Company: Tech Solutions

System/Project: Hybrid Cloud Infrastructure (Dubai)

Prepared by: Petras Kulyumba

Date: December 2, 2025

Framework Compliance: NIST 800-30, ISO 27005, Dubai ISR, NESA

Executive Summary

This risk assessment evaluates the cybersecurity posture of Tech Solutions' hybrid cloud infrastructure deployed in Dubai, United Arab Emirates. The assessment identifies critical vulnerabilities, analyzes potential threats, and recommends technical, administrative, and physical controls to mitigate risks in alignment with NIST 800-30, ISO 27005, Dubai ISR, and NESA cybersecurity frameworks.

1. System / Asset Information

- **Asset Name:** Hybrid Cloud Environment (Dubai Region)
- **Description:** Hybrid environment combining On-Premises Data Center in Dubai with AWS/Azure UAE region resources for scalability, storage, and applications
- **Owner:** Tech Solutions
- **Environment:** Hybrid (On-Premises + Cloud)
- **Classification:** Critical (Customer data + company data)
- **Location:** Dubai, United Arab Emirates
- **Components:** Virtual machines, Active Directory, SIEM server, cloud compute, storage, IAM systems

2. Purpose of Assessment

To identify and evaluate cybersecurity risks associated with the Dubai hybrid cloud environment and determine appropriate technical, administrative, and physical controls to ensure compliance with NIST 800-30, ISO 27005, Dubai ISR, and NESA cybersecurity frameworks.

3. Scope

Included Components:

- Dubai On-Premises server infrastructure (VMs, Active Directory, SIEM server)
- Cloud services (AWS/Azure – Compute, Storage, IAM)
- Data transit mechanisms between on-premises and cloud
- User access management and remote access solutions
- Critical business applications and APIs
- Network infrastructure and security controls

Data Types:

- Customer personally identifiable information (PII)
- Authentication and authorization data
- Internal company confidential files
- Business application data

4. Threat Identification

Threat ID	Threat Name	Description
T1	Unauthorized Access	External attackers attempting brute-force attacks against on-premises or cloud accounts to gain unauthorized system access
T2	Ransomware	Malicious software designed to encrypt on-premises servers or cloud virtual machines, demanding payment for decryption
T3	Cloud Misconfiguration	Improperly configured cloud resources including public S3 buckets, weak IAM policies, or open storage containers
T4	Insider Threat	Privileged users misusing access rights for data theft, sabotage, or unauthorized disclosure
T5	Data Leakage	Accidental or intentional exposure of sensitive data through mis-shared links or incorrect access control levels
T6	DDoS Attack	Distributed denial-of-service attacks targeting cloud-facing applications to disrupt availability
T7	API Exploitation	Attackers exploiting API vulnerabilities including injection flaws and broken authentication mechanisms
T8	Physical Server Theft	Physical theft of hardware from the on-premises data center location

5. Vulnerability Identification

Vulnerability ID	**Vulnerability Name**	**Description**
V1	Weak IAM Policies	Excessive permissions granted to users and services, lack of least privilege implementation
V2	Missing Multi-Factor Authentication	Absence of MFA increases risk of account takeover through credential compromise
V3	Unpatched Systems	Outdated operating systems and virtual machines with known security vulnerabilities
V4	Misconfigured Firewall	Open ports, flat network architecture without proper segmentation
V5	Insufficient Encryption	Data exposed during transit or storage without adequate encryption protection
V6	Inadequate Monitoring	Lack of SIEM alerting, logging gaps, insufficient visibility into security events
V7	No VPN for Remote Access	Remote connections without VPN protection susceptible to traffic interception
V8	Shadow IT	Unapproved cloud resources deployed without security oversight or governance

6. Risk Analysis

Risk ID	**Threat**	**Vulnerability**	**Likelihood**	**Impact**	**Risk Rating**
R1	Unauthorized Access (T1)	V1, V2	High	High	Critical
R2	Cloud Data Leak (T5)	V5	High	High	**Critical**
R3	Ransomware (T2)	V3	Medium	High	**High**
R4	Insider Misuse (T4)	V1	Medium	Medium	**Medium**
R5	DDoS Attack (T6)	Infrastructure Exposure	Medium	Medium	**Medium**
R6	Physical Theft (T8)	On-Premises Server	Low	Medium	**Low**

Risk Rating Matrix:

- **Critical:** Immediate action required, severe impact on operations

- **High:** Prioritize remediation within 30 days
- **Medium:** Address within 90 days
- **Low:** Monitor and address during regular maintenance cycles

