Company: TECH SOLUTIONS
System/Project: Hybrid Cloud Infrastructure – Abu Dhabi Region
Prepared by: Petras Guilherme Kulyumba
Date: December 2, 2025
Framework Compliance: ADSIC, NESA, NIST 800-30, ISO 27005

Executive Summary

This comprehensive risk assessment examines the cybersecurity risks associated with TECH SOLUTIONS hybrid cloud infrastructure operating in Abu Dhabi, United Arab Emirates. The assessment focuses on compliance with Abu Dhabi Systems and Information Centre (ADSIC) security standards, NESA regulations, and internationally recognized frameworks. Critical vulnerabilities have been identified, threats analyzed, and a robust control framework proposed to ensure secure operations.

1. System / Asset Information

- **Asset Name:** Abu Dhabi Hybrid Cloud Infrastructure
- **Description:** Integrated hybrid environment featuring Abu Dhabi On-Premises data center combined with cloud resources hosted in UAE availability zones (AWS/Azure Middle East regions)
- **Owner:** TECH SOLUTIONS
- **Environment:** Hybrid Cloud (On-Prem + multi-cloud)
- **Classification:** Critical / Sensitive
- **Location:** Abu Dhabi, United Arab Emirates
- **Regulatory Requirements:** ADSIC Security Standards, NESA Cybersecurity Controls
- **Data Residency:** UAE-based with geo-replication restrictions

2. Purpose of Assessment

To conduct a thorough evaluation of cybersecurity threats, vulnerabilities, and risks affecting the Abu Dhabi hybrid cloud infrastructure while ensuring full compliance with Abu Dhabi Systems and Information Centre (ADSIC) standards, National Electronic Security Authority (NESA) regulations, and NIST 800-30 risk management framework.

3. Assessment Scope

In-Scope Components:

- On-premises data center infrastructure (compute, storage, networking)
- Cloud services across AWS and Azure UAE regions
- Hybrid connectivity and VPN tunnels
- Identity and Access Management (IAM) systems
- Application Programming Interface (API) layer
- Database systems (both on-premises and cloud-hosted)
- Backup and disaster recovery systems
- Data synchronization and replication mechanisms
- Remote workforce access infrastructure

Data Classification:

- **Highly Sensitive:** Customer financial data, PII, authentication credentials
- **Sensitive:** Business intelligence, internal communications, contracts
- **Internal:** Operational data, logs, system configurations
- **Public:** Marketing materials, public documentation

4. Threat Landscape Analysis

Threat ID	Threat Category	Threat Description	Threat Actor
T1	Unauthorized Access	Credential stuffing attacks, brute force attempts targeting authentication systems	External Hackers, Nation-State Actors
T2	Cloud Misconfiguration	Improperly configured cloud resources including exposed VMs, inadequate access controls, open databases	Internal Personnel, Third-Party Vendors
T3	Ransomware Attack	Advanced persistent threats deploying ransomware targeting servers, endpoints, and cloud workloads	Organized Crime Groups
T4	Insider Threat	Malicious or negligent insiders with administrative privileges accessing or exfiltrating sensitive data	Employees, Contractors
T5	Data Integrity Compromise	Unauthorized modification or deletion of critical cloud-based data affecting business operations	Advanced Persistent Threats

T6	Man-in-the-Middle Attack	Interception of unencrypted network traffic between on-premises and cloud environments	Network-based Attackers
T7	Compliance Violation	Failure to meet ADSIC/NESA regulatory requirements resulting in penalties and operational restrictions	N/A - Regulatory Risk
T8	Supply Chain Attack	Compromise through third-party software, cloud service provider vulnerabilities, or vendor systems	Nation-State Actors, APTs
T9	Zero-Day Exploitation	Attacks leveraging unknown vulnerabilities in systems or applications	Advanced Threat Actors
T10	Cloud Account Hijacking	Takeover of cloud administrative accounts through phishing or credential theft	External Hackers

