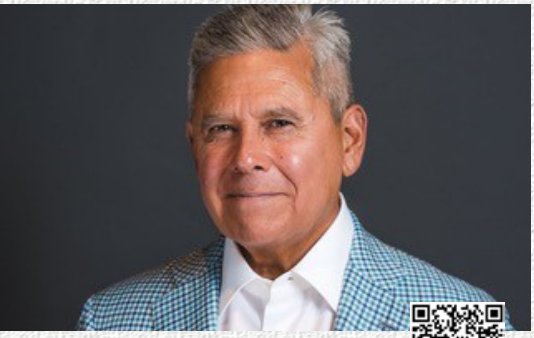
SINET

The SINET Risk Executive Handbook

A CISO's Guide to a Robust Employment Agreement, Employment Risks, and Technology Risk Governance

A SINET PUBLICATION
LED BY BRIAN FRICKE, CISSP, CISM
AND THE SINET SCOTTSDALE RISK EXECUTIVE WORKING GROUP

1ST EDITION



ADVISOR

Robert Rodriguez

Chairman of SINET

Venture Partner at SYN Ventures

Leader in the advancement of innovation within the international Cybersecurity domain, Strategic adviser on the development of global public private partnership models, connecting early-stage companies to investors and industry & government buyers.

SINET accelerates investments and innovation of early-stage, emerging growth, and publicly traded Cybersecurity companies into global marketplaces by connecting them to industry and government Risk Executives and Chief Information Security Officers, venture capital, and private equity firms. SINET brings together the world's highest level of executive Cybersecurity professionals through its Risk Executive Workshops, conferences for the larger Cyber ecosystem, and virtually on SINETConnect, their invitation–only, highly curated virtual platform that is changing the way trusted business dealings operate today and into the near future.

Previously, Mr. Rodriguez served 22 years as a Special Agent with the United States Secret Service where he held numerous executive leadership positions within the Presidential Protection Detail, Protective Intelligence, Inspection, Criminal Investigation Division, and the Counter Assault Team (CAT). His executive protection experience spanned 10 years at the White House serving Presidents Ronald W. Reagan, George H. Bush, William J. Clinton, and numerous Heads of State. He serves on several Cybersecurity Advisory Boards and has been called upon to advise private industry and federal governments as they build private sector outreach initiatives with corporations and the entrepreneurial and venture capital communities.

AUTHOR

Brian Fricke, CISP, CISM

CISO, City National Bank of Florida Board Advisor

A seasoned technology professional with a business-centric focus, specializing in strategic Enterprise Information Security Policy, Operations, and Technology Risk Management.

Mr. Fricke's career is marked by the establishment of innovative Information Security Programs for Military, Government, and Financial Institutions, ensuring compliance with some of the most stringent regulatory requirements. His broadest scope of responsibility has included the information & cyber security risk portfolio of over 600 sites, 30,000 personnel, and 20,000 systems worldwide. He also lends his expertise to the security and tech industry as a member to for-profit, and non-profit Boards, providing strategic guidance and insights based on his extensive experience. A former active-duty Marine, and Iraq War Veteran, Brian has dedicated a significant part of his career to public service, serving in various agencies with progressively expanding responsibilities. Brian was class president of The George Washington University School of Business, World Executive MBA, Class of 2013, and holds a Graduate Certificate in Strategic Cybersecurity Enforcement.

The SINET Risk Executive Handbook

A CISO's Guide to a Robust Employment Agreement, Employment Risks, and Technology Risk Governance

A guide to keeping the interests of Technology Risk Executives aligned with the Board of Directors and Executive Officers before, during, and after a Data Security Incident.

Contents

Contents

Foreword

It is with great pleasure that we present to you this handbook on mitigating career risks and empowering Chief Information Security Officers (CISOs) and Technology Risk Executives to better protect themselves. As a Venture Partner at SYN Ventures and the Chairman of SINET, I am delighted to lend my voice to this important publication.

This guide stems from a presentation by Michael Johnson (CISO, Meta Financial) and Brian Fricke (CISO, City National Bank of Florida) at the SINET Risk Executive Workshop in Scottsdale, Arizona in February 2023. I would like to recognize their efforts, in particular Brian's stewardship of this deliverable.

Historically, the CISO position was viewed as a technical blue-collar security cost center. Today, the sage and modern CISO can articulate complex matters to their BOD, is viewed as an enabler and driver of the business enterprise-wide, understands the company's business objectives, and at times can deliver ROI. Given the state of affairs in Cyber, the future belongs to the business-aligned Risk Executive.

