CYBERSECURITY

Bank-Grade Infrastructure

Terminology

The following is a list of terminology that you **must be– aware of** when you're dealing with real estate acquisition process:

- **NIST Risk Management Framework (RMF):** It's a structured process that helps organizations manage cybersecurity risks. It guides them through steps such as identifying risks, choosing security controls, and implementing them, and continuously monitoring to stay protected. It's widely used in high-security environments to keep systems safe and compliant

- **SAMA Cybersecurity Framework:** This is a mandatory set of guidelines from the Saudi Arabian Monetary Authority that requires banks to protect high-risk assets, secure privileged access, and manager cyber risks through strong governance and controls. **Though it's designed for financial institutions, family offices can adopt it as a gold standard model to protect data, assets, and systems from advanced threats like wire fraud, deepfakes, and insider misuse.**

- **ISO/IEC 27005:** This is an international standard that provides detailed guidelines for managing information security risks. It supports ISO/IEC 27001 by helping organizations identify, assess, treat, and monitor cybersecurity threats to protect sensitive data. This focus is on making informed, risk-based decisions to strengthen overall security

- **Controller:** It's a person or organization that decides why and how personal data is collected and used. Under Saudi Law (PDPL), the controller is responsible for protecting that data, including making sure it's encrypted when stored or sent. In a family office, this would usually be the person managing client information and systems.

- **Zero Trust Network Access (ZTNA):** is a security approach that ensures no user or device is trusted by default, even inside the network. It requires continuous verification of identity and device health before granting access to specific applications. Users only get access to what they need — nothing more. This minimizes the risk of breaches and lateral movement within the network.

- **Security Information and Event Management (SIEM):** It's a system that collects and analyzes security data from across an organization. It monitors events, detects threats, and provides alerts in real time. SIEM helps identify suspicious activity by spotting patterns and anomalies. This enables faster response to potential cyberattacks.

- **Data Controller**: It's a person or organization that decides *why* and *how* personal data is used. They are responsible for making sure the data is handled properly and in line with privacy laws. The controller chooses what data to collect, what it's used for, and who it's shared with. They also ensure people's data rights are respected.

- **CITC/CST: CITC** (Communications and Information Technology Commission), now called **CST** (Communications, Space & Technology Commission), is Saudi Arabia's government authority that regulates telecom, IT, emerging technologies, and digital services. It sets rules and ensures fair competition, protects users, and promotes innovation. CST also oversees areas like cloud services, IoT, space technologies, and cybersecurity compliance.

- **Digital Rights Management (DRM):** It's a technology used to control how digital content (like music, movies, books, or software) is used and shared. It prevents unauthorized copying, editing, or distribution of protected content. DRM ensures that only people with proper permission can access the content. This helps protect copyrights and digital assets.

- **Unified Threat Management (UTM):** It's a security solution that combines multiple protection tools into one system. It typically includes **firewall, antivirus, intrusion detection, and content filtering**. UTM makes it easier to manage security by providing a single point of control. This helps organizations protect their networks from a wide range of threats.

- **Pretty Good Privacy (PGP):** It's a tool used to protect emails and files through encryption. It scrambles the content so only the intended recipient can read it. PGP also verifies the sender's identity and ensures the message hasn't been tampered with. This helps keep sensitive communications private and secure.

- **User and Entity Behavior Analytics (UEBA):** it's a security tool that monitors how users and devices behave. It uses machine learning to spot unusual actions that might signal a cyberattack. For example, if an employee suddenly downloads large amounts of data, UEBA would flag it. This helps detect insider threats and advanced attacks that bypass traditional defenses.

- **IT Networks (Information Technology Networks):** On high-value assets like yachts or private jets handle digital systems that process and transmit data. These typically include guest and crew Wi-Fi, satellite internet connections, smart TVs, entertainment systems, VoIP phones, onboard computers, and management software. The main purpose of the IT network is to support communications, media, internet access, and business functions onboard. Since these systems often connect to external networks (like the internet), they are common entry points for cyber threats and must be carefully secured.

- **OT Networks (Operational Technology Networks):** Control the asset's physical systems and operations. On a yacht or jet, this includes navigation systems (GPS, radar), engine and propulsion controls, power management (generators, batteries), HVAC (climate control), lighting systems, CCTV security, alarm systems, and any automation or IoT devices that directly affect how the vessel or aircraft operates. These networks are critical to the safe operation of the asset and must remain highly reliable and secure. OT networks are ideally isolated from IT networks to prevent cyberattacks from spreading to vital control systems.

- **Domain-based Message Authentication, Reporting & Conformance (DMARC):** It's a system that helps an entity protect its domain from being used in phishing or spoofed emails. It allows the entity to specify how email servers should handle messages that fail authentication checks. DMARC ensures only authorized senders can use the domain for email. It also provides reports so the entity can monitor and improve its email security.

- **Capability Maturity Model Integration (CMMI):** It's a system that helps an entity protect its domain from being used in phishing or spoofed emails. It allows the entity to specify how email servers should handle messages that fail authentication checks. DMARC ensures only authorized senders can use the domain for email. It also provides reports so the entity can monitor and improve its email security.

- **DomainKeys Identified Mail (DKIM):** It's an email security feature that helps verify that a message was really sent by the domain it claims to be from. It works by adding a digital signature to each email, which receiving mail servers can check. If the signature is valid, it proves the email wasn't altered in transit. This helps protect against email spoofing and tampering.

- **MSC.428(98):** It's an IMO resolution that requires shipping companies to manage cyber risks as part of their Safety Management System (SMS). It ensures that cyber threats to critical ship systems (like navigation and engine controls) are identified and addressed. The goal is to enhance the safety and resilience of ships against cyberattacks. Compliance became mandatory from January 1, 2021.

- **NIST Cybersecurity Framework (NIST CSF):** It's a set of guidelines developed to help organizations manage and reduce cybersecurity risks. It provides a structured approach to identifying, protecting, detecting, responding to, and recovering from cyber threats. The framework is flexible and can be used by organizations of all sizes and industries. It helps improve overall cyber resilience and risk management.

- **MDR Services:** These are services which are outsourced cybersecurity services that help organizations detect and respond to threats. An MDR provider uses advanced tools and expert teams to monitor networks, analyze suspicious activity, and quickly respond to attacks. This gives organizations 24/7 protection without needing to build their own full-time security team. MDR helps improve threat detection and incident response capabilities.

- **Treasury Management System (TMS):** It's software that helps organizations manage their financial operations. It handles tasks like cash management, payments, bank accounts, investments, debt, and financial risk. A TMS provides real-time visibility into cash flow and automates many treasury tasks. This helps organizations improve financial control, efficiency, and decision-making.

- **TEMPEST measures:** These are security controls used to prevent sensitive electronic equipment from leaking information through unintended signals (like electromagnetic emissions). These emissions could potentially be intercepted and used to spy on data. TEMPEST protections include shielding, filtering, and secure equipment placement. They are often used in government, military, and high-security environments to protect classified information.

- **Role-Based Access Control (RBAC):** It's a security method that grants system access based on a user's role within an organization. Each role has specific permissions, and users only get access to the data and functions needed for their job. This helps enforce the principle of least privilege and reduces the risk of unauthorized access. It also simplifies managing user permissions as roles can be centrally controlled.

- **SOC 2 Type II reports:** It's an independent audit report that evaluate how well an organization's security controls operate over time (usually 6–12 months). It focuses on areas like data security, availability, processing integrity, confidentiality, and privacy. A Type II report shows not just that controls are designed properly, but that they actually work in practice. It helps build trust with clients by proving strong data protection.

- **Just-In-Time (JIT) Access:** It's a security approach where users are granted access to systems or data only when they need it, and only for a limited time. This reduces the risk of misuse or attacks by not keeping permanent access open. Once the task is complete, the access automatically expires. JIT helps enforce the principle of least privilege and strengthens overall security.

- **Bring Your Own Device (BYOD):** It's a policy where employees are allowed to use their personal devices (like smartphones, laptops, or tablets) for work purposes. It offers flexibility and convenience but also introduces security challenges. Organizations must manage risks like data leakage and unauthorized access. BYOD policies typically include security requirements and controls to protect company data.

- **Data Loss Prevention (DLP):** It's a security strategy and set of tools designed to prevent sensitive data from being lost, leaked, or accessed by unauthorized users. It monitors and controls the movement of data across networks, devices, and storage. DLP helps ensure that confidential information (like personal data, financial records, or trade secrets) stays protected. This reduces the risk of accidental or malicious data breaches.

- **Device Attestation:** It's a security process that verifies whether a device is trusted and secure before allowing it to access a network or system. It checks factors like the device's identity, software version, configuration, and security posture. If the device passes the checks, it is granted access; if not, it may be blocked or restricted. This helps prevent compromised or unauthorized devices from connecting to sensitive environments.

- **Hardened Devices:** These are computers or electronic systems that have been specially configured to reduce security risks. This involves removing unnecessary software, disabling unused services, applying strict security settings, and keeping the system updated. The goal is to make the device more resistant to attacks and unauthorized access. Hardened devices are often used in high-security environments or critical systems.

- **Cloud Access Security Broker (CASB):** It's a security tool that sits between users and cloud services to monitor and control cloud activity. It helps enforce security policies, protect sensitive data, and detect risky behavior in cloud apps (like Microsoft 365, Google Workspace, or Salesforce). CASB provides visibility into cloud usage and ensures compliance with company and regulatory requirements. This helps organizations securely adopt cloud services.

- **Network Access Control (NAC) Appliances:** These are security devices that manage and control which devices can connect to an organization's network. They check the identity, security posture, and compliance of devices before granting access. If a device doesn't meet security requirements (like missing patches or outdated antivirus), the NAC can block or limit its access. This helps prevent unauthorized or risky devices from compromising the network.

- **Software-Defined Perimeter (SDP) tools:** These are security solutions that create secure, invisible connections between users and specific applications — not the entire network. They verify the user's identity and device before allowing access and hide resources from unauthorized users. Unlike traditional VPNs, SDP tools grant access only to what the user needs, reducing attack surfaces. This helps protect against modern threats like lateral movement and credential-based attacks.

- **Voice over Internet Protocol (VoIP):** It's technology that lets people make phone calls using the internet instead of traditional phone lines. It converts voice into digital signals and transmits them over a network. VoIP is often cheaper and more flexible than regular telephony. It's commonly used in businesses for internet-based phone systems and video conferencing.

- **Public Switched Telephone Network (PSTN):** It's the traditional, global system of wired telephone lines used for voice communication. It connects calls through a network of switches, cables, and telephone exchanges. PSTN is what powers landline phones and enables people to make reliable voice calls worldwide. Unlike VoIP, PSTN does not rely on the internet for call transmission.

- **Data Processor:** A Data Processor is an external entity (such as a vendor or service provider) that processes personal data on behalf of the organization (the Data Controller). The processor does not determine the purpose or means of processing — it simply follows the controller's instructions. The controller remains responsible for ensuring the processor handles data securely and in compliance with data protection laws.

Technology Stack

Zero Trust & Identity Management

Microsoft Entra / Azure AD

A cloud-based identity and access management (IAM) service that helps organizations manage user identities and control access to apps and resources. It supports single sign-on (SSO), multi-factor authentication (MFA), and conditional access policies. Part of the Microsoft Entra product family. It helps secure hybrid and cloud environments.

Okta Identity Cloud

A leading independent identity platform for managing and securing user access across cloud and on-premises apps. Provides SSO, MFA, lifecycle management, and identity governance. Designed to integrate with a wide range of services. Supports Zero Trust strategies by verifying users and devices.

Microsoft Zero Trust Suite (Defender + Azure AD Conditional Access + Endpoint Manager)

An integrated Microsoft security approach combining threat protection (Defender), adaptive access controls (Conditional Access), and device management (Endpoint Manager). It enforces Zero Trust principles by continuously verifying users, devices, and sessions. Helps secure identities, endpoints, and data. Designed for Microsoft cloud and hybrid environments.

Google BeyondCorp Enterprise

Google’s commercial Zero Trust framework that enables secure access to apps and data without relying on a traditional VPN. It verifies users and devices before granting access, with continuous checks during sessions. Designed to protect users working from anywhere. Helps prevent lateral movement and reduce attack surfaces.

Microsoft Endpoint Manager

A unified endpoint management (UEM) platform that combines Microsoft Intune and Configuration Manager. It manages and secures devices (Windows, macOS, iOS, Android) across an organization. Supports enforcing security policies and compliance for Zero Trust. Helps ensure only healthy, trusted devices can access corporate resources.

Cisco ISE (Identity Services Engine) - NAC

A powerful Network Access Control (NAC) solution that enforces security policies for users and devices connecting to the network. It identifies, profiles, and authorizes devices before granting access. Supports dynamic network segmentation. Key tool for Zero Trust network strategies.

Fortinet NAC

A Network Access Control solution that identifies and controls all devices on the network. Enforces policies to manage user and device access. Integrates with Fortinet Security Fabric for unified security. Helps support Zero Trust by ensuring only trusted devices can connect.

Zscaler Private Access (SDP / ZTNA)

A cloud-delivered Zero Trust Network Access (ZTNA) solution that enables secure, identity-based access to private apps. It eliminates the need for traditional VPNs. Applications are never exposed to the internet, reducing attack surfaces. Access is granted based on user identity and device posture.

Palo Alto Prisma Access (SDP / ZTNA)

A cloud-delivered platform that provides secure access to apps and data from anywhere. Combines ZTNA, cloud firewall, threat prevention, and more. Enforces Zero Trust by continuously validating user identity and device posture. Designed for protecting distributed workforces.

CyberArk (Privileged Access Management - PAM)

A leading solution for managing and securing privileged accounts, credentials, and secrets. It helps prevent misuse of high-level access that could compromise systems. Enforces least privilege and strong auditing. Critical for Zero Trust architectures where privileged access is tightly controlled.

BeyondTrust PAM

A privileged access management solution that secures and manages privileged accounts and sessions. It controls, monitors, and audits privileged activities. Supports granular, just-in-time access to sensitive systems. Aligns with Zero Trust by minimizing privileged attack surfaces.

Thycotic (now Delinea) PAM

A user-friendly privileged access management solution for securing privileged credentials and controlling privileged sessions. Supports vaulting, session monitoring, and least-privilege enforcement. Designed for scalability across hybrid environments. Helps enforce Zero Trust by controlling high-risk access.

1Password Teams (password manager fallback)

A secure password management solution that helps teams store, manage, and share passwords and sensitive information. Provides encrypted vaults, SSO integration, and MFA support. Useful as a fallback for managing credentials in a Zero Trust environment. Helps reduce password-related risks.

LastPass Enterprise (password manager fallback)

A cloud-based enterprise password manager that stores and manages passwords, secrets, and credentials. Offers SSO, MFA, and secure vaulting. Helps enforce strong password hygiene. Often used as a fallback to support Zero Trust identity management.

Data Encryption & Document Vaulting

AWS CloudHSM (Hardware Security Module)

A cloud-based hardware security module (HSM) service that allows organizations to generate, store, and manage cryptographic keys in FIPS 140-2 Level 3 validated HSMs. Keeps keys isolated from AWS infrastructure. Supports strong encryption, signing, and key management. Used for protecting sensitive data and meeting compliance.

Azure Key Vault with HSM

A cloud service that securely stores cryptographic keys, secrets, and certificates. When integrated with HSM-backed pools, keys are protected by FIPS 140-2 Level 3 hardware. Supports key lifecycle management and integration with Azure services. Helps safeguard sensitive data in cloud environments.

HashiCorp Vault (secrets management, dynamic encryption)

A tool for securely managing secrets, encryption keys, and access to sensitive data. Supports dynamic secrets, on-demand encryption, and fine-grained access control. Can run on-prem or in the cloud. Commonly used to secure infrastructure and application credentials.

NextCloud (on-premises E2EE file storage)

An open-source platform for on-premises file storage and collaboration with end-to-end encryption (E2EE). Organizations retain full control over data and infrastructure. Provides secure file sharing, syncing, and team collaboration. Suitable for privacy-sensitive environments.

OwnCloud Enterprise (on-premises E2EE file storage)

An enterprise-grade, on-premises file-sharing platform with E2EE capabilities. Enables secure file access, sharing, and collaboration while keeping data under organizational control. Offers advanced compliance and governance features. Common in regulated industries.

Tresorit (secure cloud storage with client-side encryption)

A cloud storage solution with strong client-side encryption — data is encrypted on the user's device before upload. Designed for secure file sharing and collaboration. Zero-knowledge architecture ensures even the service provider can't access the data. Suitable for sensitive business documents.

Box Shield (secure cloud storage with DRM)

An advanced security layer for Box cloud storage. Enables classification, access controls, malware detection, and document-level DRM. Helps prevent unauthorized sharing and downloading of sensitive files. Designed for compliance-driven industries.

Microsoft Purview Information Protection

A comprehensive data classification and protection solution. Helps organizations discover, label, and protect sensitive information across Microsoft 365 and beyond. Supports encryption, access control, and tracking. Integral to enterprise data governance and compliance.

VERA DRM

A digital rights management (DRM) platform that protects files with encryption and granular access controls. Files remain protected wherever they go (on devices, cloud, email). Policies can control viewing, editing, and sharing. Provides detailed auditing and tracking.

PGP (Pretty Good Privacy — email encryption)

A standard for encrypting and digitally signing emails and files. Uses public/private key cryptography to ensure that only intended recipients can read the message. Verifies sender identity and prevents tampering. Widely used for personal and business email security.

S/MIME (Secure/Multipurpose Internet Mail Extensions — email encryption)

An email encryption standard that uses digital certificates to encrypt messages and add digital signatures. Built into many enterprise email systems (Outlook, Apple Mail). Helps ensure confidentiality, authenticity, and integrity of emails. Common in corporate and government environments.

Citrix ShareFile (secure file sharing / virtual data room)

A secure file sharing and collaboration platform that includes virtual data room (VDR) features. Enables encrypted file storage, sharing, and document tracking. Supports granular permissions and auditing. Often used for sensitive deal rooms and legal/financial collaboration.

