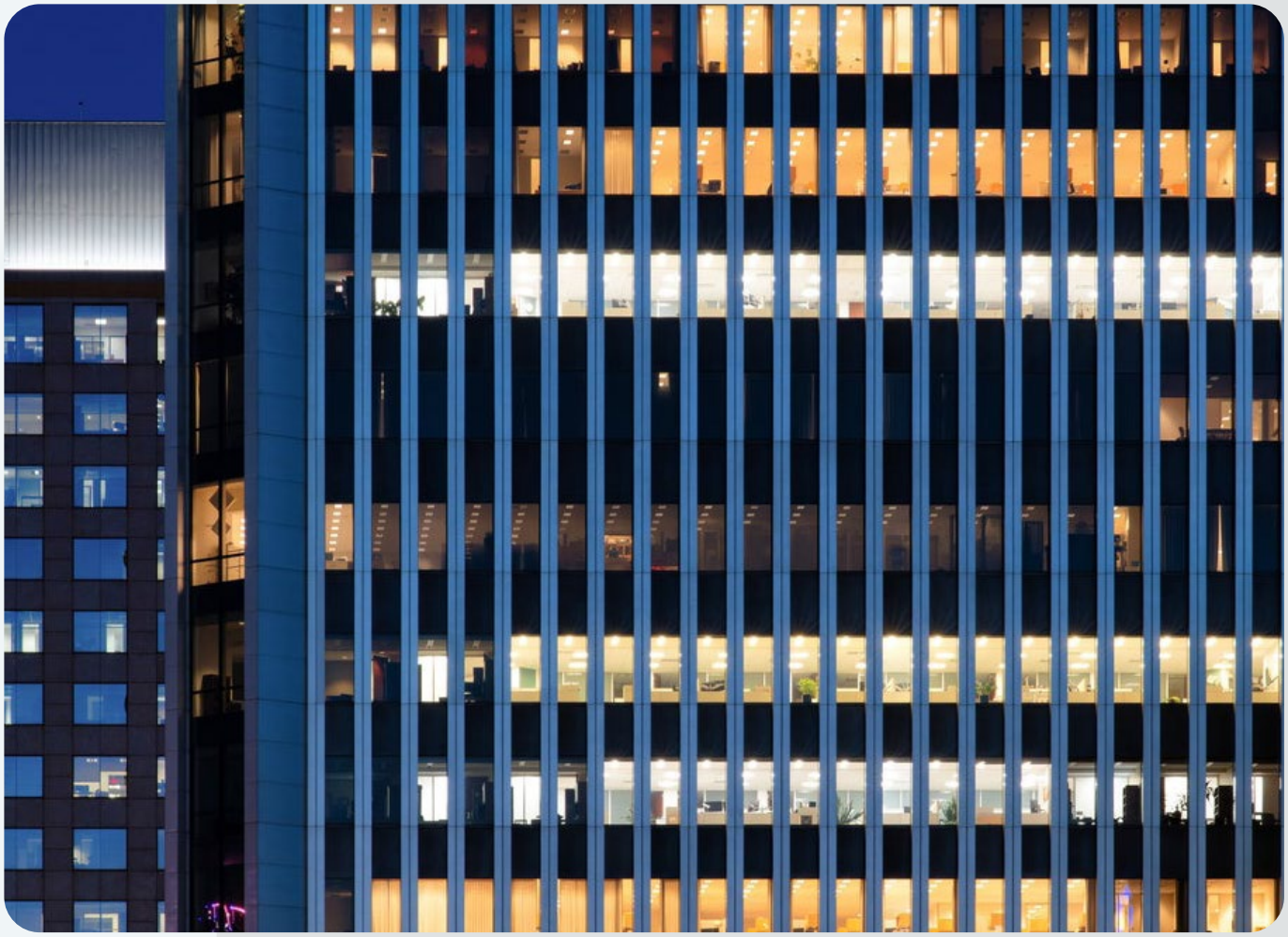
citi Private Bank

Managing cybersecurity and fraud risks

Best practices for family offices



Contents

Foreword

In today's interconnected world, family offices and the families they serve face a variety of complex risks. Among these are threats to physical and financial assets, privacy, social media and cybersecurity. These threats may become more acute as cyber criminals and other threat actors leverage emerging technologies, including generative artificial intelligence (AI) capabilities, underscoring the urgency and importance for family offices to develop a comprehensive cybersecurity program and address vulnerabilities proactively.