Throughout this document, the umbrella term "Risk Executive" refers to CISOs, Chief Security Officers, Chief Information Officers, and other executives who manage technology risk at their organization. I fervently believe that this elevated title is deserving, as these individuals are managing more risk than most executives at any corporation, while carrying a higher level of liability due to the nature of their responsibilities.

It is important to note that this handbook is not a one-size-fits-all document tailored to the particular nuances of each job or industry, but rather an overarching patchwork of areas that one should consider when re-negotiating their current employment agreement or when being interviewed for a new position.

It is unlikely that this handbook would have gained traction 5 years ago, however under the circumstances of Joe Sullivan's conviction, The Wells Act notice to Tim Brown, Mudge's need to testify on Capitol Hill, and other scenarios yet to surface, it now has a chance to gain energy. Protecting yourself as a 21st century Risk Executive requires increased awareness, beginning with a robust employment agreement and the education of BODs. In the end, no one is going to protect you but you. There is an opportunity here for a movement.

SINET is known for bringing together the highest level of executive peers at the highest level of thought leadership in a trusted format that encourages transparency, which leads to increased knowledge sharing and information gained. By fostering a deeper understanding of risk management and offering practical guidance, this handbook strengthens the protection of both individuals and their organizations.

Thank you to all the members of the SINET Community as we remain steadfast in our support of the 21st century Risk Executive as they strive to protect our nation's critical infrastructures, national security, economic interests, and our inherent right to privacy.

Robert D. Rodriguez
Chairman, SINET
Venture Partner, SYN Ventures

Introduction

In today's rapidly evolving cyber domain, the adaptive role of the CISO/Risk Executive stands as a sentinel against a relentless wave of cyber-based attacks and technology risk. Having had the honor and pleasure of serving as and engaging alongside so many Risk Executives from around the world, I can attest to the immense challenges and responsibilities that define this profession.

Our journey requires a resolute commitment to changing cultural norms in safeguarding sensitive data, meeting the needs of not-so-aligned stakeholders, ensuring regulatory compliance, and mitigating the potentially catastrophic consequences of breaches in innovative yet pragmatic ways – all to support business strategy, prevent the erosion of revenue, and maintain investor confidence. It's such a daunting path that many have begun to second guess being employed in the role altogether. Yet within these challenges lies an extraordinary opportunity for growth, resilience, and transformative and creative leadership.

In light of these challenges, I am pleased to present this guide—my contribution to the landscape of proactive cybersecurity leadership material. This guide offers considerations for a robust employment agreement that empowers Risk Executives to better navigate the complexities of their roles. From reporting lines, liability management, insurance, and financial protections - to strategic corporate policies - this guide aims to improve career resilience, protections, and organizational alignment before, during, and after a breach. Every breach has a ripple effect across the profession. Our actions and willingness to lean into the uncomfortable unknown is more likely to succeed if the risk of professional repercussions has been adequately mitigated. If we don't begin to ask for these protections, who will?

Throughout these pages, you will find practical strategies, real-life experiences, and insights derived from industry leaders that highlight critical considerations for a resilient career. We must continue to advocate for change on a broader scale through education and by amplifying the guide's message through our own outlets. A movement to positively impact cultural norms, and perhaps regulatory enhancements that may relieve some of our daily pressures, can be attained to help elevate organizational risk reporting lines and achievable professional standards with appropriate legal protections.

As we delve into the risk and liability held in this career, I invite readers to embrace a shared vision for the future—one where proactive risk management of our careers removes distractions as we build more secure and resilient digital environments. With our collective efforts, we can forge a path to a safer interconnected world—one fortified by the unwavering dedication of Risk Executives and a shared commitment to protecting what matters most.

Special Thanks to the Risk Executives who collaborated on this work:
Michael Johnson, Joe Sullivan, Tim Brown, Nick Salian, Shaun Khalfan, Pam Lindemoen, Jerry Archer and many others!

Letter to the Board

In an era of increasing risk from the use of technology and data, the role of the Risk Executive has never been more crucial. This guide illustrates how the duties of a Risk Executive have significantly expanded beyond basic computer security management. Today's landscape demands that Risk Executives have expertise in strategic, financial, operational, compliance, and reputation risk management, along with a keen understanding of the business and its geopolitical risks. They must also adeptly navigate the demands of diverse stakeholders, inform strategic decisions, coordinate crisis management, and develop comprehensive breach mitigation and response plans.

> "For certain organizations – this reality highlights the necessity to elevate or establish anew, the role of a Chief Technology Risk Executive, or otherwise ensure that technology risk reporting occurs directly to the Board.

