zainTECH

ENSURING CONTINUOUS COMPLIANCE WITH SAUDI NATIONAL CYBERSECURITY AUTHORITY ESSENTIAL CYBERSECURITY CONTROLS (ECC) FOR MICROSOFT 365 ENVIRONMENTS

INTRODUCTION

At ZainTECH, we manage over half a million seats of Microsoft 365 across the region, helping organizations optimize their cloud environments while ensuring robust security and compliance. Through our extensive experience working with government entities, enterprises, and regulated industries, one clear pattern continues to emerge – many organizations underutilize the vast security and compliance capabilities that Microsoft 365 has to offer. Whether due to a lack of awareness, misconfigurations, or the absence of continuous security management, organizations often leave critical gaps that could have been easily addressed through proper deployment and oversight of Microsoft 365's security features.

The cybersecurity threat landscape is evolving rapidly, with attackers constantly developing new tactics to exploit vulnerabilities. Business Email Compromise (BEC) scams, AI-powered phishing campaigns, ransomware targeting cloud workloads, and insider threats have become more sophisticated and frequent. Attackers are also leveraging token theft and session hijacking to bypass traditional security controls, allowing them to infiltrate environments undetected. Without properly configuring and continuously managing Identity Protection, Conditional Access Policies, Threat Intelligence, Endpoint Detection & Response (EDR), and Compliance Monitoring, organizations remain at heightened risk.

The Middle East has become a prime target for cyber threats due to its rapid digital transformation and strategic economic sectors. Nation-state actors and cybercriminal groups are increasingly targeting financial institutions, oil and gas companies, government agencies, and cloud infrastructure providers.

This rising risk is why we developed our Managed Microsoft 365 offering – to help organizations across the region fully leverage their Microsoft 365 investment, enhance their security posture, and protect their digital assets through a continuous, proactive security management service. With ZainTECH as a trusted partner, organizations can stay ahead of threats, maintain compliance, and build cyber resilience in today's dynamic threat landscape.

Kamran Ahsan
Head of Cybersecurity Business
ZainTECH

Christopher Ross
Head of Internal IT Security
ZainTECH

EXECUTIVE SUMMARY

Saudi Arabia's National Cybersecurity Authority (NCA) has established the Essential Cybersecurity Controls (ECC) as a mandatory framework to enhance cybersecurity resilience across government entities and organizations managing critical infrastructure. Compliance with ECC is essential for organizations operating in the Kingdom, as non-compliance can lead to significant legal, financial, operational and reputational risks.

Most organizations have invested in M365, which provides a robust security framework and a strong foundation to meet NCA ECC requirements. However, many organizations do not fully utilize the security capabilities within M365, leaving potential vulnerabilities unaddressed. While M365 offers a suite of built-in security tools, such as Identity Protection, Threat Intelligence, and Data Governance, these features require continuous management, monitoring, and fine-tuning to effectively secure an organization's environment. Without dedicated oversight, organizations may fail to implement best practices, optimize security configurations, and respond proactively to emerging threats.

MICROSOFT 365 – A ROBUST, YET OFTEN UNDERUTILIZED PLATFORM

Most organizations fail to fully capitalize on their investments in M365 – not deploying or correctly configure the vast array of security capabilities available within M365. While Microsoft provides powerful tools for Identity & Access Management, Endpoint Management, Data Loss Prevention (DLP), Compliance & eDiscovery, Threat Protection, and Security Monitoring from email to endpoint, organizations often lack the expertise or resources to properly configure and integrate these solutions. Without a structured approach to policy enforcement, automation, and governance, many organizations leave critical security gaps, resulting in an incomplete and ineffective security posture.

Even for organizations that initially configure their M365 security settings correctly, security drift becomes a major challenge over time. Security drift refers to the gradual deterioration of an organization's security posture due to both environmental changes and evolving platform capabilities. Organizations that achieve a high Microsoft Secure Score – a Microsoft-provided security rating that reflects how well security controls are implemented – often see their score drop by 20 to 30 points within just three months. This happens because of two primary reasons:

1. The dynamic nature of enterprise IT environments, where users leave, passwords expire, and new software and applications are deployed.
2. Microsoft continually introduces new security features and controls that require manual configuration to maintain an optimal security posture.

Without dedicated oversight and ongoing management, organizations quickly fall behind, exposing themselves to unnecessary risks and compliance gaps.

STREAMLINING ECC COMPLIANCE WITH MANAGED M365

ZainTECH's Managed M365 Service was developed to help organizations fully capitalize on their M365 investments by ensuring they maximize the security and compliance capabilities of the platform. Our service not only fully configures M365 security controls across Identity & Access Management, Endpoint Protection, Data Governance, and Compliance Monitoring, but also provides continuous management to eliminate security drift. Through proactive tuning, regular security audits, and automated remediation, our team ensures that security configurations remain aligned with evolving best practices and Microsoft's latest capabilities, enabling organizations to stay ahead of threats and maintain a strong security posture at all times.