As one of the world's leading financial institutions with on-the-ground presence in 90+ countries, Citi is at the forefront of protecting our clients' financial assets and privacy, assessing and neutralizing threats as they arise, as well as collaborating with private and public entities tasked to build a more secure and resilient cyber infrastructure for the future.

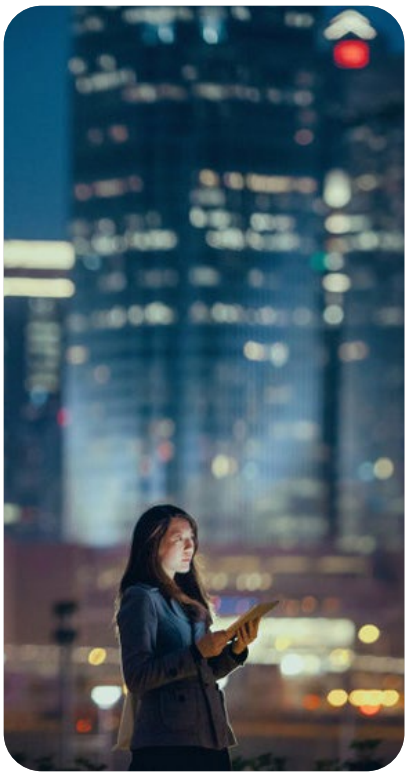
Citi Private Bank's Global Family Office Group has the privilege of serving some of the world's wealthiest individuals and families. Our Family Office Advisory team has deep experience providing guidance on all aspects of family office creation and management. In our engagement with family offices, we find that with limited resources at hand, family offices often fail to implement a robust and proactive cybersecurity program and instead find themselves reacting to breaches and incidents of fraud. On other occasions, even with the best intent, they find the sheer volume of content and complexity overwhelming, leading to inaction.

In this whitepaper, we have attempted to distill the expertise of Citi's in-house experts and provide best practices promoted by industry experts and government organizations dedicated to fighting cybercrime. We have also covered some practical tips on preventing fraud and features that you may want to activate on your bank accounts.

We hope you find this information, including the actionable checklist, helpful and that it provides an impetus to assess, act and improve your existing cybersecurity program and framework. We stand by to assist you in this journey.

Hannes Hofmann
Head
Global Family Office Group

Ajay Kamath
Family Office Advisory
North America Head
Global Family Office Group



Cybersecurity and fraud risk

Family offices face unique fraud risks due the scale of their wealth, private nature and often limited internal controls compared to financial institutions. Several of those fraud risks overlap or are exacerbated by a lack of cybersecurity preparedness. Without robust cybersecurity, family offices may find themselves more vulnerable to digital threats that can lead to fraud and loss of assets. While family offices face many fraud risks, below are a few key risks where cybersecurity plays a critical role:

Online threats and data breaches: Lack of cybersecurity measures, such as firewalls, encryption and intrusion detection systems, makes family offices highly susceptible to hacking, ransomware and potential unauthorized data access.

Social engineering and impersonation scams: Poor email security and lack of employee training on cybersecurity best practices may make family offices vulnerable to phishing and impersonation scams, leading to financial losses.

Identity theft and account takeovers: Weak access controls, weak passwords and lack of multi-factor authentication protocols may lead to unauthorized access and fraudulent transactions.

Insider fraud: Without activity monitoring, audit trails and access restrictions, insider threats can be harder to detect and prevent, allowing employees with malicious intent to exploit vulnerabilities.

Third-party fraud: Family offices without processes to vet third-party vendors increase their risk of exposure through insecure connections, compromised vendors and unauthorized access or malware risks.

Investment and financial fraud: Lack of secure communication channels and transaction monitoring may leave family offices vulnerable to a breach of confidential data, including interception and tampering by competitors and cybercriminals, leading to fraudulent investments or wire transfers.

Unauthorized access and physical security risks: Cybersecurity preparedness includes securing not just digital but also physical access to sensitive information and infrastructure. Lack of such protocols may provide entry to unauthorized access to devices, documents, data or manipulation of records.

With the advent of AI, we have seen the amplification of cybersecurity and fraud risks. However, it's important to note that while AI can aid and abet malicious acts, it can also help organizations monitor, understand and, in many cases, mitigate the amplified risks.