As fiduciary stewards of the organization, it is essential for you to have a direct line of communication with the Chief Technology Risk Executive. We exist to prevent the erosion of revenue. If the role is buried too deeply within the organization or placed in a position where conflicts of interest may arise (as between a CIO and CISO), you won't have the necessary information to make informed decisions. Direct reporting will ensure that vital technological risk insights are delivered to you without delay or dilution, thus enabling informed strategic decisions and strengthening the organization's resilience to those inevitable threats and risk events.

It's also important for you to consider supporting robust employment agreements and clauses for this role. This protection not only provides peace of mind for the Chief Technology Risk Executive, but communicates your commitment to retaining top leadership, sharpening your competitive advantage, and form tighter alignment of the security program and corporate governance strategies overall.

I encourage ongoing board education on evolving cyber threats and technology risk management strategies (see NACD resources). A well-informed Board can make decisions that are more streamlined and focused on navigating potential risks and opportunities. Additionally, establishing a well-formed Technology Risk Management Framework overseen by a Chief Technology Risk Executive is essential. This framework should align with the overall strategic objectives and account for all risk aspects mentioned earlier. Furthermore, the Chief Technology Risk Executive should be involved in strategic planning sessions (e.g., M&A, new products, services, and markets) in order to proactively manage technology risks, rather than reactively mitigate damage.

These considerations serve to underline the strategic imperative of cybersecurity in today's digital landscape. Is your Risk Executive tactical, or strategic? Do they function as a Chief Technology Risk Executive? By facilitating direct risk reporting to the Board, reinforcing employment protection, promoting Board education, and ensuring strategic involvement, you take critical steps towards enhancing resilience against digital threats.

As you peruse this guide, I encourage you to use it as a tool for understanding your key partner in establishing the technology risk appetite, materiality thresholds, and identifying ways you can contribute to strengthening your organization's resilience.

We expertly navigate these challenges together, or not at all. I am confident this guide will help organizations take significant strides towards becoming more secure and resilient in the face of an ever-evolving digital threat landscape.

Liability

In the realm of Technology Risk Management career liability, the law does not hold Chief Information Security Officers (CISOs) and other technology risk leaders to a strict liability standard where they are considered guarantors of their companies' data security. Unlike traditional negligence claims where liability is linked to direct fault or negligence, strict liability goes beyond this paradigm. It pertains to industries where inherent risks exist, and those engaged in such activities can be held responsible for damage or injury, irrespective of their level of care or diligence.

However, in the context of Technology Risk and the cyber domain, strict liability may not apply to Risk Executives as they operate in a domain influenced by various external forces, cyber threats, and ever evolving technology landscapes. Conveying the understanding to stakeholders and juries that data security incidents can occur despite the best efforts of a Risk Executive - can present unique challenges. The responsibilities of Risk Executives are vast and complex, requiring them to proactively identify and manage technology risks, protect digital assets, meet diverse stakeholder demands, and advocate for organizational change – all at the same time. Partnership and a shared vision is key.

To protect themselves and their organizations, Risk Executives must also adopt strategic measures such as

- Well-crafted employment agreements defining the legal arrangement and obligations of each party,
- Insurance, and other financial protections in the event legal action is brought against the company and the Risk Executive,
- Professional execution to comply with legal and regulatory requirements, as well as alignment with industry standards,
- Robust risk management governance to demonstrate proactive efforts in mitigating threats.
- Risk Executives must professionally execute these requirements to best position themselves to defend against claims of negligence in the event of an incident.

By leveraging practical strategies, technology risk executives can strengthen their leadership effectiveness, protect themselves, and safeguard their organization.

Agreement Clauses

An Employment Agreement is a formal, legally binding contract that outlines the rights and responsibilities of both parties during the employment relationship. The purpose of the agreement is to establish clear expectations and legal protections, promote stability and compliance, set severance and termination conditions, and serve as the foundation for a clear and mutually beneficial employment relationship. Negotiating the key terms of employment agreements at the time of the offer can be advantageous as it allows both parties to secure favorable terms in addition to the compensation package of salary, bonus, benefits, working conditions, and other relevant details.

For incumbent Risk Executives, it may not be too late to enter into such an agreement. Suggesting alternative titles for the agreement may make it more approachable, such as a "CISO Retention Agreement" or "CISO Strategic Partnership Agreement.". In such cases, renegotiating or updating the agreement periodically can ensure it remains aligned with the evolving nature of both the Risk Executive's role and the needs and challenges of the organization.

Below are non-exhaustive considerations to be included in the Employment Agreement which in totality can reduce a Risk Executive's overall career risk exposure before, during, and after a data security incident:

1. Clearly Documented Role

Many Risk Executives lose their job because of a control failure for a system wholly outside of their control, or misalignment with the needs of the business. The Agreement should clarify the Risk Executive's authority to assess and report technology risk and to make recommended changes to the Information Security Program to minimize that risk. The Agreement should be clear that no single employee – including the Risk Executive – can be designated as responsible to prevent a breach. Have a specific job description included in your contract.