5. Vulnerability Assessment

Vulnerability ID	Vulnerability Name	CVSS Score	Description	Affected Systems
V1	Inadequate IAM Implementation	8.1 (High)	Over-privileged cloud accounts, lack of least privilege principle, no regular access reviews	Cloud IAM, AD
V2	Missing Encryption Controls	8.8 (High)	Data at rest and in transit not consistently encrypted across all systems	Storage, Databases
V3	Delayed Patch Management	7.5 (High)	Extended patch cycles leading to exposure of known vulnerabilities	Servers, VMs, Endpoints
V4	Absence of Cloud Backup Strategy	7.2 (High)	No comprehensive disaster recovery plan, incomplete backup coverage	Cloud Infrastructure
V5	Insufficient Security Monitoring	6.9 (Medium)	Limited SIEM deployment, incomplete log	Network, Cloud

			collection, no automated threat detection	
V6	Flat Network Architecture	7.8 (High)	Lack of network segmentation enabling lateral movement	Network Infrastructure
V7	Weak Authentication Mechanisms	8.6 (High)	Single-factor authentication for privileged accounts	Authentication Systems
V8	Inadequate API Security	7.4 (High)	Missing API gateways, weak authentication, no rate limiting	Application Layer
V9	Poor Configuration Management	6.5 (Medium)	Inconsistent security baselines, drift from standards	All Systems
V10	Limited Incident Response Capability	5.8 (Medium)	No formal IR plan, untested procedures	Security Operations

6. Comprehensive Risk Analysis

Risk ID	Threat Source	Vulnerability Exploited	Likelihood	Impact	Risk Rating	Business Impact
R1	Unauthorized Access (T1)	V1, V7	High	High	**Critical**	Complete system compromise, data breach
R2	Data Integrity Attack (T5)	V2, V5	High	High	**Critical**	Loss of data trustworthiness, regulatory violations
R3	Ransomware (T3)	V3, V6	Medium	High	**High**	Operational shutdown, financial loss
R4	Compliance Failure (T7)	V4, V9	Medium	High	**High**	Regulatory penalties, license suspension
R5	Insider Privilege Abuse (T4)	V1, V5	Medium	Medium	**Medium**	Data leakage, intellectual property theft

R6	MITM Attack (T6)	V2, V6	Medium	Medium	**Medium**	Data interception, credential theft
R7	Supply Chain Compromise (T8)	V9, V10	Low	High	**Medium**	Backdoor access, long-term compromise
R8	Cloud Account Hijacking (T10)	V7, V8	Medium	High	**High**	Unauthorized resource usage, data access
R9	Zero-Day Exploitation (T9)	V10	Low	High	**Medium**	Unpredictable system compromise

Risk Calculation Methodology:

Risk Score = Likelihood × Impact × Asset Value

- **Likelihood:** Low (1), Medium (2), High (3)
- **Impact:** Low (1), Medium (2), High (3)
- **Asset Value Multiplier:** Critical assets (×2)

7. Recommended Security Controls

7.1 Technical Controls

Identity and Access Management

1. **Zero Trust Architecture Implementation**
    a. Implement "never trust, always verify" model
    b. Microsegmentation of network resources
    c. Continuous authentication and authorization
2. **Multi-Factor Authentication (MFA)**
    a. Mandatory MFA for all user accounts
    b. Hardware tokens for privileged administrators
    c. Biometric authentication for critical systems
3. **Privileged Access Management (PAM)**
    a. Just-in-time (JIT) privileged access
    b. Session recording and monitoring
    c. Automated credential rotation

Data Protection

4. **Comprehensive Encryption Strategy**
    a. AES-256 encryption for data at rest
    b. TLS 1.3 for all data in transit
    c. End-to-end encryption for sensitive communications
    d. Hardware Security Module (HSM) for key management
5. **Data Loss Prevention (DLP)**
    a. Content inspection and filtering
    b. Automated data classification
    c. Egress monitoring and blocking

Infrastructure Security

6. **Advanced Patch Management**
    a. Automated vulnerability scanning (weekly)
    b. Critical patch deployment within 48 hours
    c. Regular patch deployment every 14 days
    d. Virtual patching for legacy systems
7. **Network Segmentation**
    a. VLAN implementation for logical separation
    b. Micro-segmentation in cloud environments
    c. Software-defined perimeter (SDP)
    d. DMZ for external-facing services
8. **Security Information and Event Management (SIEM)**
    a. Enterprise SIEM deployment (Splunk Enterprise, Azure Sentinel)
    b. Real-time correlation and analysis
    c. Automated incident detection and alerting
    d. Integration with threat intelligence feeds
9. **Cloud Security Posture Management (CSPM)**
    a. Continuous compliance monitoring
    b. Automated misconfiguration detection
    c. Cloud workload protection platform (CWPP)
10. **Backup and Disaster Recovery**
    a. 3-2-1 backup strategy implementation
    b. Air-gapped offline backup storage
    c. Geo-redundant backup locations within UAE
    d. Quarterly DR testing and validation