Intralinks (virtual data room — VDR)

A leading VDR platform used for secure document sharing in mergers, acquisitions, and high-value deals. Provides encryption, granular permissions, watermarking, and full audit trails. Supports collaboration across organizational boundaries. Trusted by banks, legal firms, and corporates.

Drooms (virtual data room — VDR)

A secure, European-based VDR solution for managing confidential documents during transactions. Offers encryption, access control, audit logging, and workflow tools. Frequently used in M&A, real estate, and legal transactions. Known for compliance with strict European privacy standards.

Data Encryption & Document Vaulting

Kybria (Treasury Management System — TMS)

A Treasury Management System that helps organizations manage cash, payments, liquidity, bank accounts, and financial risks. Provides real-time visibility and automation of treasury processes. Helps improve efficiency, control, and compliance in financial operations. Commonly used in corporate and institutional environments.

FIS (Treasury Management System — TMS)

A leading Treasury Management System from FIS Global. Supports cash and liquidity management, risk management, bank connectivity, payments, and financial reporting. Offers advanced automation and analytics. Widely used by large corporations and financial institutions to optimize treasury operations.

SWIFT Customer Security Program (CSP — compliance framework)

A cybersecurity framework developed by SWIFT to help organizations using SWIFT services improve their security posture. Requires compliance with mandatory controls for securing SWIFT-related infrastructure. Aims to reduce the risk of cyber fraud in global financial messaging. Annual self-attestation or audit is required.

Secure Email Gateway with DMARC (anti-spoofing & fraud protection)

An email security solution that filters inbound and outbound emails to block spam, malware, and phishing. Integrates with DMARC to enforce anti-spoofing policies and prevent domain abuse. Helps stop impersonation attacks and email fraud. A key control in enterprise email security.

Monitoring, Detection & Response

Splunk (SIEM)

A leading Security Information and Event Management (SIEM) platform that collects, correlates, and analyzes security data across the enterprise. Provides real-time threat detection, investigation, and compliance reporting. Supports customizable dashboards and advanced analytics. Widely used in large-scale security operations.

IBM QRadar (SIEM)

An enterprise SIEM solution that aggregates and analyzes security data to detect and respond to threats. Offers real-time correlation, behavioral analytics, and compliance monitoring. Provides centralized visibility across networks, endpoints, and cloud environments. Trusted by large organizations and critical infrastructure sectors.

Microsoft Sentinel (SIEM)

A cloud-native SIEM and SOAR solution built on Microsoft Azure. Collects and analyzes security data across the hybrid environment. Uses AI and automation to detect, investigate, and respond to threats. Scales easily and integrates with Microsoft and third-party services.

Elastic Security Stack (SIEM)

An open-source SIEM built on the Elastic Stack (Elasticsearch, Kibana, Beats, Logstash). Ingests and analyzes large volumes of security data. Provides threat detection, investigation, and visualization. Flexible and developer-friendly, often used in highly customized security environments.

Palo Alto Cortex XSOAR (SOAR)

A Security Orchestration, Automation, and Response (SOAR) platform that automates security workflows. Integrates with diverse security tools to streamline detection, investigation, and response. Provides playbooks, case management, and threat intelligence. Helps improve SOC efficiency and response speed.

Splunk SOAR (formerly Phantom) (SOAR)

A SOAR solution from Splunk that automates security operations through playbooks and integrations. Enables rapid, automated response to security incidents. Supports complex workflows and integrates with a wide range of tools. Reduces response times and manual effort in the SOC.

Microsoft Sentinel built-in automation (SOAR)

Built-in SOAR capabilities within Microsoft Sentinel. Enables automated investigation and response through playbooks based on Azure Logic Apps. Helps orchestrate actions across Microsoft and third-party services. Enhances SOC efficiency and supports Zero Trust security models.

CrowdStrike (EDR)

A leading Endpoint Detection and Response (EDR) solution delivered via the CrowdStrike Falcon platform. Provides real-time monitoring, threat detection, and response on endpoints. Uses cloud-native architecture and AI-driven analytics. Known for strong threat intelligence and rapid deployment.

Microsoft Defender for Endpoint (EDR)

An enterprise-grade EDR solution that protects endpoints from advanced threats. Provides real-time threat detection, investigation, and response. Integrates tightly with Microsoft 365 Defender and Sentinel. Supports Zero Trust and modern security architectures.

Carbon Black (EDR)

A VMware EDR platform that provides continuous endpoint monitoring and threat detection. Focuses on behavior-based detection and prevention. Enables deep visibility into endpoint activity. Often used in environments with strict compliance and security requirements.

Microsoft 365 Defender (XDR)

An Extended Detection and Response (XDR) solution that integrates protections across endpoints, email, identities, and cloud apps. Correlates signals to detect sophisticated attacks. Provides unified investigation and response. Part of Microsoft’s Zero Trust and integrated security platform.

Palo Alto Cortex XDR (XDR)

An XDR platform that unifies detection and response across endpoints, networks, cloud, and identity data. Uses AI-driven analytics to detect complex threats. Provides centralized investigation and automated response. Extends visibility and protection beyond traditional EDR.

Secure Communications

Signal (messaging & voice E2EE)

A free, open-source app offering end-to-end encrypted (E2EE) messaging, voice, and video calls. Designed to protect communications from interception. No metadata is stored on servers. Widely trusted by security-conscious users.

Wickr Enterprise (messaging & voice E2EE)

An enterprise-grade secure messaging platform offering E2EE messaging, voice, and video. Includes message expiration, secure file sharing, and full admin controls. Used by government and enterprise sectors. Supports strong compliance and audit needs.

Wire Secure Messenger (messaging & voice E2EE)

A secure collaboration platform with E2EE messaging, voice, video, and file sharing. Designed for business use with compliance and data residency options. Supports on-prem and private cloud deployment. Used by privacy-sensitive industries.

Threema Work (messaging & voice E2EE)

An enterprise version of Threema providing E2EE messaging, voice, and video. No phone number required for identity, minimizing data exposure. Offers on-prem hosting and strong privacy controls. Popular in Europe and regulated sectors.

BlackBerry SecuSUITE (hardened secure phone)

A secure communications suite providing E2EE voice, text, and data for smartphones. Often used on hardened devices. Certified for classified use by multiple governments. Protects against interception and eavesdropping.

KryptAll (hardened secure phone)

A commercial solution providing hardened secure phones with encrypted voice calling. Routes calls through secure, private networks. Designed for high-profile users requiring privacy. Calls are protected from surveillance and interception.

Glacier secure phones

Custom-built, hardened smartphones designed for secure communications. Typically offer strong encryption, secure OS builds, and limited attack surfaces. Used by executives, government, and defense clients. Focused on privacy and resilience.

Bittium secure phones

Specialized secure smartphones built for defense, government, and critical sectors. Offer hardened OS, strong E2EE, and advanced mobile security controls. Certified for classified use in several countries. Supports secure voice, messaging, and data.

ProtonMail (secure email)

A secure email service with end-to-end encryption and zero-access architecture. Messages are encrypted before they reach Proton's servers. Based in Switzerland with strong privacy laws. Popular among journalists and privacy advocates.

Tutanota (secure email)

An encrypted email service offering E2EE and zero-knowledge architecture. Supports encrypted contacts and calendars as well. Open source and based in Germany. Strong focus on privacy and minimal data collection.

Zoom with E2EE (secure video conferencing)

Zoom's E2EE mode encrypts video, audio, and chat so only meeting participants can decrypt content. Designed to prevent even Zoom from accessing data. E2EE must be enabled by the host. Used for sensitive or private meetings.

Cisco Webex with E2EE (secure video conferencing)

Webex offers E2EE for meetings, securing video, audio, chat, and content. Ensures data is encrypted end-to-end, with keys controlled by participants. Suitable for regulated industries. Supports compliance and privacy needs.

Jitsi (self-hosted secure video conferencing)

An open-source video conferencing platform that can be self-hosted for full control. Supports E2EE and encrypted communications. No licensing costs. Popular in privacy-conscious organizations.

Cisco Meeting Server (self-hosted video conferencing)

An enterprise-grade, self-hosted video conferencing solution. Supports E2EE, federation, and integration with enterprise tools. Gives organizations full control over security and data. Used in sensitive and regulated sectors.

Apple FaceTime (secure video calls, Apple devices only)

Apple’s built-in video and voice calling app with end-to-end encryption. Only available on Apple devices (iPhone, iPad, Mac). Encryption keys are device-controlled. Simple, secure option for Apple ecosystem users.

Enterprise MDM (Mobile Device Management)

A system for managing, securing, and monitoring mobile devices across an organization. Enforces security policies, controls app usage, and enables remote wipe. Helps protect corporate data on mobile endpoints. Essential for Zero Trust mobility.

Vendor & Third-Party Access

Azure AD B2B (guest access control)

A feature of Azure Active Directory that enables secure collaboration with external users (partners, vendors). Provides controlled guest access to enterprise apps and resources. Enforces identity verification, MFA, and conditional access. Helps maintain Zero Trust for third-party users.

TeamViewer (remote support)

A remote access and support platform allowing technicians to control and troubleshoot user devices over the internet. Provides secure, encrypted connections. Often used for vendor or IT support access. Requires careful governance in sensitive environments.

LogMeIn Rescue (remote support)

An enterprise-grade remote support solution for IT teams and service providers. Enables secure, on-demand remote control of user devices. Supports audit logging, permissions, and compliance controls. Used for managing third-party and vendor support access.

BeyondTrust Remote Support (remote support)

A secure, enterprise-focused remote support platform. Enables privileged remote access with strong auditing, session recording, and granular controls. Designed for regulated and sensitive environments. Supports vendor access within Zero Trust frameworks.

BitSight (vendor cyber rating)

A cyber risk rating platform that provides external security assessments of third-party vendors. Uses external data to score a vendor’s cybersecurity posture. Helps organizations evaluate and monitor supply chain risks. Often used in vendor risk management programs.

SecurityScorecard (vendor cyber rating)

A cybersecurity ratings platform that continuously monitors the external security posture of vendors and partners. Generates risk scores based on observed vulnerabilities and exposures. Supports third-party risk management and due diligence. Widely used in supply chain security programs.

Intralinks (VDR for external parties)

A virtual data room (VDR) platform used to securely share sensitive documents with external parties (vendors, partners, deal teams). Provides encryption, access control, and full audit trails. Common in M&A, legal, and compliance-driven collaborations. Supports secure vendor document exchange.

Drooms (VDR for external parties)

A secure VDR platform designed for managing confidential document exchanges with external parties. Offers advanced access controls, encryption, and auditing. Used in regulated transactions (real estate, M&A, legal). Helps manage secure third-party document collaboration.

Physical Security

HID Card Readers (physical access control)

Electronic readers used to control physical access to buildings or secure areas. Authenticate users via contactless HID cards or badges. Integrated with access control systems and door locks. Common in corporate, industrial, and high-security environments.

Biometric Pads (physical access control)

Access control devices that verify users based on biometric data (fingerprint, facial recognition, iris scan). Eliminate reliance on cards or PINs. Provide stronger identity assurance. Used for high-security zones or sensitive facilities.

IP Cameras with NVRs (surveillance)

Digital video surveillance systems with IP-based cameras connected to Network Video Recorders (NVRs). Capture, store, and manage video footage. Support remote viewing, analytics, and alerts. Key component of modern physical security and monitoring.

PSIM Systems (Physical Security Information Management)

Software platforms that integrate multiple physical security systems (access control, video, alarms, sensors). Provide centralized monitoring, situational awareness, and coordinated response. Enable unified management of complex security environments. Often used in critical infrastructure and large enterprises.

IoT-enabled Safe Cabinets (for document protection)

Secure storage cabinets equipped with IoT sensors and connected controls. Monitor cabinet status, control access remotely, and generate audit logs. Protect sensitive documents, media, or equipment. Used in government, legal, and regulated industries.

Endpoint Management Software for USB Port / Screen Lock

Software that enforces security controls on computer endpoints. Manages USB port usage (block or restrict devices) and enforces screen lock policies. Helps prevent data leakage and unauthorized device use. A key part of endpoint physical and data security.

Saudi Arabian Regulations & Frameworks

PDPL — Personal Data Protection Law of Saudi Arabia

Saudi Arabia's national data protection law governing how personal data is collected, used, and shared. Establishes data subject rights, consent requirements, and processing rules. Applies to both public and private sectors. Enforced by the Saudi Data and Artificial Intelligence Authority (SDAIA).

SAMA Cybersecurity Framework

A mandatory cybersecurity framework issued by the Saudi Central Bank (SAMA) for banks, insurance companies, and financial institutions. Defines governance, risk management, technical controls, and monitoring requirements. Aims to protect the financial sector from cyber threats. Requires regular compliance assessments.

CITC / CST Regulations

Regulatory frameworks and guidelines issued by Saudi Arabia's Communications, Space & Technology Commission (formerly CITC). Cover cybersecurity, cloud computing, IoT, and telecom sectors. Define security, privacy, and operational standards for service providers. Help ensure safe and trusted digital services.

NCA Essential Cybersecurity Controls (ECC-2:2024)

A comprehensive set of baseline cybersecurity controls issued by Saudi Arabia's National Cybersecurity Authority (NCA). Covers governance, asset management, access control, monitoring, and incident response. Mandatory for government entities and critical infrastructure. ECC-2:2024 is the latest version.

ZATCA — Zakat, Tax and Customs Authority e-invoicing rules

Saudi Arabia's e-invoicing regulations (FATOORAH) require electronic invoicing with strict data integrity, tamper-evidence, and security measures. Enforced by ZATCA. Aimed at preventing fraud and enhancing VAT compliance. Mandates technical and process controls on e-invoice systems.

ECC-2:2024

Refers specifically to the **2024 edition** of the NCA Essential Cybersecurity Controls (ECC-2). The latest version updates and strengthens cybersecurity requirements. Focuses on practical, risk-based controls. Forms the core cybersecurity compliance baseline in Saudi Arabia.

Basic Law of Governance — guarantees privacy of communication in KSA

Saudi Arabia’s Basic Law of Governance (Royal Decree No. A/90) guarantees the privacy of communications under Article 40. Protects the confidentiality of postal, telegraphic, telephonic, and other means of communication. Establishes constitutional privacy principles. Supports legal foundations for data and communication privacy.

International Standards & Frameworks

NIST RMF — National Institute of Standards and Technology Risk Management Framework

A structured framework for managing cybersecurity risk in information systems. Guides organizations through system categorization, control selection, implementation, assessment, and continuous monitoring. Widely used in U.S. government and critical industries. Helps integrate risk management into the system lifecycle.

NIST SP 800-207 — NIST Zero Trust Architecture guidance

Official NIST guidance on designing and implementing Zero Trust Architectures (ZTA). Defines core principles, components, and deployment models for Zero Trust. Emphasizes continuous verification of identity, device, and context. Serves as a global reference for modern cybersecurity architectures.

NIST 800-53 / NIST Cybersecurity Framework (CSF)

Widely adopted cybersecurity control catalogs and frameworks developed by NIST. NIST 800-53 defines detailed security and privacy controls. The NIST Cybersecurity Framework (CSF) provides a high-level framework for identifying, protecting, detecting, responding to, and recovering from cyber threats. Used across industries globally.

ISO/IEC 27005 — Risk management standard supporting ISO 27001

An international standard providing guidance on information security risk management. Supports ISO/IEC 27001 by helping organizations identify, assess, and treat risks. Promotes systematic risk-based thinking. Essential for building and maintaining an effective ISMS (Information Security Management System).

ISO/IEC 27001 — International information security management standard

The globally recognized standard for establishing, implementing, maintaining, and continuously improving an Information Security Management System (ISMS). Defines a risk-based approach to securing information assets. Provides a framework for governance, controls, and continual improvement. Used by organizations of all sizes worldwide.

GDPR — General Data Protection Regulation (EU)

The European Union’s comprehensive data protection law governing how personal data is collected, processed, and stored. Grants data subjects strong privacy rights and imposes strict obligations on organizations. Requires transparency, accountability, and security of personal data. Has global impact beyond the EU.

Other Global / Sectoral References

ENISA Best Practices

Cybersecurity guidelines and recommendations from the European Union Agency for Cybersecurity (ENISA). Provide best practices for SIEM, SOAR, threat detection, and incident response. Support alignment with EU regulations and industry standards. Frequently used as a reference for building resilient cybersecurity programs.

CISA Best Practices

Cybersecurity best practices published by the U.S. Cybersecurity and Infrastructure Security Agency (CISA). Cover topics such as SIEM, SOAR, threat monitoring, and critical infrastructure protection. Designed to help organizations strengthen cyber defenses. Widely referenced in both public and private sectors.

Baker McKenzie Handbook on KSA

A legal reference guide published by Baker McKenzie, covering regulatory and legal frameworks in Saudi Arabia. Offers best practices on physical security, data privacy, and compliance obligations. Cited to support legal due diligence in KSA operations. Useful for aligning with local governance requirements.

Bank-Grade Cybersecurity Infrastructure

The following is a comprehensive guide for a **hardened cybersecurity infrastructure** for a single-UHNWI family office based in **Saudi Arabia.** This guide addresses threats from the following types of actors:

- **State-Sponsored Actors**
- **Organized Cybercrime**
- **Insider Risks**
- **Deepfake Impersonation**

Mapping each element to Saudi Regulations (**PDPL, SAMA, CITC/CST, ZATCA**) and international standards (i.e. **GDPR, FATCA, NIST**). The focus in this guide is on executive-level outcomes and decision points, ensuring that the principal has clarity on **what measures to adopt and why,** without delving into **low-level technical configurations**. Each section includes **recommended tools (hardware / software)** and policies that meet or exceed private banking and sovereign wealth fund security standards.

CYBERSECURITY

Risk Assessment Models

Cybersecurity Risk Model for UHNWIs

Unique Threat Profile

UHNWIs and their family offices are **alluring targets** with substantial financial assets and sensitive information. They face a range of threats from **financially motivated cybercriminals to state-sponsored espionage.** Unlike large corporates, family offices often lack comparative security maturity and may underestimate risks. Therefore, this demands a tailored risk model.