- **Job Description.** The Company should provide the Risk Executive with a clear and detailed job description, outlining the Risk Executive's responsibilities, duties, and expectations. The job description should be agreed upon by the Company and the Risk Executive and be an exhibit to the Agreement and incorporated therein.
    - **The Risk Executive should not "accept" risk above the board defined "risk appetite", as that is the function of the Board.** The Risk Executive's role is to measure, report, and advise the Board on options for risk treatment, and security measures available in the industry and marketplace. The Board and management can then determine whether to allocate resources accordingly. If the Board risk appetite is moderate, who can accept higher risk actions affecting the organization? All controls and risk mitigation options below the appetite are withing the authority of the Risk Executive to manage.
- **Operational Reporting Lines.** Who you report to is a critical consideration for Risk Executives managing significant risk for the company. The Risk Executive should be reporting to the CEO, or other appropriate level such that conflicts of interest are not present. Specifically, so that technology risk reporting is delivered without consideration if it might make other departments

"look bad." Further, budget decisions on personnel and program investments must be transparently delivered to the Board so they understand what risks may go untreated. If it won't be funded, it must be risk accepted.

a. **Relationship with Peers.** Include an explicit acknowledgment of who your peers are, your peers should be General Council, Head of Audit, and the CIO so their equity in decision making.

2. Direct Access to the Board

Securing a direct risk reporting line from the Risk Executive to the Board is mutually beneficial to remove barriers on reporting and assure transparency. Operational reporting can be defined based on the culture and structure of the company you serve. Be on the lookout for conflicts of interest where undue influence may impede accurate, truthful risk reporting.

- **Regular Updates.** The Board should receive regular updates from the Risk Executive on cybersecurity matters and the effectiveness of the Information Security Program and should be kept informed of significant technology risks and incidents in a timely manner.
- **Independence.** Management should not place any undue pressure or attempt to influence the Risk Executive in their reporting to the Board or take any retaliatory action against the Risk Executive for reporting technology risks or incidents to the Board or appropriate parties.
- **Direct Reporting.** The Company should provide the Risk Executive with direct access to the Chief Audit Executive, General Counsel, Chief Risk Officer, and/or appropriate Risk Oversight Committee to report on technology risks, reportable incidents, and trends.

3. Insurance Coverage

Legal suits not only name companies but increasingly target individuals to create divisions between employees and their employers or to trigger directors and officers liability insurance coverage. To safeguard against potential losses or expenses related to legal actions arising from alleged wrongful acts, it is essential to ensure that liability insurance covers Risk Executives throughout their tenure in the role, and after departure. The Company should be required to promptly provide the Risk Executive with a copy of each insurance policy identified below upon request and notify the Risk Executive of any material changes in coverage.

- **Director's and Officer's:** The Company should maintain D&O liability insurance coverage that includes the Risk Executive as an insured party, to the fullest extent permitted by law. The Risk Executive should be entitled to the benefits of such insurance coverage subject to the terms and conditions of the policy.
- **Error & Omissions:** In addition to D&O liability insurance, the Company should be required to ensure its Error & Omissions insurance coverage applies to any potential liability arising from the Risk Executive's professional services rendered in the course of their employment with the Company.
- **GAP Coverage:** If any insurance policy does not fully cover the Risk Executive's liability, or has exclusions in connection with any claims, damages, losses, liabilities, expenses, or settlements arising out of or in connection with the Risk Executive's employment with the Company, the

Company should provide gap coverage for any such liability. Such gap coverage should be subject to the terms and conditions of the policy and in an amount that is reasonable and customary for similar coverage for individuals in similar positions.

- **Organizational Cyber Insurance:** Because cyber is generally excluded from most D&O and E&O liability insurance, it is imperative that the Company maintain a robust Cyber Insurance policy. This policy is designed to safeguard the organization from severe financial losses resulting from cyber incidents, such as data exfiltration, business interruption, and network damage. A robust cyber insurance policy can aid in recovery by covering costs related to first-party damage, third-party claims, incident response, reputation management, ransom payments, and regulatory fines. The Company should ensure that the policy coverage extends adequately to cover potential risks and liabilities associated with the role.

4. Advancement of Legal Expenses

The Agreement should obligate the Company to pay legal fees during and after employment for any lawsuits arising or stemming from the Risk Executive's actions undertaken in the scope of their employment with the company. The company should pay for the Risk Executive's legal expenses directly to the legal counsel as they are incurred and be contractually liable for all fees. The Risk Executive should not be expected to advance their own legal fees and then wait until the end of a lawsuit or legal proceeding to be reimbursed. This can help to ensure that the Risk Executive has access to the necessary resources to defend themselves in legal proceedings related to their employment with the company.

