incident readiness.

Built for	UAE SMEs, founders, CFOs, operations leaders and IT decision makers
Includes	Checklists, governance tables, selection criteria and next actions
Prepared by	ANSI Technologies - consulting, managed IT, ERP, Microsoft, cybersecurity and CTO advisory

Visit ANSI Technologies | Request a consultation

Executive summary

Cybersecurity readiness for UAE SMEs should be practical, measurable and aligned with business risk. This checklist helps leadership review identity access, email protection, endpoint controls, backup, network security, data sharing, vendor access, incident readiness and governance cadence.

Use this as a readiness guide

This is not a substitute for a formal audit, but it gives a clear starting point for risk reduction and executive technology governance.

Explore cybersecurity services

Cybersecurity readiness model

Readiness area	Minimum target state	Why it matters
Identity and access	MFA, least privilege, admin review, leaver process and role-based access.	Most incidents start with compromised or excessive access.
Email security	Anti-phishing controls, spoofing protection, suspicious forwarding review and user reporting.	Email remains a high-risk entry point for fraud and malware.
Endpoint security	Endpoint protection, patch visibility, encryption expectations and device inventory.	Unknown or unmanaged devices increase breach impact.
Backup and recovery	Backup monitoring, restore testing, critical system list and recovery expectations.	Recovery confidence matters more than backup claims.
Network and firewall	Firewall rules, VPN access, Wi-Fi separation, documentation and ISP escalation plan.	Weak network governance increases downtime and exposure.
Data protection	Controlled file sharing, sensitive folders, access review and retention expectations.	Reduces accidental leakage and uncontrolled data sprawl.
Vendor access	Approved vendor accounts, time-bound access, MFA, logging and access removal.	Vendors often hold powerful access to systems.
Incident readiness	Contact list, escalation path, evidence preservation and decision authority.	Fast response reduces business impact.

Priority risk matrix

Risk	Early warning sign	Priority action
Account compromise	MFA missing, shared admin accounts, many global admins or old leaver accounts.	Enforce MFA, separate admin accounts and run monthly access reviews.
Invoice fraud and phishing	Users report fake payment requests, spoofed domains or suspicious forwarding.	Harden email security, review forwarding rules and train finance users.
Ransomware impact	Backups not tested, endpoints unmanaged or users store files locally.	Validate backups, endpoint protection and restore process.
Data leakage	Anonymous sharing links, excessive guest access or unmanaged file libraries.	Review sharing policies, guests and sensitive folders.
Vendor access abuse	Old vendor accounts, shared passwords or no activity review.	Create named vendor accounts, MFA and time-bound access.
Downtime from weak infrastructure	Firewall undocumented, no spare ISP plan or no network diagram.	Document infrastructure and define escalation plan.

90-day cybersecurity improvement plan

Timeline	Focus	Outcome
Days 1 to 30	Identity, admin access, MFA, leaver accounts, email forwarding and backup visibility.	Fast reduction of common high-impact risks.
Days 31 to 60	Endpoint posture, firewall review, SharePoint sharing, vendor access and security documentation.	Better operational control and reduced exposure.
Days 61 to 90	Incident response checklist, restore testing, management reporting and recurring security governance.	Repeatable readiness and leadership visibility.

Cybersecurity readiness checklist

Check	Control or decision point	Owner / Notes
[ ]	MFA is enforced for all users and admins, with exceptions approved.	
[ ]	All admin accounts are named, separate and reviewed monthly.	
[ ]	Leaver access is removed from Microsoft 365, ERP, CRM, VPN and shared drives.	
[ ]	Email forwarding rules and suspicious inbox rules are reviewed.	
[ ]	Endpoint protection and device inventory are reviewed monthly.	
[ ]	Backups are monitored and at least one restore test is documented.	
[ ]	External sharing and guest access are reviewed in collaboration tools.	
[ ]	Vendors use named accounts with time-bound access and MFA where possible.	
[ ]	Firewall, VPN, Wi-Fi and remote access are documented.	
[ ]	Incident contact list and escalation path are known to management.	
[ ]	Cybersecurity risk is reported to leadership every month.	

Relevant ANSI Technologies pages

Relevant ANSI Technologies pages	Use this when you need
Cybersecurity Services	Security governance, hardening, risk reduction and advisory.
VAPT Assessment	Vulnerability assessment and penetration testing support.
Microsoft Security	Identity, endpoint, email and Microsoft security controls.
Backup and DR Solutions	Backup strategy, restore confidence and business continuity.
Managed IT Services	Ongoing IT support and security operations discipline.
CTO as a Service	Executive technology governance and vendor risk oversight.

Recommended next step

Start with a cybersecurity readiness review across identity, email, devices, backup, data sharing, vendor access and incident readiness.

Book cybersecurity readiness review

Work with ANSI Technologies

ANSI Technologies helps UAE businesses plan, secure and modernize technology with practical consulting, managed IT, ERP advisory, Microsoft 365, cybersecurity, cloud and CTO-level governance. Use this asset as a starting point, then convert it into a focused review, roadmap or implementation plan for your business.

Next step	How ANSI Technologies can help
Request Consultation	Book a discovery call to review your current setup, risks, vendor scope or project roadmap.
CTO as a Service	Get executive-level technology direction, architecture review, cybersecurity governance and vendor oversight.
Managed IT Services	Outsource daily IT support with governance, reporting, Microsoft 365 support and infrastructure management.
Cybersecurity Services	Improve security readiness across identity, endpoint, email, backup, data access and incident response.
ERP Consulting	Plan ERP selection, RFP, process design and implementation governance across Zoho, Odoo and SAP.

Prepared for linkable blog downloads

This PDF is designed to sit in the /downloads folder and support blog readers who want a practical, shareable business asset from ANSI Technologies.

Visit ANSI Technologies

Download file name: uae-cybersecurity-readiness-checklist.pdf