Risk Assessment & Modeling

At the executive level, mandate a **formal risk management process** as the foundation of security decisions. Meaning you should conduct a thorough risk assessment to identify critical assets within the organization, this would include:

- **Banking Systems**
- **Legal Documents**
- **Personal Data**

For instance, evaluate the risks of:

Phishing-induced wire fraud

Deepfake voice scams

Ransomware

Insider misuse,

etc.,

In the context of the family office's operations. Use established frameworks such as NIST's Risk Management Framework or ISO27005, but customize it to UHNWI concerns.

Regular risk reviews are all essential, as the threat landscape evolves with new AI-driven attacks and geopolitical events. An executive risk dashboard can help prioritize investment

Executive Decision Points

Insist on **periodic risk briefings** where security staff or consultants present worst-case scenarios and mitigation status. Decide on **risk appetite** (i.e. zero tolerance for any unauthorized data access, strict thresholds for transaction fraud risk). Given UHNWIs often value privacy and convenience, leadership must consciously balance convenience with security, **avoiding the pitfall of prioritizing comfort until it's too late due to fraud or a cyber-attack which would make them re-evaluate everything.**

Therefore, it's wise to **budget for expert advisory,** engage with a cybersecurity firm experienced with family offices to perform an **initial risk baseline assessment and threat modeling exercise.** This external perspective can highlight overlooked threats and benchmark against best practices.

Regulatory Mapping

Saudi's **PDPL** mandates protecting personal data from loss, leakage, misuse or unauthorized access. Essentially requiring a risk-based approach to safeguard privacy. The Saudi Central Bank's **SAMA Cybersecurity Framework** explicitly calls for a **Risk Management Process and strict controls for high-risk assets and privileged access.**

Aligning with these, the family office should document a formal risk management policy (approved by top management as PDPL demands for accountability) and perform **Data Protection Impact Assessments (DPIAs)** for high-risk activities.

Internationally, consider **GDPR** if any EU personal data is handled, GDPR similarly requires risk assessments and appropriate security measures.

In summary, a **solid risk model** not only guides security investments but also demonstrates compliance with legal requirements to protect sensitive data.

CYBERSECURITY

Zero Trust Network Architecture

Zero Trust Network Architecture

How It Works

Adopt a **Zero Trust Architecture (ZTA)** across all networks and systems. Zero Trust means **nothing and no one is implicitly trusted,** even if already inside the network, essentially every access it continually verified. This modern approach is **critical** given the family office's distributed assets (global travel, cloud services, and personal devices) and high stakes.

*Traditional security is **insufficient**, as we assume attackers can infiltrate, so we design as if the network is already compromised and focus on protecting resources at the granular level.*

Key Zero Trust Measures

Identity-Centric Access

Strongly authenticate and authorize every user and device for each session. Implement **Multi-Factor Authentication (MFA)** universally, preferably phishing-resistant methods such as hardware security keys or biometrics for all staff and even the principal.

Integrate an **Identity and Access Management** platform (i.e. Azure AD or Okta) with conditional access policies to verify device health and user context on each login attempt.

Every access request should be **verified against dynamic policies** before being granted.

Micro-Segmentation

Divide the IT environment into isolated segments so that even if one device is breached, an attacker cannot freely move laterally. For instance segregate the:

- Banking / Payment systems
- Personal Document Vault
- Guest Wi-Fi
- IoT devices (Smart home or yacht systems)

Each would be in their own network segment or VLAN with tightly controlled communication between them. Use next-generation firewalls or software-defined networking policies such as **Policy Enforcement Points** to broker all access between segments. Solutions such as **Illumio or CISCO** Secure Workload can dynamically enforce such **micro-segmentation** at the workload level.

Continuous Monitoring and Analytics

Deploy tools that continuously monitor three key things in real-time for every login or access attempt:

Identity — *Who is trying to log in (user identity).*

Device — *What device they are using (laptop, phone, tablet).*

Context — *The circumstances of the access attempt (location, time, IP address, type of network, type of resource being accessed).*

A **Zero Trust Policy Engine** (usually part of a larger **Zero Trust Platform**) uses this real-time data along with several key inputs to decide whether to allow or block the request:

Threat Intelligence — Feeds about known attacks, malicious IPs, malware campaigns, or suspicious domains.

User Behavior Analytics — Analysis of what is normal for each user (typical login times, devices, geolocations) and detection of abnormal behavior.

Device Posture — The current security state of the device, such as:
- *Is antivirus up to date and running?*
- *Is the device jailbroken or rooted?*
- *Are operating system patches applied?*
- *Is disk encryption enabled?*

Using all these inputs, the **Zero Trust Policy Engine** makes an automated, dynamic decision to:

Allow access (everything is safe)

Challenge the user (require extra verification, like MFA)

Block access (if the risk is too high)

This process can be further enhanced by integrating a **Security Information and Event Management (SIEM) system**:

*A **SIEM** collects security logs and alerts from across the entire environment (firewalls, endpoints, servers, cloud services) and can feed threat alerts and risk signals into the Zero Trust Policy Engine to improve its decisions.*

Alternatively (or in addition), you can use a **dedicated Zero Trust Network Access (ZTNA) service**:

ZTNA dynamically adapts access based on risk level — for example, it might grant limited access to sensitive apps if the device is not fully healthy, or completely block access if an account shows signs of compromise.

Least Privilege & Authorization

Follow least privilege rigorously, each user (or service account) gets only the **minimum access** necessary, and only for the **duration** needed. Implement Role-Based Access Control (RBAC) and **Just-In-Time (JIT)** privilege elevation for administrators.

i.e. An accountant might normally view financial records but needs a one-time approval to initiate a wire above a certain limit. ***A policy administrator*** *system can handle such workflows, ensuring no direct access unless policy conditions are met.*

Tooling Recommendations

Consider enterprise solutions that offer integrated zero capabilities **(i.e. Microsoft's Zero Trust Suite (Defender + Azure AD Conditional Access + Endpoint Manager)** or **Google BeyondCorp Enterprise.** These provide device attestation, context-based access controls, and monitoring.

Network Access Control (NAC) appliances (i.e. **Cisco ISE or Fortinet NAC**) can enforce that only known, healthy devices connect to the office network. Additionally, **software-defined perimeter (SDP)** tools (like **Zscaler Private Access** or **Palo Alto Prisma Access**) enable secure remote access without exposing internal services to the internet, aligning with zero trust principles.

The goal is a **Unified Policy Layer** where every access (whether from an office PC, a home laptop, or a yacht's Wi-Fi) is evaluated and logged.

Executive Decision Points

Embracing Zero Trust is a strategic shift; the principal must support the investment and possibly usability trade-offs. Decision points include **choosing a Zero Trust Framework** (i.e. **Adopt NIST SP 800-207 guidance**) and selecting vendors / integrators to implement it.

Executives should set clear expectations, such as **no device or user gets a free pass,** even the CEO's own laptop will be checked for compliance each time. This culture of security must be endorsed top-down.

Also, decide on an implementation roadmap, it might be practical to start with a high-priority area (**like the financial transaction systems**) and gradually extend **Zero Trust** to all systems.

The benefit of using Zero Trust is that it helps contain damage if a hacker gets in.

For example, if an attacker manages to steal an employee's email password, in a normal system they might be able to move around and reach more sensitive data, like bank accounts or private client information.

With Zero Trust, each system is protected on its own. The hacker would be stopped when they try to go further, because every new access is checked again.

Even if one part is hacked, the really important data stays safe. This greatly reduces the impact of any breach.

Regulatory Mapping

While Saudi regulations don't explicitly mandate **Zero Trust** (it's a framework choice) the concept supports compliance: **PDPL's** requirement for protecting data from unauthorized access is inherently met by continuous verification. **The National Cybersecurity Authority's Essential Cybersecurity Controls (ECC-2:2024)** emphasize robust access control and monitoring, which Zero Trust Delivers.

SAMA framework encourages a **risk-based, layered defense,** Zero Trust Provides that by design (layered checks for every access). Moreover, NIST guidelines (NIST SP 800-207) are recognized globally, aligning with them demonstrates adherence to international best practices. Executives can be assured that investing in Zero Trust not only thwarts advanced threats but also positions the family office as a leader in compliance and security readiness.

CYBERSECURITY

Secure Bank Transfer Infrastructure

Secure Bank Transfer Infrastructure

Frequent multi-million-dollar transfers demand security on par with (**or beyond**) private banking. **Wire transfer fraud is a major threat** to UHNWIs, **criminals** have stolen immense sums by exploiting gaps in **transfer verification,** Deepfake voice calls or spoofed emails instructing fund transfers are a growing concern. The family office must implement an **airtight, tamper-proof process for all fund movements** to defeat both high-tech impersonation and low-tech fraud.

Secure Payment Workflow

Design the bank transfer process with **multiple independent verifications** and strict controls at each step:

Dual Authorization

Require at **least two** authorized people to approve any **significant wire transfer**. For instance, the CFO prepares the transaction and a second executive (or even the UHNWI principal via a secure app) must review and approve. This aligns with SAMA's expectations for strong internal controls on funds movement **(as seen in banking, no single individual should unilaterally move large sums)**

Out-of-Band Confirmation

Never rely solely on a single communication source for transfer instructions. If a request comes by email, **always confirm via a secondary channel (phone or in-person)** with the requester. For any transfer above a defined threshold, implement a **call back verification.**

A designated staff member calls the principal or requester at a predefined number (do not use any phone number provided in any email instruction) to verbally confirm the details.

Do not accept purely voice-based requests without a **secret verification code** or phrase known only to the principal and the office (to counter AI voice clones). As a policy, no wire details are ever changed via email alone.

If bank account details or beneficiaries change, require in-person or video confirmation. These steps address scenarios such as deepfake vishing, even if the voice sounds convincing, the imposter won't know the codeword that a quick challenge-response could require.

Multi-Factor Authentication for Banking Access

Ensure that any online banking portals or treasury management systems used by the office employ strong MFA (hardware token or biometric) for login and transaction signing. Ideally, use **dedicated hardware devices** or apps provided by the bank that generate one-time transaction codes

Some private banks issue secure tablets or smartcard readers (devices) for this purpose. This prevents hackers from stealing login credentials from actually executing transfers without the possession of the second factor.

Secure, Dedicated Banking Workstation

Use a dedicated, highly secure (hardened) computer or device only for wire transfers and financial transactions.

This device should never be used for everyday activities like email, web browsing, or document editing — only for banking. It should stay offline most of the time and only connect to the internet briefly when a transfer needs to be made.

The device should be:

- **Hardened** — meaning locked down with strong security settings
- Running an **up-to-date operating system** with all patches applied
- **No email or web browsing** installed, to avoid accidentally downloading malware
- Protected with **full disk encryption**, in case the device is stolen
- Connected to the bank using a **separate VPN** or **private network** for extra protection (if available)

In very high-security environments (such as some Ultra High Net Worth clients), the device has to be physically stored in a secure room.

The main goal is to eliminate the risk of a trojan, keylogger, or hacker stealing banking credentials or silently altering a wire transfer.

Transaction Anomaly Detection

Employ fraud detection tools or services to monitor online payments. Many banks offer customizable alerts, set these up (i.e. SMS/email to an executive for any transfer above X or to a new beneficiary).

Consider **third-party solutions that specialize in wire fraud prevention which can analyze patterns and flag suspicious requests** (for instance, if a request deviates from typical amounts and destinations).

Anomalies should trigger a manual pause and investigation before funds are irreversibly sent. As noted by industry guidance, **wire fraud often goes unnoticed for months.** Therefore, active monitoring can catch it immediately.

Tooling Recommendations

If the family office uses a **Treasury Management System (TMS)** or an aggregator platform for international transfers, ensure it's one that supports:

- Granular user roles
- Dual approval workflows
- Cryptographic signing of transactions.

*Examples would include **Kybria, FIS, or other private-banking-grade systems**, these often integrate security features like hardware cryptographic modules and out-of-band authenticators. For simpler setups use online banking, leverage the bank's highest security offering.*

For example, if the Family Office joins the SWIFT network, it must follow SWIFT's Customer Security Program (CSP) rules — or use a bank-provided VPN token to securely access banking systems.

In addition, set up a **Secure Email Gateway** with **DMARC enforcement**. This helps block fake emails that appear to come from trusted sources, such as law firms or even the principal's own email domain.

This greatly reduces the risk of falling for fraudulent payment requests sent by attackers pretending to be trusted contacts.

Additionally, consider subscription to a threat intelligence feed or service that would alert if the family office's email accounts are being impersonated on the internet.

Executive Decision Points

Executives should set clear policy that **no urgency overrides the verification protocol.** Cybercriminals **often pressure staff by creating false urgency** (this is your boss, wire now or deal falls through!), but leadership must empower employees to **slow down and verify** without fear, even if the request seems to come from the principal.

It's wise to run **drills**, **simulate a fraudulent payment request** (even using a deepfake audio if possible) to test if staff follows the protocol or they get duped. Then refine the process.

Another decision is **insurance,** evaluate cybercrime insurance that covers **fraudulent wire transfers** (though many policies would exclude **voluntary transfers authorized by the deceived staff).**

The office should also be aware of banks' stance, as noted, banks often disclaim liability if the transfer **was authorized by the office under false pretenses.** This means the family office **bears the full blunt of any mistake.** Therefore, investing in these preventative controls is non-negotiable from an outcome perspective. It could literally save millions and preserve trust.

Regulatory Mapping

Even though the Family Office is not a regulated financial institution under SAMA, it's still important to follow **SAMA's banking security guidelines**. SAMA's **Cybersecurity Framework** expects controls similar to those used by banks — such as **strong access controls, detailed logging, and internal review of transactions**.

Implementing these controls ahead of time is also wise because regulators could one day review large international transfers for **anti-money laundering (AML)** or **sanctions compliance**.

PDPL (Saudi data protection law) also comes into play — it treats financial information (like payment instructions and account numbers) as **sensitive personal data**, which means this data must be **securely transmitted and stored** (encrypted and access-controlled) to prevent misuse or leaks.

In addition, **CITC/CST telecom regulations** may apply if telecom channels (such as SMS) are used for transaction confirmations. It's important not to rely on SMS verification alone, since **SIM-swap fraud** is a known risk — and CITC has already instructed telecom providers to tighten SIM registration security for this reason.

CYBERSECURITY

Identity Access Management (IAM)

Identity and Access Management

Controlling **who can access what** is a cornerstone of cybersecurity, especially in a small but sensitive environment like a family office. **Identity and Access Management (IAM)** covers user accounts, authentication methods, and authorization policies. The goal is **zero tolerance for unauthorized access.** Every account and login must be legitimate, intended, and limited in scope.

Core IAM Controls

Strict Authentication (IAM Everywhere)

Implement multi-factor authentication for all users and all systems. This would include:

- Emails
- **VPN/remote access**
- **Banking Systems**
- **Cloud Services**
- **Cven local Windows or Mac logins if possible.**

Use **hardware-based MFA tokens** (i.e. YubiKeys or smart cards) or biometric factors for the **highest security**, as these are phishing-resistant compared to **SMS/OTP codes**. **Under no circumstances should high-risk accounts (executives, IT admins, finance officers) be allowed single-factor (password-only) login.**

MFA significantly reduces risk of credential theft leading to a breach.

Privileged Access Management (PAM)

Identify the most sensitive (“crown jewel”) systems — such as financial transaction platforms, document vaults, and security consoles — and make sure that administrative or privileged accounts for these systems are tightly protected.

Use a Privileged Access Management (PAM) solution, or at least a secure vault to store and manage admin credentials (for example, tools like CyberArk or Thycotic, which help control and audit all admin logins).

Admins should use their regular user accounts for day-to-day tasks like email or web browsing. When they need **privileged access**, they should perform **just-in-time elevation** — meaning they temporarily elevate their access, using **multi-factor authentication (MFA)** and ideally recording the session for auditing.

SAMA requires banks to secure privileged accounts, and even though the Family Office is not a bank, it should treat admin access with the same level of importance — because these accounts can control critical systems.

Role-Based Access & Least Privilege

Define roles (e.g. Relationship Manager, Accountant, and Executive Assistant) and assign **system permissions based on those roles**, ensuring each person only sees data and functions necessary for their job.

For example, an assistant might have access to calendar and travel itineraries but not to banking information, investment advisors might see portfolio data but not personal medical records of the principal.

Implement **segregation of duties,** critical operations (such as setting up a new payee and initiating a payment) should **require two different roles to complete**, so no single user misuse can slip through.

Regularly review who has access to what (e.g. quarterly access recertification by leadership). **Immediately revoke access when someone leaves or changes role (have a documented off-boarding checklist with IT).**

Identity Federation and SSO

Set up a **central identity system** (such as **Azure Active Directory** or a similar solution), so that **each user has one trusted identity used across all office systems**. This enables **Single Sign-On (SSO)** — meaning users can access all their applications (email, file storage, CRM, etc.) using **one secure login** instead of juggling multiple passwords.

This approach allows for **unified security policies** and makes it possible to **instantly revoke all of a user's access** if needed (for example, if an account is compromised or an employee leaves).

It also improves convenience: users can focus on maintaining **one strong password with Multi-Factor Authentication (MFA)**, which is both more secure and easier for them.

Finally, use **short-lived SSO tokens** that are linked to the **context of the login** (device type, location, etc.), following **Zero Trust principles** — so that even after login, access is continually verified and risk-aware.

Continuous Identity Monitoring

Invest in tools that monitor user account behavior for **anomalies**. For instance, if a normally inactive user starts downloading large amounts of data at **2AM**, the system should alert or automatically lock it for pending review.

Modern **IAM platforms** with **User and Entity Behavior Analytics** (UBEA) can detect if an account might be compromised or a rogue insider is snooping.

Also implement **password policies** (passphrases, regular rotation or better, password-less with biometrics) and check new passwords against known-breach databases to avoid weak credentials.