Application Security

11. **API Security Gateway**
    a. Centralized API management
    b. OAuth 2.0 / OpenID Connect authentication
    c. Rate limiting (1000 requests/minute per client)
    d. Input validation and sanitization
    e. API security testing (OWASP API Top 10)
12. **Web Application Firewall (WAF)**
    a. Layer 7 protection for web applications
    b. OWASP Top 10 vulnerability protection
    c. Custom rule sets for Abu Dhabi compliance
13. **Container and Kubernetes Security**
    a. Image scanning before deployment
    b. Runtime protection and monitoring
    c. Network policies for pod communication

7.2 Administrative Controls

Governance and Compliance

1. **Policy Framework Development**
    a. Information Security Policy aligned with ADSIC
    b. Cloud Security Policy
    c. Acceptable Use Policy
    d. Data Classification and Handling Policy
    e. Incident Response Policy
2. **Compliance Management**
    a. Quarterly ADSIC compliance audits
    b. Annual NESA cybersecurity assessment
    c. ISO 27001 certification maintenance
    d. Documentation of all compliance activities
3. **Risk Management Program**
    a. Annual comprehensive risk assessments
    b. Quarterly risk register reviews
    c. Continuous risk monitoring
    d. Risk treatment plan tracking

Human Resources Security

4. **Security Awareness and Training**
    a. Mandatory onboarding security training
    b. Quarterly cybersecurity awareness sessions
    c. Monthly phishing simulation exercises
    d. Role-based security training for developers, admins
5. **Access Control Procedures**
    a. Monthly privileged access reviews
    b. Quarterly user access recertification
    c. Immediate access revocation upon termination
    d. Separation of duties enforcement
6. **Background Checks**
    a. Pre-employment security screening
    b. Periodic re-verification for privileged users
    c. Third-party vendor personnel verification

Vendor and Third-Party Management

7. **Vendor Risk Assessment**
    a. Annual security assessments of cloud providers
    b. Due diligence for new vendors
    c. Contractual security requirements (SLA, data protection)
    d. Regular vendor security posture reviews
8. **Incident Response and Business Continuity**
    a. Formal incident response plan (IRP)
    b. 24/7 security operations center (SOC)
    c. Defined escalation procedures
    d. Business continuity plan with RPO/RTO objectives
    e. Annual tabletop exercises

7.3 Physical Controls

1. **Data Center Security**
    a. 24/7 CCTV surveillance with 180-day retention
    b. Biometric access control systems
    c. Mantrap entry systems
    d. Security guard presence
    e. Visitor escort requirements
2. **Environmental Controls**

a. Fire suppression systems
b. Temperature and humidity monitoring
c. Uninterruptible Power Supply (UPS)
d. Redundant power feeds

3. **Endpoint Security**
    a. Full disk encryption (BitLocker for Windows, FileVault for macOS)
    b. Mobile Device Management (MDM)
    c. Remote wipe capabilities
    d. Anti-theft tracking
4. **Secure Disposal**
    a. Certified data destruction services
    b. Physical media shredding
    c. Degaussing for magnetic media
    d. Certificate of destruction documentation

8. Residual Risk Assessment

Risk ID	Original Rating	Applied Controls	Residual Risk	Justification
R1	Critical	MFA, PAM, Zero Trust, SIEM	**Low**	Multi-layered authentication significantly reduces unauthorized access
R2	Critical	AES-256 encryption, integrity monitoring, DLP	**Low**	Comprehensive data protection prevents manipulation
R3	High	Automated patching, EDR, segmentation, backups	**Medium**	Regular patching and backups mitigate ransomware impact
R4	High	CSPM, compliance automation, SIEM	**Low**	Continuous monitoring ensures ADSIC/NESA compliance
R5	Medium	Monthly access reviews, PAM, SIEM alerts	**Low**	Enhanced monitoring detects insider threats early

