# Task A.2 - User Needs & Regulatory Requirements

## 1. User Requirements Analysis

| Requirement Type | Details | Priority |  
|----------------------------|----------------------------------------------------------------------------------------------------------|----------|  
| Departments/Facilities | Dedicated spaces for IT, HR, Finance, Admin, Development, Documentation | High |  
| Data Storage | Secure storage for source code, financial data, employee records, and government project files | High |  
| Web Services | Public and internal web servers for company sites and applications | High |  
| DNS & DHCP | Internal DNS for name resolution; DHCP for dynamic IP assignment in internal network | Medium |  
| File Services | Centralized file server with role-based access controls (RBAC) | High |  
| Database Services | Secure databases for applications (MySQL/PostgreSQL), with encryption and regular backups | High |  
| Security & Compliance | ISO27001 compliance, strong firewall, encryption (AES-256), VPN access for remote users | High |  
| Backup & Disaster Recovery | Automated backups to S3 and on-premises; Disaster recovery plan aligned with ISO27001 | High |  
| Remote Access | Secure VPN + SSH/RDP for remote team members and system administrators | Medium |  
| Scalability | Able to scale up to 50 employees and future projects | High |  
| Monitoring & Automation | SNMP/Prometheus monitoring, CloudWatch integration, automated alerting | High |

## 2. Regulatory Requirements

| Compliance Area | Details |  
|--------------------------|--------------------------------------------------------------------------------------------------------|  
| ISO 27001 | Maintain information security best practices, risk management, and regular audits |  
| Data Localization (Bahrain) | Sensitive government data must be stored according to Bahrain’s data protection laws (where applicable) |  
| Access Control | Enforce the principle of least privilege, role-based access |  
| Disaster Recovery | Comply with business continuity and disaster recovery policies |  
| Data Encryption | All data in transit and at rest must be encrypted |  
| Audit Trails | Logging and tracking of system access and critical operations |

## 3. Prioritization of Needs

| Category | Priority Level |  
|------------------|----------------|  
| Security | Critical |  
| Storage | Critical |  
| Network Services | High |  
| Backup & Recovery| High |  
| Compliance | Critical |  
| Scalability | High |