- The Company should indemnify and hold harmless the Risk Executive from all claims, damages, losses, liabilities, expenses (including reasonable legal fees and expenses) and settlements arising out of or in connection with the Risk Executive's employment with the Company, to the fullest extent permitted by law.
- The Company should advance all reasonable legal expenses and fees incurred by the Risk Executive in defending any claim, action, or proceeding related to the Risk Executive's employment with the Company, subject to the Risk Executive's agreement to repay such advances if it is ultimately determined that the Risk Executive is not entitled to indemnification or acted in bad faith.
- The Risk Executive should maintain the right to choose their own legal counsel for their defense. This right should exist both during employment and following separation if the Risk Executive is named in any claim, action, or proceeding arising out of or within the Risk Executive's employment with the Company, subject to the Company's agreement that such legal expenses and fees are reasonable and customary.
- The Risk Executive should agree to cooperate with the Company in the defense of any such claim, action or proceeding. Invocation of this section may arise from the initiation of a government investigation, declaration of a data security incident, or a pending public data security incident notification.

5. Separation & Severance

A. TERMINATION FOR CAUSE

The language should define for cause including if conditions at the Company are such that the Risk Executive is constructively terminated, i.e., compelled to resign, with the contract tying compensation to a reason for the departure. When defining "cause," start with a definition of what is under your control and what is not. Possible reasons for "cause" are lack of accountability, questioned authority, or a material regulatory issue.

For purposes of this Agreement, 'cause' means the Risk Executive's material breach of this Agreement:

- material violation of the Company's policies, procedures, or regulations, including, without limitation, those related to cybersecurity,
- failure to perform duties or obligations in a professional manner,
- Notwithstanding the foregoing, if the Risk Executive's breach, violation, or failure is capable of being cured, the Company should provide written notice thereof to the Risk Executive and the Risk Executive should have 30 days from receipt of such notice to cure the breach, violation, or failure.
- If the breach, violation, or failure is not cured within such a 30-day period, it should constitute 'cause' for termination under this Agreement.

B. TERMINATION UNRELATED TO CAUSE

This provision outlines the conditions under which the Company may decide to terminate the Risk Executive's employment for reasons not related to cause.

Conditions for Termination by the Company: The Company may choose to terminate the Risk Executive's employment under the following circumstances:

- The Company decides to change its leadership or strategic direction, which does not involve any failure or wrongdoing on the part of the Risk Executive.
- The termination is not due to any cause, such as misconduct or failure to perform duties, as defined in this Agreement.

C. MUTUAL SEPARATION WITH ACCELERATED VESTING

This provision outlines the conditions under which a mutual separation agreement between the Risk Executive and the Company may be enacted. Conditions for Mutual Separation: The Risk Executive may choose to resign from their position under the following circumstances:

- The Company fails to allocate sufficient resources to address technology risk concerns raised by the Risk Executive and,
- The Risk Executive has made reasonable attempts to escalate these concerns to the Company's management and/or Board of Directors in writing and,
- The Company has been given a reasonable opportunity to address such concerns but has failed to do so.

D. EFFECT OF SEPARATION OR TERMINATION

Upon the Risk Executive's resignation under the conditions of Mutual Separation, or the Company's decision to terminate the Risk Executive's employment under the conditions of Termination by the Company, the Company should:

- Provide the Risk Executive with a severance package or mutual separation agreement, as applicable. This may include, but is not limited to, a continuation of salary for a specified period, a lump-sum payment, or a combination of both. One Year Salary or other specific terms.
- Ensure that the severance package or mutual separation agreement includes accelerated vesting of all outstanding equity and incentive compensation, including stock, stock options, and restricted stock that would have vested within a specified period following the date of separation or termination.
- Continue to provide any other benefits as outlined in this Agreement, such as health insurance, for a specified period following the separation or termination.

6. Limitations of Liability

The contract should include provisions that limit the employee's liability for any damages arising from a data security incident, if the employee was acting in good faith and in accordance with the company's cybersecurity policies and procedures.

- The Risk Executive should not be liable for any damages arising from a data security incident, if the Risk Executive acted in good faith and in accordance with the Company's cybersecurity policies and procedures. The Company should indemnify and hold harmless the Risk Executive from any claims, damages, losses, liabilities, expenses (including reasonable legal fees and expenses) and settlements arising out of or in connection with any data security incident, to the fullest extent permitted by law. This limitation of liability should survive the termination of the Risk Executive's employment with the Company.