To aid in assessing and strengthening your family office's cybersecurity preparedness, in the following pages we have included a checklist that follows the industry-standard framework of:

Govern	The organization's cybersecurity risk management strategy, expectations and policy are established, communicated and monitored
Identify	The organization's current cybersecurity risks are highlighted
Protect	Safeguards to manage organizational cybersecurity risks are used
Detect	Possible cybersecurity attacks and compromises are found and analyzed
Respond	Actions are taken following a detected cybersecurity incident
Recover	Assets and operations affected in a cybersecurity incident are restored

Assessing your cybersecurity preparedness

Govern	Assessment
Cybersecurity strategy and policy The family office's cybersecurity risk management strategy and policy are established, communicated, enforced and updated periodically.	☐ Completed ☐ In progress ☐ Scoped ☐ Not started
Cybersecurity ownership A named role/position/title is identified as responsible and accountable for planning, resourcing and execution of cybersecurity activities.	☐ Completed ☐ In progress ☐ Scoped ☐ Not started
Oversight A comprehensive assessment is carried out periodically to identify and mitigate risks.	☐ Completed ☐ In progress ☐ Scoped ☐ Not started

Identify	Assessment
Asset inventory Maintain a regularly updated inventory of all organizational assets with an IP address. This inventory is updated on a recurring basis, no less than monthly.	☐ Completed ☐ In progress ☐ Scoped ☐ Not started
Update all software and hardware Apply regular security updates to all software and hardware to ensure that all known exploitable vulnerabilities in internet-facing systems are patched or otherwise mitigated. If software and hardware are no longer supported by the vendor, which also means that updates are no longer released, the organization should prioritize replacing them.	☐ Completed ☐ In progress ☐ Scoped ☐ Not started
Assess and validate cybersecurity coverage and defenses Vetted cybersecurity experts should regularly validate the effectiveness and coverage of family office cybersecurity defenses.	☐ Completed ☐ In progress ☐ Scoped ☐ Not started
Supply chain compromise Ensure procurement documents and contracts, such as service-level agreements (SLAs), stipulate that they notify the family office of security incidents without delay.	☐ Completed ☐ In progress ☐ Scoped ☐ Not started

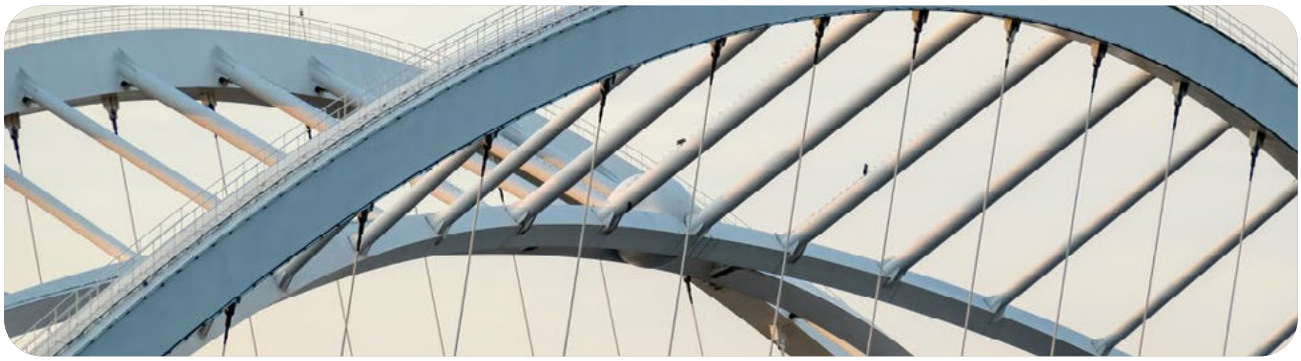
* This checklist is an adapted and simplified version of the Cybersecurity and Infrastructure Security Agency's (CISA) Cross-Sector Cybersecurity Performance Goals (CPG) Checklist. The CISA operates under the U.S. Department of Homeland Security and the CPGs are a common set of protections that all critical infrastructure entities are encouraged to implement to reduce risks. To learn more about CISA and the CPGs, please visit: Cross-Sector Cybersecurity Performance Goals | CISA

By clicking this link you will visit a third-party website that is not owned or managed by Citi Private Bank. We have no control of the content, privacy or security beyond this point.