Tooling Recommendations

Use an **enterprise-grade Identity and Access Management (IAM) system** — such as **Microsoft Entra / Azure Active Directory** or **Okta Identity Cloud** — to manage **central identity**, enforce **multi-factor authentication (MFA)**, and apply **conditional access** policies. These systems can integrate with **cloud applications (SaaS)**, **on-premises systems**, and even control access to **VPNs**.

For managing **privileged (admin) accounts**, consider using a dedicated **Privileged Access Management (PAM)** solution, like **CyberArk** or **BeyondTrust PAM**. These tools securely store (vault) admin credentials, monitor admin sessions, and automatically rotate sensitive passwords or keys to reduce risk.

If a full PAM system is too complex for your current needs, at minimum, use a **secure password manager** with access controls — such as **1Password Teams** or **LastPass Enterprise** — for any shared credentials. And enforce a strict policy: **no passwords should ever be stored in plain text or in spreadsheets**.

Additionally, enforce **device authentication**: any device connecting to the office network should present a valid **security certificate** or **token** to prove it is a trusted, managed device. This prevents unauthorized or personal devices from gaining access.

Note: Given the sensitivity of data, even trusted employees should have their access logged and subject to review. Executives should mandate **audit trails** for all privileged actions. This isn't about mistrusting staff, but rather it's having accountability and early warning if an account (whether employee or attacker using an employee's account) does something abnormal. Clearly communicate to the small team that these measures protect everyone.

Regulatory Mapping

The Saudi **PDPL** explicitly requires data controllers to implement measures to prevent unauthorized access to personal data. Strong IAM (Access Controls, Authentication, and Authorization) is the frontline in meeting this requirement, for instance, only authorized personnel should access client personal info, and only for authorized purposes.

SAMA's framework, while not binding on a family office, provides a benchmark it expects robust identity management, least privilege, and **secure management or privileged accounts** in financial entities. Emulating these controls helps to ensure the family office's security is **bank grade.**

CITC/CST regulations for the ICT sector include cybersecurity requirements that mirror IAM best practices (the CST Cybersecurity Framework 2020 requires telcos to use MFA for privileged users, for instance, which is a good standard to adopt internally).

NIST guidelines (800-53, CSF) emphasize IAM as a core function ("Protect" category), so aligning with NIST ensures international best practice.

In summary, by enforcing strong IAM, the office not only protects itself but also ticks the compliance boxes for "appropriate access control measures" demanded by regulators globally.

CYBERSECURITY

Data Encryption and Document Vaulting

Data Encryption and Document Vaulting

A family office typically handles extremely sensitive documentation, **from bank statements and investment agreements to personal legal papers and identity documents. A document vault approach is essential,** all sensitive files should be stored and managed in a way that even if attackers breach other defenses, they **cannot read or tamper with the data.**

This is achieved through robust encryption (data confidentiality) and **strict vaulting** (controlled, and monitored access).

Encryption Strategy

All data, whether at rest or in transit, should be encrypted using strong, industry-standard algorithms:

- AES-256 of symmetric encryption
- RSA-4096, or ECC with at least 384-bit for asymmetric,

The encryption must cover the following:

Data At Rest

Encrypt the storage for all **servers**, **workstations**, and **mobile devices** (full disk encryption via BitLocker, FileVault, or mobile device encryption). For shared storage or file servers, employ volume or folder-level encryption.

Ideally, use an enterprise **Digital Rights Management (DRM)** or information protection solution so that even if a document is copied off server, it remains encrypted and access-controlled. Implementing **Microsoft Purview Information Protection** or **VERA DRM**, for instance, can ensure a document is only openable by authorized users on authorized devices.

Data In Transit

Mandate encryption for all network communications. This includes using up-to-date TLS for all web and email traffic. (i.e. enforce SMTP TLS for emails with your providers), encrypted VPN tunnels for any remote connectivity, and secure voice/video calls (addressed in the communications section). Even internal network traffic should be encrypted if it carries sensitive data (i.e. use SSH/SFTP for file transfers, not FTP, use database encryption protocols, etc).

End-to-End Encryption for Confidentiality Channels

For the most sensitive communications (**Board decisions, legal strategies**, etc), consider deploying **end-to-end encryption (E2EE) tools**. For instance, **an E2EE email system (such as ProtonMail for external communication or setting up S/MIME with your own PKI**) ensures that even email providers or IT administrators cannot read the content. Similarly, **secure messaging apps with E2EE ensures in-transit and server-side encryption.**

Document Vault & Key Management

Establish a **secure document management** system (**Vault**) for all critical files. This could be a specialized and secure cloud service for an **on-premises encrypted repository**. The key features should include:

- **Encrypted Storage**
- **Granular Access Controls**
- **Versioning**
- **Audi Logging of all access**

Products such as **Tresorit, Box Shield, or SharePoint** for **sensitivity labels** can serve as a vault. Access to vault documents should require MFA and possibly device attestation (only company laptops which have certain security posture can sync documents). To prevent tampering, use **integrity controls.**

*e.g. Digital Signatures on files or at least hash comparisons, so if a document is altered, it can be detected. Some vaults provide a **secure viewer** that watermarks documents and prevents easy copying. **This is good for ultra-sensitive documents** such as passport scans or account numbers.*

Crucially, manage **encryption keys** with great care. Use a **Hardware Security Module (HSM)** or Cloud Key Management Service (KMS) for storing master keys. The keys should

be protected from insider threats as well. E.g. use a split knowledge or multi-approval system to retrieve a master decryption key.

Rotate encryption keys periodically and have a clear key lifecycle policy (as SAMA notes, organizations must manage encryption keys' generation, distribution, archiving, and destruction properly).

For data shared with external parties (Lawyers, Banks), use encrypted containers or at least password-protected files with strong encryption, exchanging passwords by a separate channel.

Anti-Tampering and Resilience

Beyond confidentiality, ensure stored data can't be silently altered, use **write-once media** or **immutable storage** for certain records.

i.e. For instance, backups or official records can be stored on **WORM** drivers or **Cloud Storage with Object Lock**

This would prevent attackers or even **administrators** from retroactively modifying or deleting records (which is important for compliance and for recovery from ransomware).

ZATCA's e-invoicing rules explicitly required stored invoices to be temper-evident, the same concept can be extended to other critical documents (e.g. a tamper-proof log of all transfers, etc.). Therefore, implement file integrity monitoring on vault files and system binaries, alerts should fire if any unexpected changes occur.

Tooling Strategies

Hardware

Invest in **Hardware Security Module** (**HSMs**) or use Cloud HSM services (such as **AWS CloudHSM, or Azure Key Vault with HSM**) to store encryption keys. This would provide a vault for the vault's keys, ensuring keys never appear in plaintext in memory and cannot be extracted even if a server is compromised.

Software

For vaulting, consider solutions such as **HashiCorp Vault** (Useful for storing secrets such as passwords, certificates, as well as handling dynamic encryption / decryption of data on the fly), as it integrates with HSMs for master key security.

For document management, if the office prefers **on-prem, NextCloud** with end-to-end encryption enabled or **OwnCloud Enterprise** with integrated encryption modules could be set up in the **Saudi Office or a Saudi Data Center**. These give full control over data location.

If cloud is acceptable, look at **Tresorit or Box Shield,** which would offer client-side encryption and data residency options (Ensuring encrypted data is stored on EU or KSA servers as needed).

Email & Data Sharing

Use PGP or S/MIME to encrypt emails when sending sensitive information. This ensures that even if someone intercepts the email, they cannot read its contents. **While this requires some user training, the executive assistants and IT team can manage the encryption keys and help enforce that sensitive attachments are always encrypted before being sent.**

As an alternative, instead of sending sensitive files by email, **use a secure file-sharing portal, such as Citrix ShareFile or a virtual data room service.** These platforms require recipients to log in and authenticate before they can download files. Additionally, all files are encrypted at rest inside the portal for added protection.

Executive Decision Points

A key decision that needs to be made is where to store **sensitive data:**

- **On-prem**
- **Private Cloud**
- **Approved Public Cloud**.

Given **PDPLs** data residency requirements, many family offices opt for **private cloud in-country** or a hybrid approach **(sensitive data stays on a secure on-prem server or local cloud zone, while less sensitive can use global cloud services).**

Executives should also approve a **data classification policy,** to define what is **Highly Confidential vs Internal vs Public data** and mandate encryption for anything confidential.

This policy guides IT in configuring which files/folders get **extra protection or vaulting.**

Another decision is whether to **invest in advanced tech such as confidential computing** (**CPUs that encrypt data in use**) for extra protection, **likely not needed initially**, but keep an eye on it as it matures because that could protect data even during processing.

Leaders must ensure **user convenience vs security** is balanced. Encryption can introduce complexity (lost keys, difficulty searching encrypted data, etc.). **To mitigate this, allocate budget and expertise for proper key management and user training.**

Show staff how to use secure tools (e.g. opening a secure email, or accessing the vault with an app) so that security doesn't get bypassed for being too hard.

Emphasize that protecting client privacy and the principal's sensitive information is a top priority, this ethos would encourage everyone to respect and adhere to encryption protocols rather than seeking workarounds.

Regulatory Mapping

This area has direct legal mandates. The Saudi PDPL (Article 19) requires controllers to implement technical measures to protect personal data, explicitly during storage and transmission. It emphasizes encryption, as **PDPL** and it's regulations expect strong encryption for sensitive personal data and following **NCA's** issued controls on encryption. By encrypting data at rest and in transit, the family office is essentially fulfilling that obligation.

SAMA's cybersecurity guidelines require financial organizations to properly define, implement, and manage encryption and cryptographic keys. The Family Office can follow this as a best practice benchmark.

Similarly, **CITC/CST regulations** for telecom providers require encryption to protect customer data. Even though the Family Office isn't a telecom company, it's still smart to align with these practices — for example, by using **CST-approved encryption standards**.

By implementing strong encryption and secure vaulting of sensitive data, the Family Office not only protects valuable information but also shows it is following best practices and maintaining compliance with both local (**Saudi**) and global data protection standards.

CYBERSECURITY

Securing Vendor & Third-Party Access

Securing Vendor and Third-Party Access

No family office operates **in complete isolation,** external vendors and third parties (investment managers, law firms, IT support provides, luxury concierge services, etc.) will require access to certain systems or data. However, every third party is a **potential new attack vector or weak link.**

Many high-profile breaches originate from **a compromised vendor**. The family office would need a rigorous **Third-Party Risk Management** program to extend its security parameter to anyone touching it's data or systems.

Third-Party Risk Management Framework

Due Diligence & Onboarding

Before engaging a vendor or giving them any access, **perform a basic cybersecurity due diligence**. This can range from a **checklist or questionnaire (Asking if they follow standards such as ISO 27001, how they encrypt data, if they do employee background checks, etc.)** to a more formal assessment for critical vendors.

For instance, if hiring an external accountant who will access financial systems, verify that their firm has adequate security **(MFA on their devices, confidentiality agreements in place, etc).** If a vendor will handle personal data, **PDPL effectively requires you to ensure they can protect that data as you would**. **Include the office's IT or CISCO advisor in vetting critical vendor's security postures.**

Contractual Safeguards

All contracts with third parties should include robust data **protection and cybersecurity clauses.** Require them to comply with the family office's security policies (or an agreed standard), to **notify the office immediately in event of any breach, and cooperate in incident investigations.**

Include **confidentiality/non-disclosure agreements** specific to cyber and data handling. Ideally, contracts should specify **consequences** for security failures (e.g. the vendor bears costs of a breach if due to their negligence).

For any **cloud or IT service providers**, negotiate for the right to audit their security controls or at least request annual third-party audit reports **(SOC 2 type II reports. Penetration test results, etc.),** Ensure agreements cover data residency if relevant **(e.g. the vendor must not transfer personal data out of Saudi Arabia without permission, therefore aligning with PDPL.**

Least-Privilege Access for Vendors

Provide vendors **only the access they absolutely need, and only when needed.** Use separate vendor accounts that are disabled when not in use. For instance, if a support engineer from an IT service provider needs to remote in to fix a computer, create a temporary account for that session or use a **remote support tool** that you can enable / disable.

Don't share internal passwords, use privileged session management tools that let vendors perform their work without learning credentials (some PAM tools allow one-time connection links).

If an external accountant needs to review files, give them a restricted portal or folder with read-only access, not your entire file server. Monitor all vendor activity, their actions should be logged and perhaps even supervised in real-time for sensitive tasks.

Network Segmentation for Third Parties

If vendors must connect with your network, put them on an isolated segment or use a VPN that only allows access to specific systems. For instance, a maintenance vendor shouldn't be on the same network segment as financial servers, give them a **contractor network** which only reaches what's necessary (e.g. a printer or a specific PC).

Better yet, adopt a **Zero Trust Network Access** approach for third parties: instead of full network VPN, give them an application-level access (through a secure gateway) to only the applications or systems they need. This would reduce the risk of them inadvertently spreading malware or snooping elsewhere.

Continuous Oversight and Revocation

Keep an up-to-date list of all third-party vendors and exactly what systems they can access, and what level of access they have.

Review this list **regularly** — for example, **every 6 months** — at the **executive level**, and ask yourself:
"Do we still need this vendor or consultant to have access to this system (such as the CRM)?"

Many times, **temporary access** granted for a specific project is never revoked afterward — this creates risk. You should actively **close that gap**.

When a contract ends, or if a **vendor employee who had access leaves their company**, their access must be **immediately disabled**. It's also important to require that **vendors notify you** when key staff members who had access leave, so their accounts can be revoked on your side.

Some Family Offices go a step further and schedule **periodic third-party access audits** — where an **internal** or **external auditor** reviews all vendor accounts and verifies that each one is still **justified** and **compliant with security policy**.

Tooling Recommendations

Use a **Vendor Access Management Solution** or features within existing systems to sandbox **third-party interactions**.

*For instance**, Microsoft Azure AD's B2B** feature can manage guest access with expiration dates.*

If using a remote support service (like **TeamViewer**, **LogMeIn Rescue, or BeyondTrust Remote Support**), configure it so that sessions require approval and are recorded. Consider a **Security Rating Service** (Such as **BitSight, or SecurityScorecard**) to continuously monitor critical vendors' external cyber health (this can alert if, say, your law firm's network is seen hosting malware, a red flag).

For highly sensitive collaborations, use a **Virtual Data Room (VDR)** platform (e.g. **Intralinks or Drooms**, this is common in private banking for sharing documents with third parties under tight access controls (watermarks, no copy/pasta, timed access).

It might be overkill for routine work, but for certain deals or disclosures, a VDR ensures third parties can view documents without ever downloading them.

Executive Decision Points

Decide **which vendors are deemed critical** (ones which could harm you if they're compromised) versus low-risk. Focus resources on managing the high criticality ones. Leadership should endorse the stance that **if a third-party wants to work with us, they must meet our security expectations.**

This might mean occasionally walking away from a vendor that has poor security (e.g. **a boutique service that refuses to use MFA or host data in-country**). These are business decisions weighing convenience / cost of vendor vs risk introduced.

Also, consider the **insider threat aspect** where sometimes **third parties** have staff working on your account who become de-facto insiders. The family office should decide on measures like background checks, you might request that any consultant handling your sensitive data undergo a background screening similar to what you'd do for employees.

While you can't dictate another company's HR, you can stipulate in contracts that named individuals will work on your account and substitutions require approval (so you at least know who has access).

Another **executive call is cyber insurance coverage for third-party breaches.** If a breach occurs via a vendor, who covers the damage? Ensure the office's cyber insurance (and or the contract's indemnities) cover such scenarios. The board or principal should be aware of the biggest third-party risks (perhaps have your IT advisor present. E.g. The external IT provider's level of access, and how they're mitigated.

Regulatory Mapping

Under **PDPL,** If the family office (as a data controller) engages a third-party (data processor) to handle personal data, the law makes **the controller responsible for ensuring the processor complies with PDPL and protective measures.** So from a legal standpoint, **you must have contractual and practical safeguards,** exactly as described in the clauses and oversight above.

Otherwise, the office could be liable for vendor's failings. **SAMA** and **NCA** both have requirements around outsourcing and third-party management for regulated entities (e.g. banks must conduct annual reviews of critical supplier's cybersecurity).

Emulating those, the family office should document it's vendor vetting process and perhaps even keep evidence of having received **ISO certs or Security reports from key vendors**.

CITC/CST regulations in sectors such as cloud computing mandate that providers isolate customer data and follow strong security, so if the family office uses any cloud, ensure the

provider adheres to **CST's Cloud Cybersecurity Controls (**Which many big cloud providers in the KSA now align with).

GDPR if in scope also requires data processing agreements with third parties and puts joint liability on controllers for vendor breaches.

In summary, showing that you **enforce strict standards on all third-party vendors** will satisfy regulators that you are not the weak link in a larger supply chain. It also protects the family office's reputation and operates from being derailed by someone else's security lapse.

CYBERSECURITY

High-Security Communications Suite

High-Security Communications Suite

Ultra-secure communications are vital to prevent the following possible attack vectors:

- **Eavesdropping**
- **Impersonation**
- **Interception**
- **Spying on Sensitive Discussions.**

The principal should set up a highly secure communication system to handle all confidential voice calls, video meetings, messages, and emails. This ensures that sensitive discussions and information are fully protected from eavesdropping, interception, or leaks.

This ensures that whether the UHNWI principal is on a yacht in the Mediterranean or staff are coordinating from Riyadh, all channels are encrypted and authenticated **end-to-end.**

Secure Video Calls

Traditional phone calls (PSTN) or unencrypted **Voice Over Internet Protocol (VoIP)** are vulnerable to interception (by attackers or even surveillance). Equip the principal and key staff with **secure phones or apps** that provide end-to-end encrypted voice calling.