7. Indemnification

Indemnification clauses in the Risk Executive's employment agreement serve the critical purpose of providing protection and financial security to the Risk Executive in the course of their employment with the Company in the event of a major data security incident. A comprehensive indemnification clause aims to instill confidence in the Risk Executive role, fostering a sense of security and allowing them to perform their duties diligently and fearlessly, even in the face of potential legal challenges stemming from government investigations or data security incidents.

- The Company should indemnify and hold harmless the Risk Executive from any and all claims, damages, losses, liabilities, expenses (including reasonable legal fees and expenses) and settlements arising out of or in connection with the Risk Executive's employment with the Company, to the fullest extent permitted by law.

The clauses below are additional, "nice-to-have" provisions, but are not as critical as clauses #1-#7.

8. Legal & Regulatory Compliance

Specifically, document accountability and responsibility as it relates to key, organizational specific requirements.

- The Risk Executive should be responsible and accountable for defining clear standards for and ensuring that the Company is made aware of its compliance status with applicable laws and regulations related to cybersecurity as advised by General Counsel or appropriate parties within the organization.
- The Risk Executive should have the authority to assess and report on compliance with these laws and regulations and should work with relevant stakeholders to implement corrective actions as necessary.
- The Risk Executive should be supported by General Counsel or appropriate 3rd party resources to remain up to date with changes to applicable laws and regulations (and/or evaluation of specific incidents) and is responsible for integration of those requirements into organizational policies and procedures to reflect those changes.
- The Company should provide the Risk Executive with the resources, support, and authority necessary to effectively manage compliance with applicable laws and regulations and should not take any retaliatory action against the Risk Executive for reporting non-compliance or refusing to engage in conduct that violates applicable laws and regulations.

9. Performance Measures

(SECTION MAY BE OMITTED IN LIEU OF THE COMPANY'S ESTABLISHED HR PROVISIONS)

Include language establishing clear performance measures and indicators to define what "good" performance is for the Risk Executive. SMART goals and KPIs are designed to assess the Risk Executive's effectiveness in properly managing technology risks, while the annual performance evaluation and performance improvement plan provisions are designed to ensure ongoing monitoring and improvement of the Risk Executive's performance.

Performance Objectives: The Company should establish clear performance objectives and targets for the Risk Executive, which should be agreed upon by the Company and the Risk Executive. The performance objectives and targets should be specific, measurable, achievable, relevant, and time-bound (SMART), and should be designed to assess the Risk Executive's effectiveness in managing technology risks.

Performance Indicators: The performance objectives and targets should be based on key performance indicators (KPIs) that reflect the Company's technology risk management priorities. The KPIs should be reviewed and updated annually, and should be designed to assess the Risk Executive's performance in key areas, such as:

- Control Effectiveness improvements over time
- Maturation of the Technology Risk Program
- Compliance with applicable laws and regulations
- Appropriate response to security incidents according to plans

Performance Evaluation: The Risk Executive's performance should be evaluated against the performance objectives and targets on an annual basis. The evaluation should be based on a review of the Risk Executive's performance against the established KPIs, as well as the Risk Executive's overall contribution to the Company's cybersecurity risk management efforts.

Performance Improvement: If the Risk Executive's performance is found to be below the established performance objectives and targets, the Company should work with the Risk Executive to develop and implement a performance improvement plan (PIP) that outlines specific actions to be taken to improve the Risk Executive's performance. The PIP should be agreed upon by the Company and the Risk Executive and should be reviewed and updated regularly.

10. Professional Development and Association Dues

In the fast-paced and complex domain of technology risk, continuous professional development is paramount. To foster innovation and resilience, organizations must prioritize and financially support the ongoing growth of their Risk Executive. This commitment should encompass access to relevant training, seminars, conferences, industry workshops, professional association memberships, and certification renewals. Such an investment not only enhances the executive's skill set and understanding of emerging threats and regulations but also fortifies the organization's overall stance on technology risk management. By covering the associated costs and dues, an organization is making a strategic investment in its leadership and reinforcing a robust approach to informed technology risk management.

Professional Development: The Company recognizes the value of continuous professional development and commits to support the Employee in these endeavors. This includes, but is not limited to, opportunities for the Employee to participate in relevant training courses, seminars, conferences, and industry workshops. The Company should reimburse reasonable costs associated with these activities, subject to prior approval and in accordance with Company policies.

Association Membership Dues: The Company should cover the annual dues for the Employee's membership in professional associations relevant to their role as Chief Technology Risk Executive. This commitment is predicated on the understanding that such memberships provide valuable opportunities for networking, professional development, and staying current with industry trends and standards.