Protect	Assessment
Password management Change all default passwords and implement a system-enforced rule requiring minimum password length and complexity. Family offices should consider deploying passphrases and password managers to make it easier for users to securely maintain such passwords.	☐ Completed ☐ In progress ☐ Scoped ☐ Not started
Remove access for departed employees Create a defined administrative process to manage offboarding for all departing employees which includes the revocation and collection by the family office of all physical badges, key cards, tokens, provisioned devices, etc., and the disablement of all user accounts and access to organizational resources, both digital and physical.	☐ Completed ☐ In progress ☐ Scoped ☐ Not started
Administrative management Withhold administrator or super-user privileges from all user accounts. Maintain separate user accounts for all actions and activities not associated with the administrator role (e.g., for business email, web browsing). Privileges are reevaluated on a recurring basis to validate continued need for permissions.	☐ Completed ☐ In progress ☐ Scoped ☐ Not started
Implement multifactor authentication Deploy multifactor authentication (MFA) where available. Use phishing-resistant MFA such as hardware MFA or application-based push notifications. Organizations should only use SMS or voice MFA as a last resort.	☐ Completed ☐ In progress ☐ Scoped ☐ Not started
User training Require at least annual trainings for all employees, family members and contractors that cover basic security concepts, such as phishing, business email compromise, password security, etc., as well as fostering an internal culture of security and cyber awareness.	☐ Completed ☐ In progress ☐ Scoped ☐ Not started
Encryption Ensure properly configured encryption is utilized to protect data in transit and at rest. This includes password-protecting Wi-Fi networks, desktop machines, smartphones, and databases with industry-standard encryption.	☐ Completed ☐ In progress ☐ Scoped ☐ Not started
Business email compromise Maintain a dedicated corporate email infrastructure with the most updated protocols to prevent business email compromise such as DKIM, DMARC, STARTTLS, and sender policy framework (SPF).*	☐ Completed ☐ In progress ☐ Scoped ☐ Not started
Disable macros Implement a system-enforced policy that disables Microsoft Office macros, or similar embedded code, on all devices by default. If macros are needed for specific tasks, there should be a request and authorization process.	☐ Completed ☐ In progress ☐ Scoped ☐ Not started

*DKIM, DMARC, STARTTLS and SPF are email security protocols that work together to prevent unauthorized emails and protect against cyber attacks. DKIM (DomainKeys Identified Mail) verifies the authenticity of an email's sender and ensures that the email is from the claimed domain. DMARC (Domain-based Message Authentication, Reporting and Conformance) defines how to handle emails that fail DKIM or SPF authentication checks. STARTTLS (Secure Transport Layer Security) encrypts email content during transit. SPF (Sender Policy Framework) helps verify that emails are sent from authorized servers.

Protect	Assessment
Hardware / software additions / downloads Enforce an approval process for the installation or deployment of any new hardware, firmware or software/software version, based on a risk-informed allowlist where technically feasible.	☐ Completed ☐ In progress ☐ Scoped ☐ Not started
Documentation Maintain accurate documentation describing the baseline and current configuration details of all critical IT and network assets to facilitate more effective vulnerability management and response and recovery activities. Periodic reviews and updates are performed and tracked on a recurring basis.	☐ Completed ☐ In progress ☐ Scoped ☐ Not started
Drills and testing Test, simulate and review incident response plans for cybersecurity preparedness at least annually. Document and take corrective action from lessons learned.	☐ Completed ☐ In progress ☐ Scoped ☐ Not started
Back up and data destruction: Regularly create backups of all systems and data necessary for operations, with copies stored separately from the source systems and re-tested at least annually.	☐ Completed ☐ In progress ☐ Scoped ☐ Not started
Disable external USB and removable media Maintain policies and processes preventing connection to office systems of unauthorized media and hardware, including restricted or disallowed use of USB devices and removable media.	☐ Completed ☐ In progress ☐ Scoped ☐ Not started



Detect

Assessment

Detection logs
Gather and store access and security-focused logs (e.g., IDS/IDPS, firewall, DLP, VPN) for use in both detection and incident response activities (e.g., forensics).* Security teams get notified when a critical log source is disabled, such as Windows Event Logging.

- ☐ Completed
- ☐ In progress
- ☐ Scoped
- ☐ Not started

Respond

Incident reporting
Define how to report all confirmed cybersecurity incidents to relevant internal and any external entities (e.g., state/federal regulators etc.).