*For instance, use reputable encrypted calling apps such as **Signal Private Messenger** or **WhatsApp** (which use the signal protocol for encryption) for routine secure calls.*

These are user-friendly and offer strong encryption. For more sensitive or mission-critical communication, consider specialized **secure phones,** solutions would include **BlackBerry SecuSUITE, KryptAll** or devices from **Glacier** or **Bittium** provide hardened phones with **256-bit AES voice encryption.**

Some ultra-secure phone kits (such as **Glacier's encrypted phones**) even come with custom hardware, Faraday carry sleeves, and private VPN routing. To ensure calls and texts travel through an anonymized, encrypted network. These can be used for the most sensitive conversations (e.g. discussing deal negotiations, political or security issues).

The trade-off is **cost and some convenience**, so the executive team can decide which calls truly need this military-grade approach. At a minimum, **never discuss sensitive business over normal, unencrypted phone lines,** always switch to a secured channel.

Secure Messaging and Chat

Standard SMS or messaging apps without E2E encryption are not acceptable for **confidential information.** All internal and principal-to-staff messaging should use **end-to-end encrypted messengers. Signal** again is a top choice (open-source, vetted). Others like **Wicker Enterprise, Wire Secure Messenger, or Threema Work** are available for enterprise-managed scenarios.

These allow for self-destructing messages, preventing any history from accumulating. Configuring disappearing messages for especially sensitive chats (e.g. messages auto-delete after a day or a week).

Also, ensure **identity verification** features are used, for instance, **Signal has safety numbers to verify contacts.**

Staff should always verify new contacts in person or through a trusted secondary channel when communicating for the first time. This helps prevent **man-in-the-middle attacks**, where an attacker pretends to be someone else.

If the Family Office needs to send a message to all staff (for example, an **emergency alert**), it's safer to use a **secure group chat** within an approved communications app — rather than sending it by **email** or **SMS**, which can be intercepted or spoofed.

Secure Emails

Email is often the hardest communication channel to fully secure, simply because it is so widely used. However, because email is a common target for **phishing** and **interception**, the Family Office's email should be properly **hardened**.

One option is to use a **secure email provider** that offers **end-to-end encryption (E2E)** and ensures emails are stored in **privacy-friendly countries** with strong data protection laws.

For example:

- **ProtonMail** (servers in Switzerland, with built-in E2E encryption)
- **Tutanota** (servers in Germany, also with E2E encryption)

This helps protect sensitive emails from being read or tampered with — both during transmission and while stored.

Alternatively, stick with **Microsoft 365 or Google Workspace** but layer on **S/MIME or PGP encryption** for particularly sensitive email threads. The IT team can generate **S/MIME** certificates for each user so that emails between principal and office, or between office and known external recipients (like a lawyer) are automatically encrypted and signed.

This would ensure confidentiality and also **authenticity** (digital signatures confirm the sender's identity, mitigating impersonation). Educate all correspondents that whenever an email concerns funds or confidential instructions, it **must be signed or encrypted** to be considered valid. This habit also makes any unsigned email claiming urgent actions stand out as suspicious.

Secure Video Conferencing

For board meetings or confidential discussions that happen over video, use platforms that support end-to-end encryption for calls. For instance, **Zoom now offers an option** for end-to-end encrypted meetings (thought it has limitations like no phone dial-ins), and **Webex** has an E2E encryption mode as well.

Another option for secure video calls is to **host your own video conferencing server** — for example, using **Jitsi** (with end-to-end encryption enabled), or **Cisco Meeting Server** on-premises.

If the list of participants is **small and known**, using an **app** like **FaceTime** (which is end-to-end encrypted between Apple devices) can also be a simple and secure choice for **one-on-one calls**.

However, because **enterprise control** is limited with consumer apps, it's often better to use a more **managed platform** for larger or more sensitive meetings — such as **Signal's secure video** feature, or **Webex with end-to-end encryption**.

For **any video call**:

- Always use **unique meeting IDs** and **strong passcodes**
- Share those details **only over secure channels**
- Enforce a policy that **no sensitive meeting should allow unknown participants** → For example: **disable "join before host"**, and use **waiting room features** to manually admit only trusted attendees.

Physical & Environmental Security

In addition to digital encryption, be mindful of **physical eavesdropping.** For the most critical in-person meetings, consider using **Privacy Measures**

e.g. *meet in a room that has been swept for bugs, use a white noise generator outside the room to prevent laser microphone spying through windows, and ban all personal devices in the room (so no one unintentionally has a malware recording audio).*

While this is beyond IT, it's part of communications security for a UHNWI, the office's security chief should handle this in coordination with cybersecurity.

Tooling and Integration

Deploy an **Enterprise Mobile Management (MDM)** solution to manage secure communication apps on staff mobile devices. For instance, if using an enterprise chat such as **Wickr or Wire,** manage it via **MDM** so **you can remotely wipe it if a phone is lost.**

For email, if you remain on **Outlook 365**, use Microsoft's information protection and encryption plugin which lets users click **Encrypt** on an email. This uses **Azure Rights Management** to encrypt the email even if going out to external recipients (they get a secure web portal to read it). That may be easier operationally than **PGP for less technical users.**

Also train everyone on verifying they're on the phone/app with the right person.

E.g. teach how to check Signal safety numbers or verify that an email digital signature is valid.

These steps ensure that Trust is never implicit in communications, echoing the Zero Trust philosophy on the human communication level.

Executive Decision Points

The principal and executives should determine **which communication channels will be official for what purposes.** For instance, decide that **Signal will be used for any urgent financial instructions,** and anything else will be **ignored.**

This would help staff know how to expect genuine communications and how to avoid falling for imposters. It might be decided that all voice instructions be followed up with a secure text confirmation (**Yes, I just told you to do X**) using the known secure app.

This double layer would defeat a pure voice deepfake attempt. The family may also choose to keep some communications entirely **offline, particularly the most sensitive information**

(e.g. extremely sensitive account numbers or vault codes only delivered in person or via a paper document).

Executives should weigh the convenience, requiring the use of a separate secure phone for all calls vs only the highest sensitivity. A risk-based approach can be taken. **Importantly, commit to consistency,** as **a secure system is only effective if everyone consistently uses it.** Leadership has to set the example (The principal uses it, so all follow the suit).

Budget decisions come into play too, specialized secure phone hardware and services can be expensive (secure phone kits can be thousands per month). Therefore, the office must decide if the **Ultra-High security provided by those is worth the cost for their needs,** perhaps opting to equip only the principal and key security staff with them and using software solutions for the rest.

Regulatory Mapping

CITC (now called CST) used to regulate the use of encryption for communications in Saudi Arabia. But since 2017, consumer **VoIP apps (like WhatsApp, FaceTime, etc.)** have been allowed, and using strong encryption is no longer prohibited.

Today, there is no regulatory issue with using fully secure, encrypted communications inside the Family Office — as long as you can meet lawful access requirements if authorities ever request it (for example, being able to provide access through proper legal channels if needed).

i.e. If the government needed data for an investigation, **but if you use end-to-end encryption,** you simply might not have the keys, **this is a known tension point, though Saudi Law hasn't banned E2E encryption).**

From a compliance perspective, **Basic Law of Governance in KSA guarantees the privacy of telephone and postal communications,** which implicitly supports using encryption to uphold that privacy. **PDPL** requires protecting personal data during transfer, end-to-end encryption is the strongest way to do that, so it actually puts you in compliance when sharing personal data over email or messaging.

From a **compliance perspective**, the **Basic Law of Governance** in Saudi Arabia guarantees the **privacy of telephone and postal communications**, which in turn **supports the use of encryption** to protect privacy in modern communications.

In addition, **PDPL** (the Personal Data Protection Law) requires that **personal data is protected during transfer** — and using **end-to-end encryption** is the strongest way to meet this requirement. In fact, encrypting emails or messages that contain personal data actually helps you **stay in compliance** with PDPL.

In summary: using a **high-security communications suite** protects **sensitive deals, financial transactions, and personal conversations**, ensures that **executive instructions can't be impersonated or altered**, and shows that the Family Office is taking the right **technical measures** to meet both **PDPL** and **international best practices** for communications security.

CYBERSECURITY

Incident Detection and Response (SIEM + SOAR)

Incident Detection and Response (SIEM + SOAR)

Prevention alone isn't enough, **even military-grade** defenses can be **breached** by a determined adversary. **The family office** must be able to **detect intrusions or anomalies quickly and respond decisively** to minimize damage.

This is where a **Security Information and Event Management (SIEM)** system combined with **Security Orchestration, Automation, and Response (SOAR)** becomes invaluable. Together, they serve as the digital nerve center of cybersecurity operations, **collecting signals from everywhere and orchestrating a rapid defense and recovery.**

Security Information and Event Management (SIEM)

A **SIEM** platform aggregates logs and events from all the office's IT systems:

- Firewalls
- Servers
- Endpoint Antivirus
- IAM system
- Cloud Services
- Etc

For instance, the **SIEM** will log every login, every file access, and every network connection, and can be turned to detect patterns like multiple failed login attempts (potential brute force), or a login from an unusual location. Or a device suddenly communicating with an IP known for malware.

The SIEM provides a **unified view of the security landscape** and can raise real-time alerts for investigation. In an environment as small as a family office, a properly configured SIEM helps a leanIT/security team punch above its weight.

It automates the heavy lifting of monitoring vast data for the **needle in a haystack,** that could indicate a breach. Modern **SIEMS** (Like **Splunk, IBM QRadar, or Azure Sentinel**) also incorporate **UBEA (User and Entity Behavior Analytics)** to detect anomalies in behavior, and can ingest threat intelligence feeds (to flag if any communication is going to known bad domains, for instance).

Security Orchestration, Automation and Response (SOAR)

SOAR picks up where SIEM alerts leave off, it **automates and coordinates the incident response actions.** When the SIEM flags something (say, a possible malware infection on a PC), a SOAR platform can automatically take a series of steps which are:

- **Create a Ticket**
- **Send an Alert to the IT/Security Personnel**
- **Isolate the Affected Machine from the network**
- **Pull Relevant Logs**
- **Trigger a Virus Scan**

All within seconds, **24/7 without waiting for human intervention.** The aim is to drastically reduce the **dwell time of threats.** In practice, we will configure **playbooks** in the **SOAR**, predefined workflows for certain incidents, such as for instance:

- *If suspicious login, then push MFA re-authentication or lock the account and alert admin*
- *If ransomware behavior is detected, then disconnect the system, kill processes, begin backup restore workflow.*

With SOAR, the response becomes **consistent, fast, and less reliant on an individual's presence or judgment in the heat of the moment.**

Integrated Security Operations

In an ideal setup, the SIEM and SOAR (which may be combined into a single solution would provide the following **benefits:**

24/7 Monitoring

Even if the office is small, threats can strike anytime. The SIEM should be monitored around the clock, **either by an internal on-call rotation or via a Managed Detection & Response (MDR) service.** Given resource constraints, the family office might contract a reputable **MDR provider** or a **Security Operations Center (SOC)** service to monitor the SIEM alerts.

There are **firms that specialize in serving HNW and small organizations with high security needs.**

Rapid Incidence Response

The moment an **incident is confirmed** (whether a malware outbreak, unauthorized access, or data leakage), have an **Incident Response Plan** in place which would include:

- Who to call?
- What systems to isolate?
- How to communicate if systems are compromised

The SOAR can enforce the first steps, but human oversight is needed **for complex decisions,**

For instance, if a device is suspected of being compromised, the playbook might cut off the network and notify IT.

Then IT follows the IR plan to forensically investigate that device (perhaps utilizing an external incident response retainer if needed) and determine the scope.

The Plan should also handle external notifications, i.e. PDPL requires notifying the authority and possibly impacted individuals if a breach has the potential to harm data subjects.

The SIEM will have the audit trails needed to understand what happened, and the SOAR logs will show what actions were taken and when, which is very useful for post-incident reporting.

Tooling Recommendations

Deploy a cloud-based SIEM such as **Microsoft Sentinel** (especially if the environment is largely **Microsoft/Azure oriented**) or **Splunk Cloud or Elastic Security Stack.** Cloud SIEMs can be easier to manage for a small team and can even scale without **on-prem hardware.**

Microsoft Sentinel for instance has built-in connectors for Office 365, Azure AD, etc. and comes with AI analytics. **Splunk is very powerful and can ingest from virtually anything (Firewalls, VPN, endpoint logs, etc).**

For SOAR, tools such as **Palo Alto Cortex XSOAR or Splunk's Phantom (now Splunk SOAR),** or even Sentinel's Built in Automation (using Logic Apps) can be used. These allow creating the automated playbooks.

The following is an example of what a playbook would look like:

Disable User in Azure AD ➔ Quarantine Machine in Defender ATP ➔ Send Slack/Teams alert to admin channel ➔ Create ticket in ServiceNow

Also consider **Endpoint Detection and Response (EDR)** solutions such as:

- CrowdStrike
- Microsoft Defender for Endpoint
- Carbon Black

These systems often integrate with **SIEM** and **SOAR** platforms. They can automatically detect and block many threats directly at the device level. They also provide **telemetry** to the SIEM and can take immediate action on known malicious patterns (for example, stopping a suspicious process in real time).

XDR (Extended Detection and Response) is the current industry term for solutions that integrate **endpoint, network**, and **cloud** detection capabilities. Tools like **Microsoft 365 Defender** or **Palo Alto Cortex XDR** consolidate signals across these domains and work as a strong complement to the **SIEM/SOAR stack**.

You should ensure that **all critical assets** are sending their logs to the **SIEM** — this includes **VPN logs, email security logs, cloud admin activity logs**, and others. Additionally, define **alerts** for key events

For example, if a new user account is created, which could indicate a silent compromise if not performed by a known administrator.

Leverage **threat** intelligence subscriptions (many **SIEM** platforms include this feature) to receive continuously updated indicators of compromise (**IOCs**).

Executive Decision Points

Even though this is technical, executives do have **key roles here,** first, **supporting in investing in monitoring,** it's not as viably satisfying as a shiny gadget, but it's insurance. Leaders should ask for regular reports from the **SIEM** e.g. a monthly summary of incidents detected and responded to.

This would keep visibility high and justifies the ongoing cost. Decide whether to **staff internally or outsource the 24/7 monitoring. A family office likely cannot have a full in-house SOC team working shifts,** outsourcing to a trusted SOC provider (Perhaps one with experience in baking or government security) is wise. **The cost can be wrapped into a service contract.** Therefore, ensure proper **NDAs and maybe have that provider vetted (they will see sensitive logs).**

Another decision, is to define **what constitutes as a security incident** that warrants informing the principal or halting operations.

For instance, if an admin account is compromised, does the office temporarily pause wire transfers?

Having an executive-agreed threshold ensures in an incident the responders don't waste time seeking approval for necessary actions.

Also determine how to handle **public communications** and **legal disclosure obligations** in the event of a data breach or other security incident. While the family office will naturally prefer to keep incidents **confidential**, laws such as **PDPL** (Saudi Personal Data Protection Law) or **GDPR** (if applicable to cross-border operations) may require some level of **disclosure**.

The **executive team**, in coordination with **legal counsel**, should pre-draft **response plans** — for example, if personal data is leaked, how to **notify affected individuals**, **regulatory authorities**, and **mitigate** the incident. As part of this planning, explicitly define **which regulatory authorities** would need to be notified under various scenarios (e.g. **SDAIA** in Saudi Arabia for PDPL compliance, **EU supervisory authorities** for GDPR-covered data, or **local data protection regulators** in other jurisdictions where the family office operates or holds assets).

Regulatory Mapping

Detecting and responding to incidents ties into compliance on multiple fronts. **PDPL Article 20 demands that upon a breach leading to illegal access of personal data, the organization must inform authorities (and data subjects if harm is likely) without undue delay.**

Without a robust detection system, you might not even know you were breached, which would itself become a compliance failure if you failed to notify in time. **So SIEM+SOAR indirectly helps meet breach notification laws by ensuring you catch incidents early.**

SAMA expects banks to have **continuous monitoring and incident response capabilities**; it's not a stretch to say a family office managing large funds should do the same. In fact, the **National Cybersecurity Authority's Essential Cybersecurity Controls** require government and critical organizations to have incident detection systems and to report serious incidents to **NCA.**

While the family office does not formally fall into those regulatory categories, **aligning to those standards** is highly beneficial — and establishing a **communication channel with the NCA** (National Cybersecurity Authority) or **Saudi CERT** for major incident support would further strengthen the office's posture. Leading frameworks such as **CISA** (USA) and **ENISA** (EU) also recommend deploying **SIEM** and **SOAR** systems to align with models like the **NIST**

Cybersecurity Framework (Detect and Respond functions) and **ISO 27001 operations management**.

By implementing **SIEM+SOAR** with **24/7 coverage**, the family office demonstrates that it is **proactively detecting and responding to threats**, significantly reducing potential business impact while fulfilling its **fiduciary duty** to protect its principal's and family's assets.

As one best practice guideline notes, maintaining **offline log backups** and a **trained incident response capability** is essential for identifying and neutralizing threats **before they cause damage**.

In short, **SIEM and SOAR** serve as the family office's equivalent of **radar and automated defense systems** in cybersecurity — just as a high-end physical estate would have sophisticated **surveillance** and **countermeasures**. This investment can mean the difference between **rapidly stopping an intrusion attempt** versus being **silently infiltrated for months**, which could result in **major financial losses** or **sensitive data exposure**.

CYBERSECURITY

Physical Layer Security

Physical Layer Security

Cybersecurity doesn't stop at the keyboard; the physical security of IT assets and sensitive information is equally important. A sophisticated attacker may attempt to gain physical access to plant bugs or steal devices, and insider threats might try to exfiltrate data via printed papers or USB drivers.

Therefore, a **comprehensive physical security program** must complement digital security, creating an environment where systems are tamperproof and information is protected from physical spying or theft.

Secure Office Premises

Treat the family office location like a mini-bank or vault. Implement **Access Controls** to enter the office, this could include **badge entry systems, biometric readers (fingerprint or face scan)** for especially sensitive areas, and a **sign-in process for visitors**. Maintain **a need-to-be-there** rule.