Certification Renewals and Continuing Education: If the Employee holds professional certifications requiring renewal and continued education, the Company agrees to cover the cost of renewal fees. The Company also acknowledges that achieving the necessary continuing education credits may require time for study or examination. As such, the Company will provide a reasonable amount of paid time off for the Employee to fulfill these requirements.

11. Outside Activities

This provision allows the Risk Executive to engage in outside activities as long as they do not interfere with their duties and obligations to the Company or create a conflict of interest. The provision requires the Risk Executive to promptly notify the Company of any such outside activities and prohibits the Risk Executive from engaging in any activities that may be harmful to the Company's interests. It also allows the Company to require the Risk Executive to terminate or modify any outside activities that create a conflict of interest or otherwise interfere with the Risk Executive's duties and obligations to the Company.

The Risk Executive may engage in outside activities, including but not limited to serving on advisory boards, consulting, or teaching, provided that such activities do not interfere with the Risk Executive's duties and obligations to the Company or create a conflict of interest.

The Risk Executive should promptly notify the Company of any such outside activities and should not engage in any such activities that may be harmful to the Company's interests.

The Company may require the Risk Executive to terminate or modify any such outside activities if the Company determines that such activities create an actual or perceived conflict of interest or otherwise interfere with the Risk Executive's duties and obligations to the Company.

Intellectual Property rights are retained by the Risk Executive for any property developed not created for the benefit of the Company.

12. Dispute resolution

These provisions can establish a mechanism for resolving any disputes that arise between the company and the Risk Executive, such as through arbitration or mediation, rather than through litigation in court.

a. In the event of any dispute arising out of or related to this employment agreement, including but not limited to any claims arising out of or related to the Risk Executive's employment, termination of employment, or compensation, the parties agree to first attempt to resolve the dispute through good faith negotiations. If the dispute cannot be resolved through negotiations within a reasonable period of time, the parties agree to submit the dispute to binding arbitration in accordance with the rules of the American Arbitration Association.

Technology Risk Governance

Incumbents in the Risk Executive role should establish and enhance organizational Technology Risk Governance and Response Plans. By championing the formation of Key Policies, Standards, Programs, and Committee Structures into place, the accountability for Technology Risk can be more precisely defined and shared with key stakeholders in the organization. This can help to reduce the likelihood of misunderstandings, disagreements, or disputes later. These policies can also provide the Risk Executive with a clear framework for managing technology risks and incidents and can help to establish the Risk Executive's role as a key stakeholder but not solely accountable for Technology Risk Management decisions.

1. Information Security Policy: Provides a framework for the Risk Executive to establish, implement, and govern the organization's information security program. By outlining the Risk Executive's responsibilities and authorities related to technology risk management, and its execution, It empowers the Risk Executive to effectively manage risks, ensure compliance, establish committees/working groups, and foster a culture of security across the organization. The policies should establish the Risk Executive's role as the primary point of contact for technology risks and security incidents and can also contain a RACI or other outline of responsibilities of your key stakeholders (GC, HR, Legal, CIO, Board, etc.)

2. Written Information Security Program: A comprehensive written information security program should be developed that clearly enumerates and defines an organization's Management Control Programs and reporting processes (i.e., Asset Management, Patch & Vulnerability Management, Access Management, Vendor Management, Security Operations, Risk Management, etc.)

> **2.1. Management Control Programs:** MCPs define the attributes and relationships between key resources (People, Processes, and Technologies) and the processes used to achieve Key Control Objectives and service outcomes. The reporting and KRI measures should also be enumerated. Each MCP should have a corresponding Standard.

3. Crisis Management Plan: Define a team of Technology, Legal, Compliance, Risk and Technology executives to review and decide actions to be taken in the event of a crisis. This includes 3rd party notifications (Law Enforcement, Regulators, Customers, etc.), and additional documentation processes. This will help the Risk Executive guide incident response teams, facilitate decision-making processes, collaborate with internal and external parties, and mitigate the impact of security incidents. The plan serves as a vital tool for the Risk Executive to safeguard the organization's assets, maintain business continuity, and protect the organization's reputation in the face of adversity.

4. Incident Response Plan: An incident response plan should be developed that outlines the response team, and their roles in responding to cybersecurity incidents. Specific steps to take, and conditions for invocation of the crisis management plan or declaration of a Breach. The plan should establish the process to investigate and respond to incidents with the aim of restoration to normal operations as the key goal.

> 4.1. It should require an Incident Response (IR) Retainer with security response firms, and outside IR counsel for legal support.

4.2. Include steps for escalating breaches / major incidents to executive management, and the Board of Directors as necessary. Include external stakeholder notice requirements (IR provider, Outside Counsel, Law Enforcement, Regulators, Insurance, etc.)