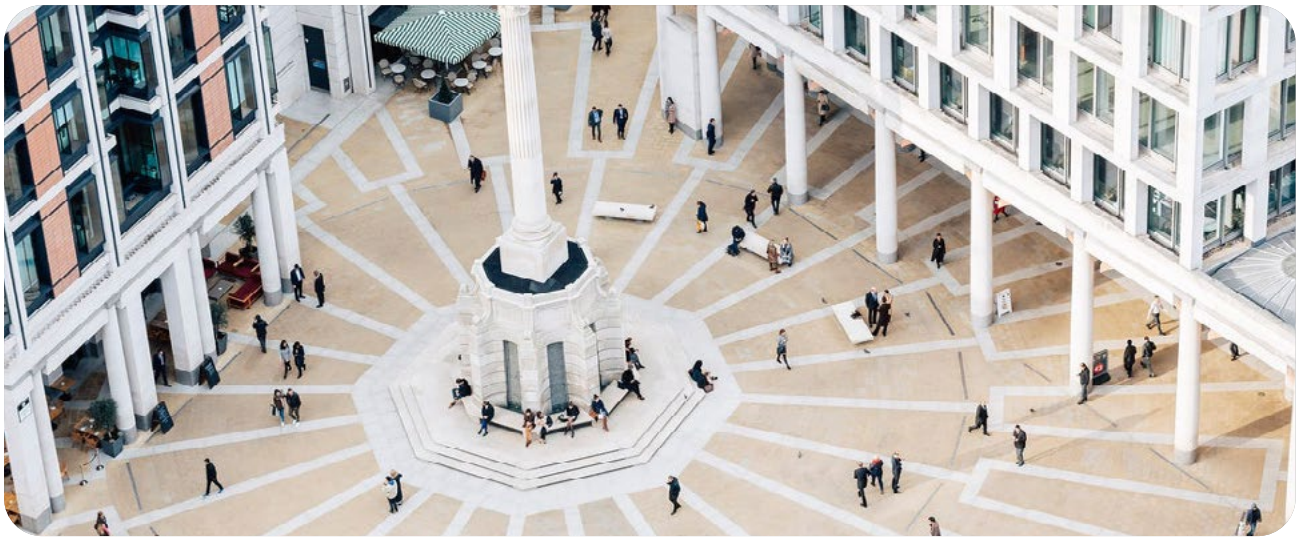
- ☐ Completed
- ☐ In progress
- ☐ Scoped
- ☐ Not started

Recover

Recovery plans
Develop, maintain and execute plans to recover and restore to service business or mission-critical assets or systems that might be impacted by a cybersecurity incident.

- ☐ Completed
- ☐ In progress
- ☐ Scoped
- ☐ Not started

*An IDS/IDPS (Intrusion Detection/Prevention System) monitors network traffic for suspicious activity and alerts administrators, while a firewall acts as a filter to control incoming and outgoing network traffic, DLP (Data Loss Prevention) aims to prevent sensitive data leaks by monitoring and blocking unauthorized data transfers, and a VPN (Virtual Private Network) creates a secure encrypted connection over a public network, protecting data privacy by masking the user's IP address.

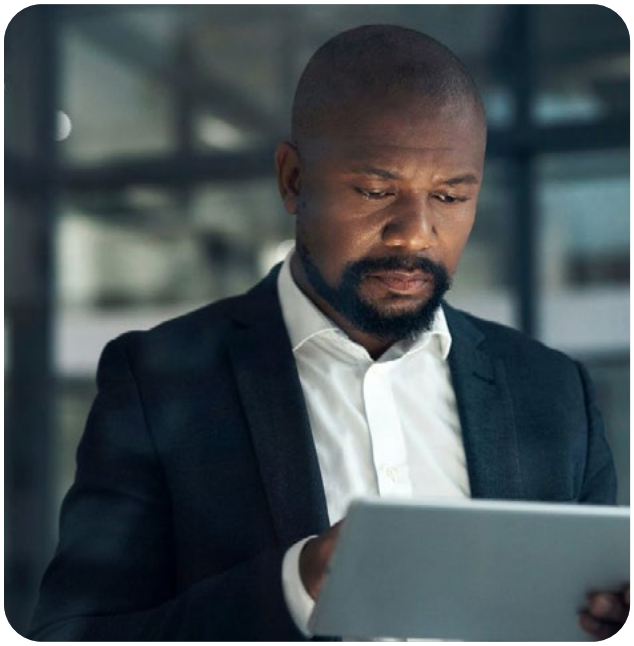


Considerations for managed security service providers

Owing to complexity and ever-evolving threats, and niche expertise required to run an effective security program, many family offices may choose to outsource their security to a managed security service provider (MSSP) instead of going through the effort to hire, train and maintain their own cybersecurity program.