By leveraging M365's extensive security and compliance features, organizations can establish a solid baseline for NCA ECC compliance. The NCA stresses the importance of continuous compliance and monitoring, as cybersecurity is not a one-time exercise but an ongoing process. ZainTECH's Managed M365 Service directly addresses this need by providing continuous security assessments, automated threat detection, and compliance tracking. This ensures organizations can not only achieve compliance with ECC today but also sustain and improve their compliance posture over time, adapting to regulatory updates, security best practices, and new M365 capabilities.

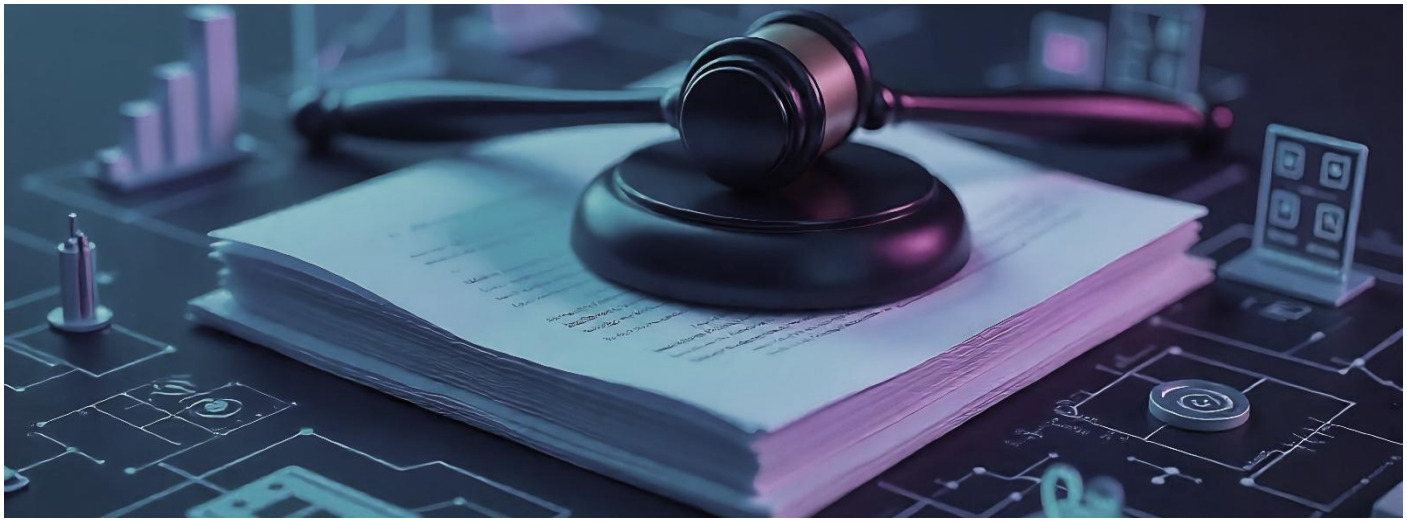
ECC	ZAINTECH MANAGED M365
Compliance with Cybersecurity Standards (1-7)	Provides regulatory compliance tracking via Microsoft Compliance Manager, ensuring continuous alignment with Saudi cybersecurity regulations.
Cybersecurity Awareness & Training (1-10)	Delivers end-user security awareness training through Microsoft Defender Security Awareness and phishing simulation campaigns to enhance cybersecurity culture.
Identity & Access Management (2-2)	Implements Microsoft Entra ID (formerly Azure AD) with role-based access controls, Multi-Factor Authentication (MFA), and privileged identity management.
Email Protection (2-4)	Uses Microsoft Defender for Office 365 to detect and filter phishing, spam, and malware threats in email communications.
Network Security Management (2-5)	Provides Zero Trust-based network segmentation, Microsoft Defender for Endpoint protection, and cloud-native firewall security integrations.
Mobile Device Security (2-6)	Enforces Microsoft Intune policies for Mobile Device Management (MDM) and encryption, ensuring compliance with ECC mobile security standards.
Data & Information Protection (2-7)	Uses Microsoft Purview to classify, encrypt, and monitor sensitive information, enforcing Data Loss Prevention (DLP) policies.
Cryptography (2-8)	Leverages M365 encryption mechanisms such as BitLocker and Transport Layer Security (TLS) to protect data in transit and at rest.
Backup & Recovery Management (2-9)	Implements automated cloud-based backup and disaster recovery solutions with Azure Backup and Microsoft OneDrive versioning.
Vulnerability Management (2-10)	Conducts continuous vulnerability assessments with Microsoft Defender Vulnerability Management and automated patch management through Microsoft Intune.
Penetration Testing (2-11)	Supports penetration testing by offering security analytics, automated risk assessments, and compliance readiness reports.
Cybersecurity Event Logs & Monitoring (2-12)	Provides centralized log management with Microsoft Sentinel (SIEM) and real-time security monitoring to detect threats and anomalies.
Cybersecurity Incident & Threat Management (2-13)	Automates threat detection, incident response, and remediation with Microsoft Defender XDR and 24/7 security operations support.
Web Application Security (2-15)	Uses Azure Web Application Firewall (WAF) to protect web applications against threats like SQL injection and Cross-Site Scripting (XSS).