7. Recommended Controls

Technical Controls

1. **Identity and Access Management**
   a. Enforce Multi-Factor Authentication (MFA) for all user accounts
   b. Implement Zero Trust architecture with least privilege access
   c. Regular automated IAM policy reviews and access certifications
2. **Encryption**
   a. Data at rest: AES-256 encryption for all storage
   b. Data in transit: TLS 1.2 or higher for all communications
   c. Key management through AWS KMS or Azure Key Vault
3. **Patch Management**
   a. Automated patch deployment cycles every 14 days
   b. Critical security patches applied within 48 hours
   c. Vulnerability scanning and assessment tools
4. **Network Security**
   a. Cloud firewall and on-premises firewall configuration
   b. Network segmentation with VLANs
   c. Web Application Firewall (WAF) for internet-facing applications
5. **Security Monitoring**
   a. SIEM implementation (Wazuh, Splunk, or Azure Sentinel)
   b. Real-time alerting for security events
   c. Log retention for minimum 90 days
6. **DDoS Protection**
   a. Cloudflare or AWS Shield implementation
   b. Rate limiting and traffic filtering
   c. Auto-scaling capabilities
7. **API Security**
   a. API gateway with authentication
   b. Rate limiting and throttling

    c. Input validation and sanitization

Administrative Controls

1. **Training and Awareness**
    a. Quarterly cybersecurity awareness training for all staff
    b. Phishing simulation exercises
    c. Security incident response training
2. **Policy and Procedures**
    a. Updated cloud security policy aligned with NESA guidelines
    b. Incident response plan with defined escalation procedures
    c. Business continuity and disaster recovery plan
3. **Access Reviews**
    a. Monthly privileged access reviews
    b. Quarterly user access recertification
    c. Immediate access revocation upon termination
4. **Vendor Management**
    a. Cloud provider security assessment
    b. Third-party risk assessment program
    c. Contractual security requirements

Physical Controls

1. **Facility Security**
    a. CCTV monitoring with 90-day retention
    b. Biometric entry systems for data center access
    c. Access logs and visitor management system
2. **Equipment Security**
    a. Secure server room with environmental controls
    b. Laptop and mobile device encryption (BitLocker/FileVault)
    c. Asset tracking and inventory management

8. Residual Risk Assessment

Risk ID	Original Rating	Applied Controls	Residual Risk

R1	Critical	MFA, Zero Trust IAM, Access Reviews	**Medium**
R2	Critical	Bucket policies, AES-256 encryption, DLP	**Low**
R3	High	Automated patch management, EDR	**Medium**
R4	Medium	Monthly access reviews, SIEM monitoring	**Low**
R5	Medium	DDoS protection, auto-scaling	**Low**
R6	Low	Physical security controls, CCTV	**Low**

9. Risk Decision

Risk ID	**Decision**	**Justification**
R1	**Mitigate**	Critical risk to customer and encrypted data; controls are cost-effective and immediately implementable
R2	**Mitigate**	Regulatory compliance requirement under NESA; data breach would result in significant financial and reputational damage
R3	**Accept**	Medium residual risk acceptable after implementing automated patch management
R4	**Avoid**	Strong administrative controls reduce risk to acceptable levels; additional monitoring provides early detection
R5	**Transfer**	DDoS protection through cloud provider and third-party services transfers majority of risk

10. Implementation Roadmap

Phase 1: Immediate (0-30 days)

- Deploy MFA across all accounts
- Enable encryption for cloud storage
- Implement basic SIEM logging

Phase 2: Short-term (30-90 days)

- Complete Zero Trust IAM implementation
- Deploy automated patch management
- Establish DDoS protection

Phase 3: Long-term (90-180 days)

- Full SIEM integration with automated response
- Complete network segmentation
- Establish comprehensive training program

11. Compliance Mapping

Framework	Requirements Met	Gap Areas
NIST 800-30	Risk assessment methodology, threat identification	Continuous monitoring enhancement needed
ISO 27005	Risk treatment, control implementation	Annual risk review process
Dubai ISR	Data protection, incident response	Quarterly compliance audits
NESA	Technical controls, governance	Enhanced logging capabilities

12. Conclusion

The Dubai hybrid cloud environment presents manageable cybersecurity risks when appropriate controls are implemented. After applying the recommended technical, administrative, and physical controls in alignment with NIST 800-30, ISO 27005, NESA, and Dubai ISR frameworks, the environment will maintain a strong security posture suitable for production operations handling critical and sensitive data.

The residual risk levels are within acceptable thresholds for the organization's risk appetite. Continuous monitoring, regular reviews, and periodic reassessments are recommended to maintain compliance and adapt to emerging threats.

13. Approval and Sign-off

Role	Name	Signature	Date
Risk Assessor	Petras Kulyumba	____________________	________
Chief Information Security Officer	____________________	____________________	________

Chief Technology Officer	____________________	____________________	________
Business Owner	____________________	____________________	________