What is an MSSP?*

An MSSP is an external party that provides cybersecurity services to its customers. An MSSP's services are broad and can range from baseline system monitoring to comprehensive offerings that fully manage a customer's security.



Some key MSSP services may include:

- **Security event monitoring:** This can range from basic event monitoring to comprehensive management and observation.
- **Managed detection and response (MDR):** This includes supporting their customers in the event of a breach to contain, investigate and remediate the issue and recover from the event.
- **Penetration testing (pentests):** A simulated cyberattack can be a great way to prepare, train and identify needed improvements to a customer's cybersecurity posture.
- **Managed firewall:** MSSPs can manage, maintain and establish clear firewall policy rules to better secure outgoing and incoming traffic on a customer's network.
- **Vulnerability management:** The ongoing, regular process of identifying, assessing, reporting on, managing and remediating cyber vulnerabilities across endpoints, applications, software, workloads and systems.

* There are numerous resources available on how to choose an appropriate MSSP for your needs. We encourage you to research this topic further to make a decision that is right for you given the services you require and the best expertise to execute on them.

Cybersecurity hygiene basics

With so many threats and controls to mitigate them, maintaining cybersecurity hygiene can seem like an overwhelming challenge, perhaps leading to paralysis of decision-making and inaction.

Below are six strategies that our in-house cybersecurity experts believe are important steps that individuals and family office teams can implement to make a significant improvement to their cybersecurity readiness.

Create strong passwords

a. Family offices should enforce a minimum password length of at least 12 alpha-numeric and special characters consisting of numbers, symbols, and capital and lowercase letters. These passwords should be unique to each user and complex.

b. Individuals should consider using passphrases, or a long string of words and text, as opposed to traditional passwords. Avoid common phrases, famous quotations and song lyrics.

c. Always change default passwords for all hardware and software. Be sure to change your passwords regularly and never share or reuse the same password.

d. Individuals and family offices should ideally use password managers. Password managers securely store all your passwords across accounts in encrypted vaults. The user only must remember the login information for their password manager. Examples of password managers include Apple Passwords, 1Password, Bitwarden and KeePass.* Credentials should not be stored within browsers.

Use multifactor authentication

a. All accounts which offer multifactor authentication (MFA) should have it enabled.

b. MFA adds an additional layer of security via the use of a unique code, key or biometrics, making it significantly harder for gaining unauthorized access to devices and data.

c. If available, hardware MFA using FIDO such as YubiKey should be used. Otherwise, users should opt for application-based MFA such as Google Authenticator or Authy.* Family offices should rely on SMS or voice MFA only as a last resort.

Keep devices and software updated

a. Enable automatic updates for all devices, software and applications to reduce the risk of exploitable vulnerabilities. Leveraging this measure can also introduce new or improve existing functionality.

b. If devices have reached end of life and no longer receive manufacturer updates, the family office should prioritize replacing them.

* This list is provided for informational purposes only. Citi does not endorse any specific tools or solutions.

Back up and secure data

a. Back up all computers and systems necessary for operations regularly.
b. Store backup data separately from the source systems, such as in a cloud environment or offsite from the regular work location.
c. Encrypt and password-protect all devices and sensitive data.
d. Install antivirus software and regularly scan devices.

Practice safe web browsing

a. Keep browsers updated and routinely close out of them.
b. Use firewalls as a first line of defense to prevent unauthorized users from accessing your network, websites, mail servers and other sources of information that can be accessed from the web.
c. Block third-party cookies and remove those already on the browser.
d. Manage the advertising settings on browsers.
e. Properly vet extensions before adding them to browsers.

Use caution when clicking

a. Beware of clicking on unknown links received via texts, emails or unsolicited messages from social media platforms.
b. A malicious actor can send a link to an otherwise legitimate looking website that, if clicked on, will lead to the delivery of malware and potential data loss.
c. Do not click on links or attachments until verifying the sender is who they claim to be.