Only authorized staff and vetted visitors can enter areas where sensitive work is done. Security guards or a receptionist should verify identities of anyone coming in. **Surveillance Cameras** should cover all entry points, server rooms, and areas where sensitive work is done **(with due consideration for privacy of employees, focus cameras on doors and high-security zones).**

Ensure camera feeds are recorded and stored securely (encrypted storage) for a reasonable period as evidence in case of an incident. Intrusion alarm systems should be in place for off-hours, with motion detectors, glass-break sensors, etc. So any unauthorized entry triggers an immediate alert to security personnel.

The office **should ideally be in a secure building with 24/7 security,** and if possible, in an unmarked or discreet location to avoid drawing attention.

Server and Network Hardware Security

If the family office has any on-premises servers (for file storage, backups, etc.), keep them in a **locked server cabinet or room.** Limit who holds the keys, probably just the IT manager or a very small number of execs. The server room should have **environmental controls (cooling, fire suppression)** and should also be in locked racks to prevent someone from unplugging or plugging in rogue devices.

For ultra-sensitive setups, consider **tamper-evident seals** on server cases or ports, so you can tell if someone has opened a chassis or inserted a device. Use **BIOS/UEFI** passwords and disable USB boot on critical machines to prevent unauthorized booting from external media. On workstations, use cable locks to secure them to desks (to deter quick theft).

Protection of Documents and Media

Despite going digital, there will be some physical documents (**contracts, passports, etc.**) and removable media (**USB drives, backup disks**). Maintain **secure cabinets/safes** for storing any highly confidential documents. Ideally **a fireproof safe for irreplaceable documents.**

Enforce a **clean desk policy,** where employees shouldn't leave sensitive papers out, they must be locked away when not in use.

Provide **cross-cut shredders** for paper disposal or use a **bonded shredding service** for large disposals (witness the shredding if it's that sensitive).

For digital media, **use encrypted USB drivers** (hardware-encrypted drivers that require a PIN or have auto-encryption).

Have a procedure for **media destruction,** old drives and USBs should be securely erased (with DoD-grade wipe or degaussing) or physically destroyed (crushed or shredded) when retired.

Workstation and Device Controls

Ensure all computers auto-lock after a short inactivity (**and require password/MFA to unlock**), this prevents someone from sneaking onto an unlocked PC.

USB port control: if possible, use software that disables unauthorized USB devices (to stop someone plugging in a rogue device or copying files to a flash drive).

Provide employees with only the USB devices they need (e.g. an official encrypted flash drive) and discourage random use of others.

For mobile devices, ensure **remote wipe** is enabled (via **MDM**) so if a phone or laptop is **lost/stolen,** you can erase it immediately.

When travelling, use privacy screen filters on laptops to prevent shoulder surfing of information.

Preventing Physical Intrusions and Insider Threats

Regularly brief staff on recognizing **social engineering in person**,

e.g. an unknown technician showing up claiming to fix something should be verified.

Keep networking closets locked and **consider an alarm on them as well** (so it logs when opened). For executive residences **(as family offices often extend security there)**, ensure home offices have similar protections.

A locked study, perhaps a small safe for devices, and certainly home Wi-Fi network security **(segmented and encrypted, which overlaps with cyber).** Also consider **TEMPEST** measures (electromagnetic shielding) if discussing extremely sensitive topics.

In high security government, they **shield rooms** to prevent eavesdropping via electronic emissions. For the highest security conversations, **a faraday-cage** style conference room could be considered, though that’s an extreme step typically.

Tooling Recommendations

Physical security tools include: **Electronic Access Control Systems** (HID card readers, biometric pads, etc.), **IP Cameras** with **NVRs** (Network Video Records) that support encryption so camera feeds aren't hackable.

Alarm systems that integrate with a security company for armed response. **Safe Cabinets** rated for document protection (some are even IoT-enabled to log openings). For PCs,

Endpoint Management Software that can disable ports or screen lock.

There are also **Physical Security Information Management (PSIM)** systems that integrate alarms, badge entries, and camera, for a small office **this might be overkill, but at least ensure someone is responsible for reviewing camera footage and alarm reports.**

Executive Decision Points

Security vs **privacy** vs **cost** is a balance here. Leadership must decide how far to go e.g. **do you want cameras inside the office space (which could be seen as intrusive by staff,** or perhaps limit them to entry points and server areas to balance privacy. Decide on **guard presence,** as some family offices hire **ex-military** or **police** for physical protection, which can also deter physical intrusion attempts.

If the office is in a shared building, decide if you need additional private security on your floor or not.

Another decision would be **policy enforcement, e.g.** if an employee tailgates a visitor without following sign-in, what's the consequence? Executives should make it clear that physical security rules are **just as important as cyber rules.** Leading by example is key, principals and executives should also follow badge rules, not prop doors open, etc., to set the tone.

Consider periodic physical security audits, perhaps an annual review by a **security consultant** who will, for instance, attempt to **covert entry** to test your measures, or at least evaluate weakness (such as server room lock is easy to pick, replace it with a better one).

Regulatory Mapping

Physical security of personal data is explicitly required by **PDPL** and other laws, PDPL's definition of protecting data extends to **physical records and printouts.** For instance, if someone walked out with a file with personal **data, that's as much a breach as a hack.**

Showing you have **a clean desk policy, lockage storage, and shredding procedures demonstrates compliance.**

Note: In the Baker McKenzie Handbook on KSA, physical security measures are noted as part of best practices.

SAMA's framework also covers physical security of IT assets as one of it's domains, ensuring that member organizations control physical access to systems. While not directly binding, if the family office data or operations were ever reviewed (say in an audit for a banking partnership), having those controls align with SAMA's expectations.

If you host data in a data center in Saudi Arabia, **CITC/CST regulations** require the facility to have strong physical security — such as biometric access controls, CCTV monitoring, and more. If you are using co-located servers (servers hosted at a provider's facility), make sure the provider meets these requirements (most data centers in KSA already do).

Additionally, if the office handles any government-related data, NCA (National Cybersecurity Authority) controls will apply, requiring an even higher level of physical security.

In essence, robust physical security **prevents old-fashioned breaches,** as the adage goes, *why hack in when you can walk in?* We eliminate that possibility and threat vector.

It also underpins cyber measures, fancy encryption means nothing if an attacker can steal a logged-in laptop off a desk.

By **fortifying the physical layer,** we create an all-round tamper-proof environment consistent with the military-grade security promise.

CYBERSECURITY

Data Sovereignty, Compliance, and Storage

Data Sovereignty, Compliance, and Storage

Operating in Saudi Arabia while managing global dealings, the family office must navigate a complex landscape of **data sovereignty** and **compliance** requirements. This means ensuring that **sensitive data**. Especially **personal data** is stored in **approved locations**, that **cross-border data transfers** are conducted lawfully, and that **records** are maintained to satisfy regulatory bodies such as **SAMA**, **SDAIA** (for **PDPL**), **ZATCA**, and applicable **foreign laws** such as **GDPR**. In short, the office's **data management practices** must be both **highly secure** and fully **compliant**.

Data Residency and Sovereignty

Saudi Arabia's PDPL and related regulations heavily emphasize keeping personal data within the Kingdom unless certain conditions are met. The family office should **architect its storage such that primary personal data repositories are located on servers / datacenters in Saudi Arabia.**

If using cloud services, opt for those with **Saudi data centers or the ability to specify region** (many major clouds such as **Oracle** and **Google** have active regions in **KSA,** and **Azure/AWS** have regions in neighboring countries and plan local zones, ensure any used cloud app that will host personal data is configured to KSA **or at least Middle East region** in absence of KSA region, and confirm with legal if Middle East region is acceptable or if an exemption is needed).

For any data that must reside outside (perhaps a global service with no local option), the **PDPL** requires either **SDAIA approval** or that the destination country has equivalent data protection and it serves the Kingdom's interest, likely you'd seek explicit consent from the data subjects (e.g. principal or family members) for such transfer and document that decision.

Mapping Data to Regulations

Create a **data inventory and classification** mapping, for each type of data the office handles, for instance:

- Personal IDs and employee data (PDPL applies)
- Financial account data (which might be under SAMA's purview if a bank is involved),
- Tax and invoice records (ZATCA),
- Client investment data (possibly CRS for international tax sharing), etc.

Mark which laws apply, this will inform retention and storage. For instance, **ZATCA e-invoicing** rules would mandate that electronic invoices be stored in Saudi Arabia for a minimum period (**typically 6 years**) in a tamper resistant format. Therefore, if the family office issues any invoices or receives them, ensure your accounting software or archive meets these.

Store those invoice files on a Saudi Arabian server, perhaps with an immutable file system or digital signatures to detect tampering.

Retention and Backup Compliance

Compliance often dictates how long data must be kept. Under **PDPL**, personal data should not be retained longer than needed for it's purpose, unless otherwise required by law. But other laws (Tax, Commercial) might require longer retention.

For the family office, set retention policies e.g. keep transaction records 10 years (common for financial records), keep personal employee data only as long as the employed + X years (due to compliance), etc.

Use backup systems that align with this.

For instance, don't keep personal data indefinitely in backups either. Implement a schedule to delete or archive data that is no longer needed to stay compliant with PDPL's minimization principle.

Conversely, ensure data needed for **regulatory reasons (such as VAT records, audit trails of transfers) are not permanently deleted,** have an archive solution for these.

Cross-Border Data Transfers

Inevitably, some data will cross borders (perhaps a legal team in London receives documents, or the principal in the US accesses files). Under **PDPL**, cross-border transfer is restricted.

If it **must happen,** comply by obtaining the data subject's consent (easy in this case since it's the principal's data mostly), and ensure the receiving party will also protect the data. For regular transfers, **draft a Data Transfer Agreement** referencing **PDPL** requirements with foreign entities (similar to **GDPR's Standard Contractual Clauses Concept**).

If the office shares financial information with foreign banks or advisors, **ensure those communications are secure (as we've covered) and that any stored data in those jurisdictions is minimal and protected.**

For CRS, when transmitting account information to tax authorities (e.g. sending to local tax authority under CRS for other nationals), use secure channels (encrypted emails or the official government portals which are typically secure by design).

Document these transfers for audit, including what data was sent, when, and under what authorization.

Compliance Management

It's recommended to maintain a **compliance calendar and checklist** for the various obligations, **PDPL** (annual compliance audit perhaps, DPIA for new projects), SAMA if any reporting is needed, though likely not useless part of regulated activity), **CITC/CST** (if using local cloud providers, they might be certified under **CST** cloud frameworks, so get their compliance letters).

ZATCA (annual or periodic audit of e-invoicing system), etc. The family office may consider appointing a **Data Protection Officer (DPO)** or at least an internal privacy champion to ensure **PDPL** compliance since now (as of 2024) PDPL is in full effect. This person ensures policies are followed and handles any data subject access requests (for employees or others) per PDPL.

Tooling Recommendations

Use a **Governance, Risk, and Compliance** (**GRC**) **tool** or even simple project management to track compliance tasks (for large organizations, use tools such as **MetricStream or RSA Archer** are used. For smaller scale, a well-structured **SharePoint** or **Excel** tracker could do).

Therefore, deploy a **data loss prevention (DLP) tool** to ensure data doesn't leave to unauthorized places, for instance, a **DLP system can block someone emailing a document to an external address or uploading it to an unapproved cloud server, therefore enforcing the data residency policy.**

Many cloud storage providers also allow **geofencing**, therefore configure such that (for example) **Microsoft 365 data** is only accessible from certain countries of certain IP ranges.

Keep an eye on **Saudi's Evolving Regulations, SDAIA** may publish a list of approved countries for data transfers, therefore adjust practices accordingly. **National Cybersecurity Authority (NCA) Essential Controls (ECC-2 2024)** remove some strict localization but clarified guidelines. Meaning government entities have slightly more flexibility now, but for private data, PDPL is the main rule.

Executive Decisions

The board or principal should approve a **formal data governance policy** which states where the data will be stored and under what conditions it can be transferred out of the country. This gives clear top-down direction (and is something regulators would like to see).

*For instance, All personal data and critical financial data will be stored on servers located in Saudi Arabia. Exceptions require legal approval and data owner consent. Another direction is whether to pursue **any certifications** as a way to demonstrate compliance, e.g. going for ISO 27001 certification or an ISAE 3402 audit for the family office's processes.*

While not required, it can force discipline and reassure counterparties of your adherence to best practices.

Also, discuss with legal counsel how to handle any foreign legal requests for data, if, say, a US court subpoenas some data, how will you respond while respecting **PDPL?** These are strategic calls, possibly keeping data local until absolutely needed gives you more control.

Regulatory Mapping

This section is itself about regulation mapping. Let's recap the specific ones:

PDPL (Personal Data Protection Law)

Fully effective as of **2023**, and requires local storage unless stringent conditions are met. It also requires controllers to implement measures such as (**encryption, access control**) which we've covered, and not to keep data beyond necessity.

Non-compliance can lead to fines up to 5 million SAR or more, and even criminal liability for certain violations.

So, the family office must treat **PDPL compliance seriously** even if it primarily handles the principal's data (which it does cover, by the way, personal data of even one individual is under PDPL, though risk of complaints is low if it's mostly family.

SAMA

If the family office for instance manages a family investment fund that falls under CMA or SAMA oversight then there could be specific data requirements (such as maintaining records for X years, reporting any cybersecurity incidents to regulators within 24 – 72 hours, etc.). We already apply SAMA Cybersecurity Framework controls voluntarily, which does cover much of the security compliance.

CITC/CST

The **CST's Cloud Computing Regulatory Framework** (**4th version, 2023**) sets requirements for **cloud providers** regarding **customer data location** and **breach handling**. As a **cloud customer**, you should ensure that any provider you use is **compliant with this framework** and request their **adherence statement**. Additionally, if you are hosting a service that could potentially be classified as providing a **digital service** (unlikely in this case for an internal family office), note that **CITC** may require certain **licenses**—though this is generally not applicable to purely internal office operations.

ZATCA

Electronic records related to tax (invoices, zakat filings, etc.) must be stored in Saudi Arabia and safeguarded. ZATCA can audit at any time, so maintain those and be able to retrieve them in human-readable format.

GDPR

If the family office stores any EU personal data (i.e. the family has EU household staff or properties with personal data about the tenants, etc.), GDPR would require not transferring that out of the EU without basis.

Luckily Saudi Arabia now has a comprehensive Law (PDPL), but it's new so the EU hasn't adequacy approved it, so you'd rely likely on consent or contractual necessity for any EU data moved to Saudi Arabia.

By building data storage and management alignment to these rules, the family office not only avoids legal penalties but also gains trust of banks and partners (who might ask, are you PDPL compliant? How do you handle data?).

The answer will be, ***we have a rigorous policy about keeping data local and encrypted, in line with all applicable regulations, reassuring stance that's part of a military grade posture.***

CYBERSECURITY

Secure Mobile & Remote Work

Secure Mobile & Remote Work

A modern family office isn't confined to a single location. Staff may work remotely, travel with the principal, or access resources from home or abroad. Likewise, the principal and family members themselves are constantly on the move. This mobility introduces risk, as devices outside the protected office environment are more susceptible to loss, theft or compromise by unsecure networks.

Therefore, a secure mobile & remote work strategy would ensure that whether someone is working from a yacht, a private jet, a hotel, or home, the security controls remain as stringent as on-premises.

Device Hardening and Management

All mobile devices (**laptops, tablets, smartphones**) used for family office business should be **corporate-managed and hardened.** This would include:

Full Device Encryption

Laptops must use Full Disk Encryption (e.g. **Bitlocker** or **FileVault**) so that if lost or stolen, the data would remain **safe.** Phones and tablets should be encrypted (most modern IOS/Android do this by default when a PIN/password Is set).

Use **strong passwords or PIN codes**, not just **fingerprint or face unlock**, because in some situations — like going through **border checks** — you can be forced to use your fingerprint, but not your password. Before traveling, it's a good idea to **turn off fingerprint and face unlock** and use a strong **PIN** instead.

Mobile Device Management (MDM)

Deploy an **MDM solution** (e.g. **Microsoft Intune, VMware Workspace One, or MobileIron**) to enforce security policies on all devices. Through MDM, require screen lock, control app installations (block risky apps), push VPN configurations, and have the ability to **wipe** a device that is lost or stolen.

MDM can also geo-locate devices if needed during an emergency (with user consent considerations). If staff use their personal devices at times (BYOD), use **MDM** to containerize work data on those devices or provide them with separate work devices to avoid mixing personal and work data.

Endpoint Protection

Ensure every laptop has **advanced endpoint protection** (next-gen antivirus/EDR) that can work offline and online. It should be centrally monitored (Feeding logs to SIEM). Also enable host-based firewalls on laptops with strict rules (when on public networks, limit inbound connections, etc.).

Mobile devices can have threat defense apps that detect malware or suspicious behavior (like **lookout mobile security, or Microsoft Defender** for Mobile).

Secure Connectivity (VPN / Zero Trust Access)

When accessing internal resources remotely, use a **secure VPN or Zero Trust Network Access (ZTNA)** solution. A traditional VPN with **(AES-256 encryption, certificate-based authentication)** can tunnel remote traffic through the office or a cloud security stack, protecting it from local network threats.

However, VPN should not open full network access broadly, it should be **split-tunnel** or software-defined so that the user only reaches what they need. Better, consider a **ZTNA service.**

For instance, set up a cloud-based secure access broker where remote logins are authenticated (with MFA) and then connected to specific applications (similar to how Google's BeyondCorp works).

This ties back to the Zero Trust model and reduces reliance on device location.

Also, for web-based services, use **secure web gateways** or CASB (Cloud Access Security Broker) to ensure even from remote, internet access is filtered for malware and sensitive data isn't uploaded to unauthorized cloud apps.

Safe Remote Work Practices

Use of Trusted Networks

Instruct that wherever possible, use either the company-provided mobile hotspot or VPN over a known cellular network rather than using public Wi-Fi. If public Wi-Fi must be used (say for instance, at an airport), **VPN is mandatory**. A nice investment is providing employees with a **travel Wi-Fi device** that has a pre-configured **VPN** and perhaps an embedded firewall.