R6	Medium	TLS 1.3, VPN, network segmentation	**Low**	Encryption eliminates MITM attack vectors
R7	Medium	Vendor assessments, SBOM, monitoring	**Low**	Rigorous vendor management reduces supply chain risk
R8	High	MFA, PAM, cloud security monitoring	**Medium**	Strong authentication prevents most account hijacking
R9	Medium	Virtual patching, behavioral analysis, SOC	**Medium**	Defense-in-depth approach limits zero-day impact

9. Risk Treatment Decisions

Risk ID	Treatment Strategy	Rationale	Timeline	Responsible Party
R1	**Mitigate**	Critical business asset; cost-effective controls available	30 days	CISO
R2	**Mitigate**	Regulatory requirement under ADSIC; reputational impact	30 days	CTO
R3	**Mitigate**	Ransomware is prevalent threat; backups provide recovery	60 days	Security Team
R4	**Avoid**	Non-compliance leads to operational suspension; mandatory	Immediate	Compliance Officer
R5	**Mitigate**	Insider threats preventable with proper controls	45 days	HR + Security
R6	**Mitigate**	Encryption is standard practice and cost-effective	30 days	Network Team
R7	**Accept with Monitoring**	Low likelihood but requires ongoing vigilance	Continuous	Procurement
R8	**Mitigate**	Cloud account compromise has severe consequences	30 days	Cloud Security Team
R9	**Accept with Monitoring**	Zero-days unpredictable; focus on detection and response	Continuous	SOC

10. Implementation Roadmap

Phase 1: Critical (0-30 days) - Total Budget: $150,000

Priority Items:

- Deploy MFA across all systems ($15,000)
- Enable AES-256 encryption for all cloud storage ($10,000)
- Implement basic SIEM with critical alerts ($45,000)
- Establish privileged access management ($35,000)
- Deploy API gateway with authentication ($25,000)
- Conduct emergency compliance gap assessment ($20,000)

Success Metrics:

- 100% MFA adoption rate
- 0 unencrypted data stores
- SIEM capturing 90%+ of security events

Phase 2: High Priority (30-90 days) - Total Budget: $300,000

Priority Items:

- Complete Zero Trust architecture rollout ($80,000)
- Deploy automated patch management system ($40,000)
- Implement network segmentation and microsegmentation ($70,000)
- Establish 24/7 SOC operations ($60,000)
- Deploy DLP solution ($50,000)

Success Metrics:

- Zero Trust policies covering 80% of resources
- Patch compliance rate >95%
- Mean time to detect (MTTD) <30 minutes

Phase 3: Medium Priority (90-180 days) - Total Budget: $250,000

Priority Items:

- Full SIEM integration with automated playbooks ($70,000)
- Complete network segmentation across all environments ($60,000)

- Implement CSPM with automated remediation ($50,000)
- Establish comprehensive training program ($30,000)
- Deploy container security platform ($40,000)

Success Metrics:

- 90% of incidents handled by automated playbooks
- Network lateral movement reduced by 90%
- Employee security awareness score >85%

Phase 4: Ongoing (180+ days) - Annual Budget: $400,000

Priority Items:

- Continuous compliance monitoring and reporting
- Threat intelligence integration and hunting
- Advanced security analytics and AI/ML-based detection
- Quarterly penetration testing and red team exercises
- Annual disaster recovery drills

11. Compliance Mapping

ADSIC (Abu Dhabi Systems and Information Centre) Requirements

ADSIC Control ID	Control Description	Implementation Status	Evidence
ADSIC-AC-01	Access Control Policy	Implemented	Policy document, access logs
ADSIC-CM-02	Configuration Management	In Progress	CMDB, baseline configs
ADSIC-IR-03	Incident Response	Implemented	IRP document, drill reports
ADSIC-RA-04	Risk Assessment	Implemented	This document
ADSIC-SC-05	System and Communications Protection	In Progress	Encryption status, firewall rules
ADSIC-SI-06	System and Information Integrity	In Progress	Integrity monitoring logs

NESA (National Electronic Security Authority) Controls

NESA Control	Requirement	Implementation	Gap Analysis
Authentication	Strong authentication mechanisms	MFA deployed	None
Encryption	Protect data confidentiality	AES-256, TLS 1.3	Legacy system encryption pending
Logging	Comprehensive audit trails	SIEM with 90-day retention	Increase to 365 days
Incident Response	Formal IR capability	IR plan established	SOC staffing in progress
Business Continuity	Resilience and recovery	DR plan documented	Annual testing required