Closing thoughts

The constantly evolving landscape of cybersecurity and fraud prevention calls for robust and adaptive frameworks to safeguard family offices against emerging threats. This white paper has outlined comprehensive strategies and practical steps to mitigate risks and act based on frameworks that are recognized by cybersecurity professionals. By proactively addressing vulnerabilities and implementing effective measures, enhancing employee awareness, and fostering a culture of vigilance, we believe family offices can build resiliency, protecting their critical assets and maintaining family trust.

Please reach out to your Private Banker for more information on managing cybersecurity and fraud risks and view the appendix for treasury management best practices and tools to combat fraud.

Appendix: Treasury management best practices to combat fraud

Based on extensive experience serving family office clients, we can offer best practices and tools available to reduce fraud risk on banking and treasury accounts. These can be used independently or in conjunction with an overall cybersecurity program.

Mitigating security risk

- Maintain separate accounts for payables and receivables
- Manage payments via secure bank online platforms versus manual transfers such as check writing
- Utilize a minimum standard of dual approvals for all outbound payments
- Institute a strong multi-layered process when providing bank account instructions to vendors/counterparties, i.e., validate beneficiary and payer accounts – review in detail any requests for changes.
- Reconcile often, using any available bank reporting features to assist
- Monitor for red flags, such as marked as urgent/secret or when bank account information has been altered after an order is placed

At least annually, family offices should review the following with their banking partner:

- Implementation of robust internal controls – segregation of duties
- Entitlements, account structure, products and services attached to each account
- Moving or closing dormant accounts
- Adding available fraud protection tools to all eligible accounts
- Swift removal of entitlements of exited family office employees or those who have changed roles internally
- Fine-tuning adjustments to bank systems/platforms for individuals' access to ensure adherence to family office policies

Anti-fraud tools & reconciliation services

- **Check positive pay** – Bank reviews checks presented for payment against check issuance data uploaded by the company, flagging discrepancies to the family office
- **Positive pay no issue file** – Bank treats every check as potentially suspicious where the family office has signed up for positive pay but has not uploaded check issuance data
- **ACH positive pay** – Bank reviews electronic payments and transfers (automated clearing house transactions or ACH), flagging for family office confirmation where the transaction does not appear on the family office–supplied approved list
- **ACH debit blocks** – Bank automatically blocks all ACH debits by any entity, such that only authorized outgoing payments occur and no ACH debits
- **ACH debit filters** – Bank processes only ACH debits that appear on the family office–supplied approved list

About the Global Family Office Group

Citi Private Bank's Global Family Office Group serves single family offices, private investment companies and private holding companies, including family-owned enterprises and foundations, around the world.

We offer clients comprehensive private banking and family office advisory services, institutional access to global opportunities and connections to a community of like-minded peers.

For more information, please contact your Private Banker or the group head in your region.

citiprivatebank.com/globalfamilyoffice

Regional Contacts

Richard Weintraub
Americas Head
Global Family Office Group
richard.weintraub@citi.com

Alessandro Amicucci
Europe, Middle East & Africa Head
Global Family Office Group
alessandro.amicucci@citi.com

Bernard Wai
Asia Pacific Head
Global Family Office Group
bernard.wai@citi.com

Important information:

The information contained in this Communication is based on generally available information and, although obtained from sources believed by Citi to be reliable, its accuracy and completeness cannot be assured, and such information may be incomplete or condensed. Any assumptions or information contained in this Communication constitute a judgment only as of the date of this document or on any specified dates and is subject to change without notice.

Citi and its employees are not in the business of providing, and do not provide, tax or legal advice to any taxpayer outside Citi. Any statement in this Communication regarding tax matters is not intended or written to be used, and cannot be used or relied upon, by any taxpayer for the purpose of avoiding tax penalties. Any such taxpayer should seek advice based on the taxpayer's particular circumstances from an independent tax advisor.

Communication is for the sole and exclusive use of the intended recipients and may contain information proprietary to Citi which may not be reproduced or circulated in whole or in part without Citi's prior consent. The manner of circulation and distribution may be restricted by law or regulation in certain countries. Persons who come into possession of this document are required to inform themselves of, and to observe such restrictions. Citi accepts no liability whatsoever for the actions of third parties in this respect. Any unauthorized use, duplication, or disclosure of this document is prohibited by law and may result in prosecution. Other businesses within Citigroup Inc. and affiliates of Citigroup Inc. may give advice, make recommendations, and take action in the interest of their clients, or for their own accounts, that may differ from the views expressed in this document. All expressions of opinion are current as of the date of this document and are subject to change without notice. Citigroup Inc. is not obligated to provide updates or changes to the information contained in this document.