*For instance, something like a **portable router (Skyroam or a Cradlepoint Travel Router)*** where the SIM data goes through your VPN automatically, this way the user just connects to their private hotspot.

Burner or Travel Devices

For travel to high-risk areas (some countries known for aggressive cyber surveillance), issue clean **burner laptops** and **phones** with minimal data on them. These devices should have only the necessary info, connect via VPN to get what they need, and be wiped after returning.

The AP News tip and the FBI recommendations to Olympians illustrate this approach. If the ***principal or staff are attending, say, a conference in a country with active Cyber Espionage, consider temporary email accounts or communication devices for that trip, then decommission those accounts.***

Remote Workspaces

If working from home, provide **secure setups** for staff. This can include a **locked file cabinet** for any printed documents, a **privacy screen** for their laptop, and even a **dedicated home router or firewall** pre-configured by the office IT team. For example, you could provide a **firewall appliance** that creates an **always-on VPN connection** back to the office.

Also, ensure their **home Wi-Fi** uses **strong WPA3 encryption** and a **unique password** (and assist executives with setup if needed). Where possible, **segment the home network**—put **work devices** on one Wi-Fi network (SSID) and **IoT devices** (smart TVs, cameras, etc.) on a separate one, to reduce risk.

User Awareness

Remote workers should be vigilant, remind them of things such as **not leaving devices unattended** (**use cable locks for laptops even in hotel rooms**), beware of **shoulder surfers** or people eavesdropping in public (don't have sensitive calls in a crowded space), and don't plug devices into unknown chargers or computers (juice jacking is a risk, therefore provide them with USB data blocker devices for charging or have them carry their own battery packs).

You should have an easy way for them to report lost devices or incidents while being remote (i.e. an emergency number or point of contact they can call 24/7 if, say, a phone Is missing or they clicked a suspicious link).

Tooling Recommendations

Collaboration Tools

Use secure collaboration suites that are cloud-based but are also protected (e.g. Office 365 with conditional access). Leverage their features for remote wipe (Intune can wipe O365 data from a lost phone).

Virtual Desktop Infrastructure (VDI)

For **highly sensitive access**, consider using a setup where **no data is stored on the user's device**. Instead, provide a **virtual desktop** (such as **Citrix** or **Azure Virtual Desktop**) that users log into remotely. In this model, all **processing and data** stay securely in the **cloud**, and only the **screen image** is sent to the user's device.

This way, even if the device is compromised, the data remains safe inside the virtual environment. You can use this approach selectively — for example, if a staff member is using a **personal computer**, have them work through **VDI (Virtual Desktop Infrastructure)** rather than downloading sensitive files to their local device.

Geo-fencing & Mult-factor

Configure conditional access such that if a login occurs from an unusual country or location, additional verification is required or access would be limited. Many IAM systems can enforce policy like **if user is not on corporate IP or device, allow email access only via web and block downloads, etc.**

Executive Decision Points

There is often pushback on locking down personal devices for travel convenience. Leadership must decide to what extent they enforce using corporate devices only and following these protocols. The principal and key executives should also abide.

*If the policy is to use the **secure phone or VPN abroad, the principal should do so too** (leaders not following would encourage staff to slack off too).*

From a **budget standpoint**, decide whether it makes sense to provide **key staff** with an **extra travel laptop or phone** (for key personnel, this is likely a good investment given the sensitive assets involved).

Also, plan ahead for how to handle **incidents during travel**:

- If a **laptop is stolen** overseas, do we have a **spare device ready to ship**?
- How quickly can a replacement be **configured and sent**?

While **equipment insurance** is helpful, it's even more important to ensure that **all data on remote devices is backed up** (such as through **cloud syncing**) so that if a device is lost or stolen, **no data is permanently lost**.

Regulatory Mapping

Facilitating remote work securely helps compliance **indirectly**. **PDPL** doesn't forbid remote work, but it mandates protecting data wherever it is, by using **encryption, VPN, and access control remotely,** you extend those protections to wherever personal data might be accessed, fulfilling PDPL's requirements to prevent unauthorized access or leakage.

If remote connections were insecure and a breach happened, that would be a failure in required safeguards. **SAMA's** guidance during pandemic times stressed secure remote access, aligning with that, the office should meet similar standards a bank did when shifting to remote work (like **MFA or VPN**, no sensitive data on home printers, etc.)

CITC has guidelines for teleworking security (the National Cybersecurity Authority also issued some telework cybersecurity guidelines in 2020), where it's generally advising VPN, updated software, etc.

The office's measures are described would satisfy those. If any work involves EU data, **GDPR expects that personal data accessed from home or abroad is equally protected**, if an employee saved EU client data to an unsecured home computer and it got hacked, that's a GDPR violation.

Therefore, our approach of using MDM, encryption, and possibly not storing data locally avoids that.

The Bottom Line

Secure mobile and remote practices *enable the family office to operate* ***globally and flexibly*** *without lowering its* ***security standards****.* ***Information security*** *must remain* ***"always on"****, aligning with the* ***principal's constantly on-the-go lifestyle****, while ensuring that* ***threats are blocked****—regardless of where or how they emerge.*

CYBERSECURITY

Executive Protection Protocols

Executive Protection Protocols

UHNWI principals are high-value targets not only in the cyber realm but also in social engineering and impersonation attacks. The rise of **deepfake technology,** AI voice cloning, and classic con tactics would mean the family office must implement rigorous **Executive Protection Protocols** to ensure that instructions or communications purportedly from the principal (or other VIPs) are genuine, and to protect the principal's own digital identity and safety.

Impersonation Defense (Verify Identity)

Adopt a strict **verification protocol for any unusual or financial request** that appears to come from an executive. No matter if it's a voice call, an email, or even an in-person request relayed by someone, establish a habit of verifying via a second factor.

For instance, if the CEO gets a call from someone sounding like the principal urgently instructing a fund transfer, the CEO should **politely** say they will call back via the principal's known number or verify via the secure messenger. The office should have an internal **code word or challenge-response** system between staff and principal for urgent commands.

For instance, the principal and key staff agree on a secret code phrase ("green tiger" or any random string) that would naturally come up in a verification question. If a requester can't produce it correctly, the instruction is assumed fraudulent. This simple "Safe Word' system can thwart the most convincing deepfake voice because the fraudster likely won't know the correct response.

Likewise for emails, any email from the principal asking for something sensitive should be confirmed via a pre-established method (e.g. **a quick signal message**: did you just send an email about X?).

Better yet, ask the principal to use only the secure office email or messaging for official requests, if you get a request from their personal Gmail or a random SMS, always **double-check.** This might **slow things down slightly**; however, it would provide near-immunity against impersonation scams which are among top threats for UHNWIs.

Secure Executive Communications

Provide the principal with **dedicated secure communication devices,** and train them to use them for anything sensitive. If the principal normally calls in for approvals, **ensure those calls use the secure phone app, making interception or impersonation harder.**

Also train them to be **cautious** of what they say on open lines, even casual information can be misused by adversaries to social engineer (e.g. mentioning a child's name or a pet, which often are answers to security questions).

Implement **voice authentication measures,** if possible, as some institutions use voice biometrics to authenticate callers. The family office **could** record the principal's voice pattern (with consent) and use a service that alerts if a voice doesn't match exactly. However, even **deepfakes can potentially dupe voice biometrics, so don't rely on that, use it as a supplement check.**

Personal Digital Hygiene

The principal's personal digital footprint should be tightly managed. Ensure their **social media privacy settings** are locked down (or consider having no social media presence or a very controlled one).

Adversaries often scrap information from sources such as:

- **LinkedIn**
- **Facebook**
- **Instagram**
- **Etc**

To craft personalized scams. Therefore, limit what **personal information (birthdays, addresses, frequent locations)** is publicly available. Possibly employ a **privacy service** to regularly scan for and remove the principal's personal information from data broker sites and the internet.

Executive Cyber Training

Provide one-on-one security briefings to the principal and their immediate family. Cover common tricks:

- **Phishing emails that look like from their bank**
- **Fake texts that appear to come from their assistant**
- **Deepfake scenarios, etc.**

Perhaps simulate a harmless attack to show how convincing it can be, then demonstrate the proper response **(verification steps).**

High-profile individuals may not want lengthy training, **but real anecdotes (like how a deepfake CEO voice conned a company out of €220k can drive the point home.**

Insider Threat Precautions

Sometimes, impersonation can come from within the office, an unhappy staff member who might pretend to be the principal to others. Maintain a culture of **clear, direct communication channels.**

For instance, if the principal has an instruction, it comes in a known format and way (written and signed, or from their verified email).

If a different employee claims **the boss said to do X, there should be a policy to verify that. Therefore, encourage a trust-based-verify norm with no offense taken for double-checking.**

Emergency Protocols

Develop a protocol in case the principal's accounts or devices are suspected to be **compromised**. For instance, if the principal loses a phone, the staff should know to immediately revoke that device's access (**remember remote wipe via MDM**) and assume any messages from it could be fake.

Or if a deepfake video or audio of the principal appears online making some claim, have a plan for public/media response and technical analysis (there are firms that do **deepfake forensics** to confirm it's fake).

In terms of immediate steps, have an **alternate secure channel to reach the principal that only they control, this could be a secondary phone or a known personal contact, so if one identity is hijacked, you can still verify through another.**

Tooling Recommendations

Use Identity Verification Tools

Pindrop or similar audio analysis for calls can sometimes detect synthetic audio (by examining audio artifacts). Not foolproof but something to consider for calls into the office.

There are services such as **BlackCloack, Q6 Cyber, etc that specialize in digital executive protection,** they monitor the dark web for chatter about the principal, look for leaked personal information or accounts, and provide personal device security for the executive. **Engaging one of those might add a layer of intel to tacth target attacks in planning stage.**

Email Tagging

Ensure any email coming from outside (even if name looks like the principal) is clearly marked as external. Implement DMARC, DKIM on domains to prevent spoofing.

*i.e. Nobody should be able to send an email that looks like **boss@familyoffice.com** if it's not actually from your mail server.*

Personal VPN and Anti-tracking

For the principal's own internet use, have them use a trusted VPN service and anti-tracking browser configurations to minimize exposure of their IP or location **(harder for hackers to target them specifically if their internet traffic is obscured).**

Executive Decision Points

The principal's buy-in is the most critical. They need to understand that these protocols protect them, not to become an inconvenience for them unnecessarily. It's important to have a frank discussion, **we will sometimes double-check instructions that appear to come from you.**

This isn't lack of trust, it's to **ensure no one can pretend to be you to cause harm**. Ideally, the principal actively participates, perhaps even suggesting a personal safe word they'll remember. They should also decide who their **inner circle** is that can verify things. Maybe their spouse or chief of staff can validate an urgent instruction if the principal is unreachable (like a second factor human).

Consider in the case of controlling the narrative for anyone who decides to hack into emails, etc of using **cover names or project names for sensitive projects internally, i.e. acquisitions of valuables, etc.** so even if someone overhears of hacks an email, they can't immediately know what it refers to.

Regulatory Mapping

While there is no specific law addressing **deepfakes** yet, **fraud prevention** is an expected standard in **financial operations**. For example, **SAMA** requires banks to implement controls against **executive impersonation fraud** — a threat that has already impacted the banking sector. By adopting similar **verification protocols**, the family office aligns itself with industry **best practices in fraud prevention**.

In addition, under **PDPL**, any mistaken **fund transfer** or **data disclosure** caused by impersonation could be classified as an **unauthorized access incident** — meaning that preventing such events is part of the office's responsibility to protect **personal data**.

Internationally, regulators such as **MAS** (Singapore) and **FCA** (UK) have issued guidelines addressing the unique **fraud risks** faced by **high-net-worth clients**. The protocols adopted here reflect the spirit of those global standards.

Finally, these measures are fully consistent with **CISA** and **FBI** warnings to executives regarding the rising threat of **deepfake scams**. By proactively implementing **verification steps** and **secure communication channels**, the family office positions itself as a **resilient defender** against one of the most advanced forms of emerging fraud — the use of **cyber and social deception** to exploit trust.

This ensures that the **principal's instructions** can never be hijacked or mimicked without detection, thereby preserving the integrity of **executive decision-making**.

CYBERSECURITY

Secure Onboarding of Luxury Assets

Secure Onboarding of Luxury Assets

This family office's portfolio spans **luxury assets like:**

- **Private jets**
- **Yachts**
- **Real Estates**
- **Cars**
- **Possibly Collectors**
- **Etc**

Each of these modern assets comes with **digital components** and connections that could possibly pose potential cybersecurity risks. Therefore, **onboarding** a new asset would mean not only adding it to the financial inventory but also integrating it securely into the office's operational and IT ecosystem. We must treat a new Gulfstream jet or a 100m superyacht almost like adding a new branch office or network to protect.

Cybersecurity Due Diligence

Before and during the purchase of a high-tech asset, do conduct a **cybersecurity assessment of the asset itself. For instance,** when acquiring a used yacht, investigate it's onboard networks, as yachts often have **Wi-Fi for guests, satellite internet, navigation systems, engine control systems, IoT devices (like smart TVs, CCTV, climate control).**

Assess how segregated those systems are (Navigation should be isolated from the guest Wi-Fi). Check if default passwords for onboard equipment have been changed, if the latest firmware updates for the ship's systems are applied, etc. It's wise to hire a specialist maritime cybersecurity firm to do a vulnerability assessment on the yacht's **IT/OT networks.**

Similarly for a private jet, while aviation systems are highly regulated, ensure any **in-flight connectivity (Wi-Fi)** is separate from avionics, and that any provided devices or cockpit iPads are secured. Ask the manufacturer or seller about known cyber issues (for instance, some modern aircrafts have cybersecurity service bulletins to patch Wi-Fi vulnerabilities).

For real estates and properties, perform a **penetration test on the home network** and IoT (**security cameras, smart locks, HVAC**) as part of the takeover. Many luxury homes have automation systems (Creston, KNX, etc.) get an **integrator** to review and secure those, change default credentials, apply encryption where possible, and segment them from the office VPN that might be present there.

Integration into the Network (Segmentation & Access)

When an **asset** is in operation under our control, it should be fully integrated into a **secure management framework**:

- Each asset (such as a **yacht** or **private jet**) should operate on its own **secure network segment**, connected back to the **family office**.
- For example, equip the yacht with a dedicated **firewall** and **VPN appliance** that connects securely to the family office network or to a secure cloud environment — creating an **encrypted tunnel** for all **office-related data** (such as financial syncs, camera feeds, or monitoring data).
- Ensure that the **guest internet** onboard the yacht is kept **completely separate** (ideally also **filtered**) so that any compromised guest device cannot access the yacht's **control systems** or its **secure office link**.
- Apply the same principles to **private jets** — sensitive traffic should always run through a **VPN**, and **crew devices** should be separated from **passenger devices** via **separate VLANs**.

Access to **asset systems** must also be strictly controlled:

- Define and manage **who can log into** critical systems such as the **yacht's monitoring systems** or an estate's **CCTV**.
- Where possible, integrate this with a **central IAM (Identity & Access Management)** system; at minimum, enforce **strong passwords** and **2FA**.
- Maintain an up-to-date **inventory of all third-party/vendor access** to these assets (such as yacht IT support, or estate smart home support), and apply **third-party risk controls** accordingly.

Ongoing Asset Cyber Maintenance

Include the assets in regular security routines. Just like the yacht gets regular mechanical maintenance, schedule **cyber maintenance,** apply patches to onboard Windows PCs, update the navigation software from the manufacturer (They often release updates to address bugs and cyber issues as IMO regulations now require cyber risk management onboard).

Ensure the yacht's satcom system credentials are changed from **default,** back in 2018, some researches showed they could hack into satellite comms because of default credentials. For real estate, update home device firmware (such as cameras or smart appliances) since old vulnerabilities could let a hacker spy or pivot into networks.

Also implement **monitoring on assets** e.g. put a network monitoring device on the yacht that sends logs back to the SIEM (so you can see if there's unusual traffic from the yacht's network).

The same for a smart home, perhaps have a dedicated appliance that monitors IoT for anomalies (some solutions exist that profile IoT devices and alert if they behave oddly).

Secure Asset Documentation and Onboarding Procedures

Each asset will come with **sensitive documents, deeds, titles, registration, maybe historical provenance (for collectibles).** Treat these like other sensitive documents, store them in the encrypted document vault with limited access.

If the asset involves staff (crew on a yacht, pilots of a jet, estate household staff), onboard those personnel with background checks and have them sign **confidentiality and cybersecurity agreements**. Train them too, a yacht captain should know basic cyber hygiene (e.g. don't plug unknown USBs into the navigation computer, beware of phishing emails on the yacht's computer, etc.)

Tooling Recommendations

For maritime and aviation, there are specialized systems such as **Paolo Alto's Maritime Cybersecurity Solution** or services by companies such as **Moran Cyber or DNV** that provide cybersecurity for yachts, use them for periodic audits.

Install a **Unified Threat Management (UTM)** device on yachts and real estates (such as Fortinet or CISCO Meraki Appliance) which do firewall, IDS/IPS and content filtering. These often support satellite links and can be remotely managed.

Real Estate

Consider **Professional Smart Home Security** systems e.g. Crestron has **Cybersecurity Guidelines,** implement network isolation for security cameras (potentially have them record to a local NVR that's encrypted and accessible remotely only via VPN). Also consider physical Faraday pouches for key fobs of luxury cars (this is to prevent relay theft hacks).

Maintain an asset register with Cyber-related information e.g. List of IP-enabled devices on the asset, software versions, last patch date, responsible IT or vendor contact for each. This would help ensure nothing falls through the cracks.

Executive Decision Points

When acquiring a luxury asset, factor in the **Cybersecurity aspects from day one,** this may affect cost and timing. Executives should approve a **cyber review as part of purchase due diligence** (just like legal or structural inspections). That might mean delaying a yacht's integration until it's networks are refitted securely.