NIST 800-30 Compliance

Phase	NIST Requirement	Status
Prepare	Risk assessment preparation	Complete
Conduct	Threat, vulnerability, risk identification	Complete
Communicate	Risk communication to stakeholders	Complete
Maintain	Ongoing monitoring and updates	Continuous

ISO 27005 Compliance

- Context establishment completed
- Risk assessment methodology documented
- Risk treatment plan established
- Risk acceptance documented
- Continuous monitoring framework in development

11.Performance Indicators (KPIs)

KPI	Current Baseline	Target	Measurement Frequency
Mean Time to Detect (MTTD)	45 minutes	<15 minutes	Daily
Mean Time to Respond (MTTR)	4 hours	<2 hours	Daily
Patch Compliance Rate	78%	>95%	Weekly
MFA Adoption Rate	65%	100%	Monthly
Security Training Completion	82%	100%	Quarterly
Vulnerability Remediation SLA	65%	>90%	Monthly

Compliance Score (ADSIC)	72%	>95%	Quarterly
Security Incident Rate	12/month	<5/month	Monthly
Backup Success Rate	94%	>99%	Daily

13. Monitoring and Review

Continuous Monitoring Plan

- **Daily:** SIEM alert review, backup verification, patch status
- **Weekly:** Vulnerability scan analysis, threat intelligence review
- **Monthly:** Access reviews, KPI dashboard review, security metrics
- **Quarterly:** Risk register update, compliance audit, policy review
- **Annually:** Comprehensive risk assessment, penetration testing, DR drill

Review Schedule

- **Next Risk Assessment:** December 2026
- **Interim Reviews:** Quarterly (March, June, September 2026)
- **Compliance Audits:** Quarterly for ADSIC, Annual for NESA
- **Management Review:** Monthly to Executive Committee

14. Conclusion

The Abu Dhabi hybrid cloud infrastructure cybersecurity assessment reveals a mature understanding of the threat landscape with identified critical risks requiring immediate attention. The implementation of recommended controls, aligned with ADSIC, NESA, NIST 800-30, and ISO 27005 frameworks, will establish a robust security posture capable of protecting critical assets and sensitive data.

Key Findings:

- Two critical risks (R1, R2) require immediate mitigation within 30 days
- Compliance gaps exist but are addressable through systematic implementation
- Residual risks are within acceptable tolerance after control implementation
- Investment of approximately $700,000 over 180 days required for full implementation

Strategic Recommendations:

1. Prioritize MFA and encryption deployment immediately
2. Establish 24/7 SOC capability within 90 days
3. Achieve ADSIC compliance certification within 6 months
4. Implement continuous monitoring and improvement culture

With proper execution of the implementation roadmap, the Abu Dhabi hybrid cloud environment will exceed regulatory requirements and industry best practices, positioning TECH SOLUTIONS as a leader in secure cloud operations within the UAE.

15. Approval and Authorization

Role	Name	Signature	Date
Risk Assessment Lead	Petras Kulyumba	_____	_____
Chief Information Security Officer	_____	_____	_____
Chief Technology Officer	_____	_____	_____
Chief Compliance Officer	_____	_____	_____
Chief Executive Officer	_____	_____	_____

16. Appendices

Appendix A: Glossary of Terms

- **ADSIC:** Abu Dhabi Systems and Information Centre
- **NESA:** National Electronic Security Authority
- **PAM:** Privileged Access Management
- **SIEM:** Security Information and Event Management
- **CSPM:** Cloud Security Posture Management
- **Zero Trust:** Security model requiring verification for all access attempts

Appendix B: References

- NIST SP 800-30 Rev. 1 - Guide for Conducting Risk Assessments
- ISO/IEC 27005:2022 - Information Security Risk Management
- ADSIC Information Security Standards
- NESA Cybersecurity Controls Framework

Appendix C: Contact Information

For questions or clarifications regarding this assessment:

- Email: petras.kulyumba@techsolutions.ae
- Phone: +971-XX-XXX-XXXX
- Office: Abu Dhabi, UAE