Citi Private Bank is a business of Citigroup Inc. ("Citigroup"), which provides its clients access to a broad array of products and services available through bank and non-bank affiliates of Citigroup. Not all products and services are provided by all affiliates or are available at all locations. In the U.S., investment products and services are provided by Citigroup Global Markets Inc. ("CGMI"), member FINRA and SIPC, and Citi Private Alternatives, LLC ("CPA"), member FINRA and SIPC and Citi Global Alternatives, LLC ("CGA"). CGMI accounts are carried by Pershing LLC, member FINRA, NYSE, SIPC. CPA acts as distributor of certain alternative investment products to clients of Citi Private Bank. CGMI, CPA, CGA and Citibank, N.A. are affiliated companies under the common control of Citigroup.

Outside the U.S., investment products and services are provided by other Citigroup affiliates. Investment Management services (including portfolio management) are available through CGMI, CGA, Citibank, N.A. and other affiliated advisory businesses. These Citigroup affiliates, including CGA, will be compensated for the respective investment management, advisory, administrative, distribution and placement services they may provide.

Citibank, N.A., Hong Kong / Singapore organised under the laws of U.S.A. with limited liability. This communication is distributed in Hong Kong by Citi Private Bank operating through Citibank N.A., Hong Kong Branch, which is registered in Hong Kong with the Securities and Futures Commission for Type 1 (dealing in securities), Type 4 (advising on securities), Type 6 (advising on corporate finance) and Type 9 (asset management) regulated activities with CE No: (AAP937) or in Singapore by Citi Private Bank operating through Citibank, N.A., Singapore Branch which is regulated by the Monetary Authority of Singapore. Any questions in connection with the contents in this communication should be directed to registered or licensed representatives of the relevant aforementioned entity. The contents of this communication have not been reviewed by any regulatory authority in Hong Kong or any regulatory authority in Singapore. This communication contains confidential and proprietary information and is intended only for recipient in accordance with accredited investors requirements in Singapore (as defined under the Securities and Futures Act (Chapter 289 of Singapore) (the "Act")) and professional investors requirements in Hong Kong(as defined under the Hong Kong Securities and Futures Ordinance and its subsidiary legislation). For regulated asset management services, any mandate will be entered into only with Citibank, N.A., Hong Kong Branch and/or Citibank, N.A. Singapore Branch, as applicable.

Citibank, N.A., Hong Kong Branch or Citibank, N.A., Singapore Branch may sub-delegate all or part of its mandate to another Citigroup affiliate or other branch of Citibank, N.A. Any references to named portfolio managers are for your information only, and this communication shall not be construed to be an offer to enter into any portfolio management mandate with any other Citigroup affiliate or other branch of Citibank, N.A. and, at no time will any other Citigroup affiliate or other branch of Citibank, N.A. or any other Citigroup affiliate enter into a mandate relating to the above portfolio with you.

To the extent this communication is provided to clients who are booked and/or managed in Hong Kong: No other statement(s) in this communication shall operate to remove, exclude or restrict any of your rights or obligations of Citibank under applicable laws and regulations. Citibank, N.A., Hong Kong Branch does not intend to rely on any provisions herein which are inconsistent with its obligations under the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission, or which mis-describes the actual services to be provided to you.

Citibank, N.A. is incorporated in the United States of America and its principal regulators are the US Office of the Comptroller of Currency and Federal Reserve under US laws, which differ from Australian laws. Citibank, N.A. does not hold an Australian Financial Services License under the Corporations Act 2001 as it enjoys the benefit of an exemption under ASIC Class Order CO 03/1101 (remade as ASIC Corporations (Repeal and Transitional) Instrument 2016/396 and extended by ASIC Corporations (Amendment) Instrument 2024/497).

In the United Kingdom, Citibank N.A., London Branch (registered branch number BR001018), Citigroup Centre, Canada Square, Canary Wharf, London, E14 5LB, is authorised and regulated by the Office of the Comptroller of the Currency (USA) and authorised by the Prudential Regulation Authority. Subject to regulation by the Financial Conduct Authority and limited regulation by the Prudential Regulation Authority. Details about the extent of our regulation by the Prudential Regulation Authority are available from us on request. The contact number for Citibank N.A., London Branch is +44 (0)20 7508 8000.

citi Private Bank