24/7 CONTINUOUS MONITORING, DETECTION, AND RESPONSE

ZainTECH provides a proven security framework backed by our Cyber Resilience Centers (CRCs) in UAE, KSA, and Egypt, as well as The Bunker in Jordan. With over 10,000 servers managed across our datacenters and public cloud environments, our team ensures that security events are detected, analysed, and responded to in real time. Our 24/7 monitoring, detection and response capabilities give organizations the confidence that their M365 environments are monitored by seasoned cybersecurity professionals who proactively address vulnerabilities, conduct investigations, and prevent security breaches before they escalate. We combine automation, AI-driven threat detection, and expert analysis to deliver a resilient security posture that meets the stringent requirements of the NCA ECC framework.

Transformed from an army command control center, The Bunker is our 4,300sqm, state-of-the-art, fully redundant NOC and SOC situated at the King Hussein Business Park in Amman, Jordan. This military-grade facility is located 12 meters underground, safeguarded by 2-meter thick concrete walls and reinforced with 2-ton blast doors at both entrances. Designed to withstand fires, earthquakes, and missile attacks, The Bunker's disaster recovery center features automated blast walls that act as the sole source of fresh air intake and shut down in the event of an explosion, allowing operations to continue uninterrupted underground. As one of the most secure data centers in the region, The Bunker plays a crucial role in ZainTECH's cybersecurity ecosystem, ensuring that organizations benefit from an unparalleled level of protection and resilience.

REGULATORY REPORTING AND AUDIT READINESS



Ensuring regulatory compliance requires proper data governance, structured audit processes, and clear visibility into security controls. With ZainTECH's Managed M365 service, organizations can leverage built-in M365 capabilities such as eDiscovery, Audit Holds, and Data Classification to simplify regulatory reporting and demonstrate adherence to compliance frameworks like the NCA ECC.

Our team ensures that these features are properly configured out of the box, enabling organizations to track security events, monitor privileged access, and enforce compliance policies with minimal customization. Additionally, we continuously monitor and maintain a high Microsoft Secure Score, ensuring that security best practices remain in place. By reducing security drift and proactively managing compliance settings, ZainTECH helps organizations stay audit-ready at all times, minimizing the risks of compliance failures and regulatory penalties.

CONCLUSION AND NEXT STEPS

Achieving and maintaining compliance with the NCA ECC framework requires more than just deploying security tools – it demands continuous assessment, proactive threat management, and strategic planning. ZainTECH's Managed M365 service ensures that organizations are not only compliant today but remain secure and compliant as threats evolve and regulations change.

To help organizations better understand their security posture and compliance gaps, we invite you to participate in a Data Security or Threat Protection workshop. Our Microsoft security architects will work with you to assess your current security and compliance requirements and provide a clear roadmap to leveraging the full capabilities of your M365 licenses. This hands-on engagement will help you identify risks, optimize your security settings, and build a comprehensive action plan to address any gaps.

Get in touch with your ZainTECH account manager today to learn more about ZainTECH's Managed M365 services or schedule your Data Security or Threat Protection workshop and take the next step toward a more secure and compliant M365 environment.

ABOUT ZAINTECH

ZainTECH is a regional integrated digital solutions provider, unifying Zain Group's ICT assets to offer a unique value proposition of comprehensive digital solutions and services under one roof. The company drives the digital transformation of customers in the MENA region by providing a center of excellence and managed solutions across cloud, cybersecurity, big data, drones and robotics, digital solutions, and modern infrastructure.

ZainTECH operates in Kuwait, Saudi Arabia, Bahrain, Jordan, Iraq, Sudan, South Sudan, and the United Arab Emirates, as well as in other key markets in the Middle East.

Discover how ZainTECH Software Licensing Services can **help your organization achieve greater operational resilience and improved business outcomes.**

info@zaintech.com

+(971) 4 360 1622