Leadership must back this, understanding the risk of rushing it (a vulnerable yacht could be a gateway to hack personal communications or worse, cause safety issues). **Therefore, budget accordingly, e.g. allocate funds in the yacht's operating budget for IT security upgrades.**

Decide on the trade-offs for convenience, as some owners want to use devices on their jet just like at home. We can enable that but with security, with the possibility of adding some restrictions such as (no unknown USB sticks, or certain websites blocked). Get the principal's buy-in that If, say, their new car comes with a fancy internet-connected infotainment, the office will secure it (potentially update it, or disable features that phone home with data).

Explain in executive terms (where any device with connectivity can be a spy or entry-point and our job Is to minimize that threat vector.

Safety Overlap

Especially for planes and yachts, cyber incidents can threaten physical safety (navigation hacks, engine interference). Emphasize to the principal that by securing these, you're also protecting lives.

For instance, prevent a scenario like the well-known experiment where researchers **hijacked a yacht's navigation via GPS spoofing or where hackers took over a yacht's digital systems.** Those were wake-up calls that have since led IMO and aviation authorities to push Cybersecurity; therefore the family office should **exceed those minimums to achieve truly military-grade safety.**

Regulatory Mapping

In transportation, there are emerging regulations, **IMO (International Maritime Organization)** guidelines **MSC.428(98)** require cyber risks to be addressed in safety management by 2021 for vessels, so any commercially registered yacht above a certain size will need a cyber section in it's management plan. The office should ensure compliance with those maritime rules (it will cover basics such as network protections, access control, backup navigation data).

Aviation has its own standards (**FAA and EASA** have issued cyber rules for aircraft manufacturers, operators should follow **cybersecurity best practices**, though private jets aren't as regulated as commercial airlines). Adhering to manufacturer security notices and using certified equipment is important to meet any insurance requirements.

On the data side, an asset like a property with CCTV may collect personal data (images of people), therefore PDPL would consider that personal data, so secure storage and limited use of CCTV footage is necessary (and perhaps posting privacy notice if that's in a place with staff/guests). If the real estate property is in the EU or UK you have GDPR/ICO CCTV guidelines to follow (like not keeping footage longer than necessary, using it only for security).

Using **CITC/CST** if the asset uses telecom (satcom on a yacht) ensures licensed equipment is used per CITC rules and that any local network frequencies are approved. Usually vendors handle that, but it's part of compliance.

CYBERSECURITY

Backups, Disaster Recovery, and Cyber Reliance

Backups, Disaster Recovery, and Cyber Reliance

Even with the best defenses, incidents can happen, whether a ransomware attack, hardware failure, or even a regional outage. The family office must be prepared to **withstand and rapidly recover from disasters, cyber or otherwise.** This would involve robust backups, tested disaster recovery plans, and a general culture of resilience that ensures continuity of operations (especially important when managing time-sensitive financial transactions or overseeing critical assets).

Comprehensive Backup Strategy

Keep 3 copies of important data, stored on **2 different types of media**, with **1 copy off-site** (and preferably offline).

For the **family office**, this translates into:

- The **primary data** resides on **secure servers** — either **on-premises** or in the **cloud**.
- A **secondary backup** is maintained **locally** — on a **NAS** (Network Attached Storage) or a **backup server** in the office — to enable **fast restores**.
- A **tertiary backup** is stored **off-site** — ideally in **secure cloud storage** or a **physically secure location** (such as another office or a **bank vault**). Critically, this off-site backup should be **offline** or **immutable**, so that **ransomware** cannot encrypt or corrupt it.
    - *For example: rotate an **external hard drive** daily and disconnect it after backup, or use **cloud object storage** with **write-once (WORM)** settings. Many modern backup solutions now provide **immutable storage** that prevents **modification** or **deletion** of recent backups.*

You should back up **all critical systems**:

- **File shares**
- The **password manager / vault**
- **Emails**
- **Financial databases**
- And do not overlook “hidden” data — for example:
    - **Network device configurations** (export firewall/router configs so you can **rebuild quickly** after an incident)
    - Any **custom code** or **macros** used in office operations.

Automate backups to run nightly (or more frequently for very critical data transaction logs which **could be hourly).** Ensure backups themselves are **encrypted** so if a backup drive is stolen, the data isn't exposed.

Regular Testing and Drills

A backup is only good if you can restore it. Perform **disaster recovery drills** periodically, where you would simulate a scenario (e.g., the file server got wiped by ransomware) and practice restoring from backups.

Time how long it takes and see if the data is intact up to the expected points. This would help establish **RTOs and RPOs,** which are **Recovery Time Objectives** (How quickly can you be up again) and **Recovery Point Objective** (How much data max you might lose).

For instance, you might decide that in the worst case you can tolerate 1 day of data loss (so daily backups suffice) and potentially 4 hours of downtime. If tests show it takes 2 days to recover a server, that's a gap to address **(potentially by using faster backup technology or active-passive replication).**

Also test **alternative restore scenarios,** for instance

- **What if the office is physically inaccessible?**
- **Could you restore critical data to a cloud server or an alternate site?**

Document the procedures to restore systems, which includes any decryption keys needed for backups (store those keys securely offline as well, potentially with a trusted executive or in a safe).

Ransomware Resilience

In a cyber context, the biggest threat to data integrity is ransomware. Our backup strategy is the key defense, by having offline backups, we ensure we can recover without paying ransoms. Additionally, implement **anti-ransomware measures** the SIEM/SOAR could detect mass encryption behavior and act.

File servers could use snapshotting to quickly rollback if encryption starts. Ensure backup systems themselves are isolated, use separate credentials and network segments so malware that hits the main systems **can't** directly reach backup servers. A best practice is using **different admin accounts** for backup infrastructure, and not keeping those credentials on the domain.

Disaster Recovery Sites / Plans

Identify what resources are critical to continue operations and consider having a **DR site or cloud failover.**

*For instance, if the primary office is down (power outage, fire), can essential functions (such as approving transactions or monitoring assets) be done from elsewhere? Perhaps set up a **small secondary office or the capability to work from home,** as we already have secure remote work solutions, so ensure in a quick amount of time everyone can switch to remote work entirely.*

In tech terms, maybe maintain a **cloud-based replica** of key servers. Where many businesses use cloud backups that can **spin-up** a VM directly from backup in the cloud (for instance, **Azure Backdrop** or **Druva** can do that). This means in an emergency, the family office could run minimal operations from the cloud until on-prem is restored.

Have a **Business Continuity Plan (BCP)** alongside **technical DR**, list emergency contacts (for IT, for banks, etc.), alternate communication methods if email is down (such as a **phone tree** or **WhatsApp group,** albeit use the secure one as much as possible). Include procedures for scenarios such as **Office not accessible, systems compromised by cyberattack, key staff unavailable, for each, outline how work will continue.**

*For instance, if the financial system is locked by **Ransomware,** your BCP might state **We switch to manual mode, use read-only backup to get account balances,** coordinate with the bank by phone for urgent transactions, and rebuild systems on clean hardware. It's not pretty, but having it planned is vital!*

DR planning should also extend to assets where applicable. If the estate's security system fails, have a backup way to secure it (guards, manual locks). If the yacht's navigation IT is attacked, ensure crew have traditional navigation training/backup instruments (which they should per maritime regs).

Cyber resilience in these cases ties to safety – but knowing, for example, that the yacht's critical data (like its logs or configuration) is also backed up means quicker restoration of systems after a cyber incident at sea.

Tooling Recommendations

Use a robust **backup** software solution, examples would include:

- **Veeam Backup & Replication** (Very popular, supports immutability features),
- **Acronis Cyber Backup** (includes Anti-Ransomware defense),
- enterprise solutions such as **CommVault.**

These can automate multi-destination backups (even just an occasional manual check that backup files haven't been tampered with.

For resilience, maintain **spare equipment,** have at least one spare laptop pre-imaged, spare firewall or a subscription to a virtual firewall if primaries fail, etc. Keep bootable recovery media handy (with latest antivirus and tools).

Executive Decision Points

Determine acceptable downtime (**RTO**) for various services, the principal might say email must never be down more than an hour, but can live with financial system down for a day If needed, or vice versa.

These priorities will shape investment e.g., if near-zero downtime is required for communications, maybe invest in a secondary email system or a very redundant setup across data centers.

Budget for backups is **like insurance,** sometimes as **a cost with no direct ROI until disaster strikes.** Executives must champion it. Also decide on the **backup retention,** how far back to keep data (**that's where you have to consider compliance vs cost of storage**). Possibly decide to use offline/off-site storage for archival (e.g. annual backups stored indefinitely in a safe) in case of a long—term need or a future audit discovery.

Crucially, support the **drills and tests.** Leadership should occasionally participate or at least review the results. It's reassuring to know **we restored our critical server in 4 hours in a test.** This gives confidence in the face of ransomware news, etc. Encourage a culture where testing backups is as routine as financial audits.

Regulatory Mapping

Regulators care about resilience. **SAMA** requires banks to have DR sites and to test disaster recovery periodically, while not mandated here, adopting similar rigor is important. **PDPL** implicitly requires the ability to restore the availability of personal data in case of incidents

Similar to GDPR's Article 32 which explicitly includes backups and restores procedures as a security measure. Not being able to recover personal data after an incident could be seen as failing to protect it. loss of availability is a violation in GDPR terms, likely PDPL too.

ZATCA however, you must be able to reproduce invoice records even if systems crash – backups ensure compliance with record-keeping. NCA ECC emphasizes resilience and continuity for critical infrastructure; one could argue family office handling massive funds has critical elements akin to those.

Finally, having strong backups and DR will reassure the principal that, come what may, fire, flood, cyberattack, **their operations and legacy are safe.** It's a hallmark of banking grade security to say, **even if our data center is wiped, we can be up elsewhere in hours, and the family office should aim for that level of assurance.**

CYBERSECURITY

Audit & Governance

Audit & Governance

All the advanced security measures must be continuously governed and audited to remain effective. **Audit & Governance** provide the oversight, accountability and continuous improvement needed to sustain a military-grade cybersecurity posture over time. They ensure that the policies are not just on paper, but are followed in practice, and that the security program adapts to new challenges and regulations.

Governance Structure

Establish clear roles and responsibilities for cybersecurity within the family office. Given the small size, there may not be layers of management, but it's crucial to designate a **Chief Information Security Officer (CISO)** role, even if **part-time** or virtual who reports to the principal or the **CEO** on security matters.

This person (or committee if formed) should develop and maintain security policies, risk assessments, **and ensure all 15 areas we've discussed are being managed**. They act as the champion for security in executive discussions and ensure it remains a priority (so it doesn't slip due to convenience or cost pressures).

In governance, also involve the principal/family periodically e.g. a quarterly cybersecurity briefing to the principal, covering the current threat landscape, status of controls, and any exceptions or incidents. This keeps the top leadership engaged and shows commitment form the top, which is key to a strong security culture.

Policy Framework and Maintenance

Develop a suite of **top-level security policies** — covering key areas such as:

- **Access control**
- **Data protection**
- **Acceptable use**
- **Incident response**, and more.

Ensure these policies are **formally approved by management** and **communicated to all staff**.

The policies should be aligned with established standards such as **NIST Cybersecurity Framework (NIST CSF)** or **ISO 27001**, both of which provide a comprehensive set of **security controls**. While the family office can **tailor** these policies to its specific context, aligning with an **international framework** ensures that no **critical gaps** are overlooked.

For example, the office should maintain:

- An **Information Security Policy**
- A **Business Continuity & Disaster Recovery (BC/DR) Policy**
- A **Vendor Risk Management Policy** — updated when there are **regulatory changes** or the adoption of **new technologies**.

Regular Audits and Assessments

Perform **independent cybersecurity audits** periodically. This could be hiring an external firm to do a full review against a standard (like a mock audit against SAMA or NCA controls, or an ISO 27001 readiness assessment). They will identify any gaps or weaknesses objectively.

Additionally, do technical **penetration testing** annually on your external footprint and perhaps internally (these tests if, despite controls, a hacker could get in). Include **social engineering tests** too (phishing campaigns, etc.) to audit employee vigilance.

For processes, consider **internal audits,** e.g., have someone not involved in daily IT check that backups are happening per schedule, or that user access reviews are done.

If an independent auditor for financials is present, loop them into verifying some IT general controls as part of their audit (many family offices integrate that to satisfy any stakeholders that financial reports are produced in a controlled environment).

Importantly, audit findings must be documents with clear remediation plans and tracked to completion. This creates a cycle of continuous improvement, aiming for that **Adaptive Maturity (Level 5)** where cybersecurity is continuously refined and integrated into risk management.

Metrics and Reporting

Governance should be data-driven. Define a set of **Key Risk Indicators (KRIs)** or metrics for cybersecurity and report them to leadership regularly. Examples here would include:

- Number of blocked attacks per month
- Average time to apply critical patches
- Number of incidents detected and responded to
- Compliance status with training (e.g. % of employees who completed security training), results of phishing tests (e.g. 0% clicked last quarter vs 5% the quarter before shows improvement).

Also track compliance metrics like **all endpoints encrypted** – 100% or vendor contracts with security clauses, 95%, one in progress, these are all examples of course.

These metrics give executives a high-level view and help justify investments. It also shows accountability, if metrics slip, **governance processes should question why and demand correction.**

Adaptive Improvement

Use a recognized maturity model to gauge progress, so for instance, measure against **SAMA's maturity levels** or **CMMI**, and strive towards the higher levels (Managed, Measurable, Adaptive). If initially some practices were ad-hoc, the goal is to formalize them, then make them metrics-driven then constantly improve.

Governance forums (even if just a monthly security meeting) should discuss new threats or changes (such as **AI deepfake scams on the rise, what are we doing about it?**) and ensure the program adapts, possibly allocating budget for new controls or approving policy changes swiftly.

Alignment with Regulations and Standards

Governance ensures ongoing compliance. Assign someone (likely the CISO or DPO) to stay updated on regulatory changes.

E.g. If PDPL issues new executive regulations or SDAIA updates cross-border rules, incorporate those and brief leadership.

Keep evidence of compliance activities (training records, policy sign-offs, risk assessment reports), in case of a regulatory inquiry or an incident, being able to show **we have a governance framework,** we did our due diligence, can greatly reduce penalties and damage!

Additionally, consider voluntary certification for assurance. **Achieving ISO 27001 certification, for instance, could be a proud milestone demonstrating the office meets international security management standards.** Quiet possibly beyond typical family offices.

It involves audits which becomes part of governance routine. Alternatively, an **SOC 2 Type II Report** could be obtained if the family office ever needs to demonstrate controls to external parties (less likely unless they host services for others, but it's an option). The act of preparing for these certifications often strengthens governance.

Tooling Recommendations

Use GRC software (like **ZenGRC, Riskonnect, or even modules in Office 365 Compliance Center)** to track controls, map them to requirements (**PDPL, NIST, etc.)** and log audit results and remediation. Use **task management (JIRA or Planner)** for tracking audit findings.

Some companies implement **continuous control monitoring** tools that automatically check systems for compliance, (for instance, a tool that checks weekly if any critical patches missing or if any privileged account was created outside change process).

This can be heavy, but scaled to the family office by focusing on key controls.

Executive Involvement

Governance is ultimately an executive responsibility. The principal or CEO should formally endorse the security program and possibly **sign off on risk acceptance** when needed. If there's any area where the office can't fully implement a control (say, a legacy system on a yacht that can't be patched quickly), that risk should be presented to executives and either mitigated or explicitly accepted with rationale.

This ensures no critical risk is ignored inadvertently. It's similar to how a bank's board reviews risk reports, here, the family principal or a trusted advisor takes that role. It elevates cybersecurity to a strategic level, not just IT ops.

Regulatory Mapping

Good governance and audit practices are exactly what **regulators expect to see**:

- Under **PDPL**, organizations must maintain documented **privacy policies** and **procedures** formally **approved by the head of the entity**, along with clear **evidence of compliance**. Regulators can request proof, such as **Data Protection Impact Assessments (DPIAs)** or **demonstration of implemented controls**. A well-run **governance program** ensures all of this is readily available.
- **SAMA** expects its members to perform **self-assessments** against their **cybersecurity framework**. While a family office is not required to do this, it can **voluntarily adopt this practice** — and even share the results with **partner banks** as assurance of cyber maturity. This is valuable, as some banks will inquire about a **family office's cyber posture** before authorizing certain types of high-value transactions — and our strong governance would stand out positively.
- **NCA ECC-2** places strong emphasis on **governance** and **clearly defined responsibilities** within the organization. By mirroring this structure — designating a clearly **accountable cybersecurity leader** and performing **regular risk assessments** — the family office would be aligning with **government-level expectations**.
- **GDPR** and other **global privacy norms** also strongly favor having a robust **security governance structure**. For example, under GDPR, regulators specifically check whether **security policies** and **employee training** were in place when investigating a **data breach**.

In short: establishing **solid audit and governance** transforms cybersecurity from a **one-time project** into an **ongoing, living program**. This approach ensures that **military-grade security** is not only **achieved**, but also **sustained** and **continuously improved**.

At any time, the family office would be able to clearly demonstrate:

- **How risks are managed**
- **What controls are in place**
- **Evidence that the controls are effective**
- **Leadership oversight of the program**.

This level of diligence completes the **cybersecurity blueprint**, builds strong **confidence for the principal**, and ensures the office meets — or even exceeds — the standards expected by **private banks** and **sovereign wealth funds**.

The above guide synthesizes best practices from industry standards and regulatory requirements, augmented by insights from high-net-worth cybersecurity advisories and relevant laws. Key references ***include Saudi Arabia's PDPL law and data security guidelines****,* ***SAMA's Cybersecurity Framework expectations for financial institutions****,* ***international standards like NIST's Zero Trust Architecture*** *and* ***ransomware recovery guidelines****, as well as expert commentary on family office cyber threats. These and other cited sources underpin the recommendations, ensuring the strategy is grounded in proven approaches. The result is a comprehensive, defense-in-depth blueprint poised to protect the UHNWI's wealth and privacy against even the most formidable adversaries.*