5. Technology Risk Management Policy: A risk management policy should be developed that outlines the Risk Executive's role in Identifying and Reporting on technology risks. The policy should establish the Risk Executive's authority to assess and prioritize technology risks and should provide objectives for implementing risk mitigation measures (controls).

5.1. Materiality and Risk Appetite: Through policy - The Board must establish a Technology/ Cyber Risk Appetite and define a Materiality threshold which will trigger escalations to the Board (typically a dollar threshold/cost that is intolerable for a Risk Event). The Risk Executive/ Management should not be authorized to "Risk Accept" any risk above the Board's Risk Appetite, forcing notification and collaboration with the Board or Board Committee.

5.2. Technology Risk Oversight Committee: Establish a dedicated Technology Risk Committee comprising key stakeholders, such as the CISO/CSO, Chief Information Officer (CIO), Chief Risk Officer (CRO), General Counsel, Audit, and representatives from Key business units. This committee should oversee and review technology risk matters, especially in support of any 10-K/Q filing for public companies.

6. Compliance Policy: A compliance policy should be developed that outlines the Risk Executive's role in ensuring compliance with applicable laws, regulations, and industry standards related to cybersecurity. The policy should establish the duties of General Counsel or other party to monitor regulatory changes, and the Risk Executive's authority to assess and report on compliance of those identified applicable requirements and provide guidelines for implementing corrective actions as necessary.

7. Privacy Policy: A privacy policy should be established to outline the organization's commitment to protecting personal and sensitive data. The policy should define the Risk Executive's role in safeguarding privacy and ensuring compliance with relevant privacy laws and regulations. It should provide guidelines for handling, storing, and sharing personal information, as well as procedures for responding to privacy incidents and managing data subject rights requests. The Risk Executive should collaborate with legal and compliance teams to develop and implement privacy policies and procedures that align with applicable privacy requirements.

8. Public Filings and SEC Reporting (10K/10Q) Considerations: Ensure that 10K/Q filings do not contain misrepresentations of technology risks. This requires adequate stakeholder engagement for signoffs on Technology Risk matters. Consider:

8.1. Risk Assessment Process: A robust risk assessment process is essential for identifying and evaluating potential technological threats and vulnerabilities aligned with section 5 above. This process should be reflected in your company's 10K/10Q filings, demonstrating to the SEC and investors that your organization is proactive in managing cybersecurity risks. This process should involve conducting regular technology risk assessments, identifying threats, potential vulnerabilities, and assessing control effectiveness, residual risk, and determining appropriate risk mitigation strategies.

8.2. Technology Risk Reporting: Develop a standardized reporting mechanism for technology risks. The Risk Executive should provide regular reports to the Technology Risk Committees and Board, highlighting significant technology risks, their potential impact, and the effectiveness of existing controls. This reporting should be based on objective data and include both quantitative and qualitative analysis. These drive Specific Statements to be made in the filing.

8.2.1. Public companies are required to disclose their cybersecurity risk management, strategy, and governance in their filings.

8.2.2. Companies must **notify the SEC and the public within four days of determining that a cybersecurity incident will have a "material" impact on their operations.** This includes information on the nature, scope, and timing of the incident, as well as the likely material impact on the company's financial conditions and operations.

8.3. Independent Audit and Review: Engage an independent third-party auditor or an internal audit function to conduct periodic reviews of the technology risk management processes and controls. This audit should assess the accuracy and completeness of technology risk disclosures and evaluate the effectiveness of risk mitigation measures.

8.4. Documentation and Sign-Off: Implement a process for documenting and obtaining sign-off on technology risk matters. This should involve multiple signatories, including the CISO/CSO, CIO, CRO, and General Counsel. The Technology Risk Committee should review and approve the final disclosures related to technology risks.

8.5. Continuous Improvement: Establish a culture of continuous improvement by conducting post-mortem reviews of any incidents or breaches that occur. These reviews should identify lessons learned, assess the effectiveness of risk management strategies, and inform updates to the technology risk management process.

Appendix: Agreement Guide

Before signing anything confer with qualified legal counsel. The Agreement below is aspirational and merely a guide of what you should look for in a CISO/Risk Executive Agreement as you confer with counsel.

Certain states have specific requirements for the language and placement of indemnification provisions in employment contracts. For example, in **California**, an indemnification provision in an employment contract must be presented in boldface type or in conspicuous typeface and must be initialed or signed by the employee. Other states, such as **New York and Delaware**, also have specific requirements for the language and placement of indemnification provisions in employment contracts.

It is important to consult with a labor and employment contract lawyer who is familiar with the laws and regulations of the state(s) where the contract will be executed to ensure that the indemnification provision is drafted in compliance with state law. The lawyer can advise on the specific language and placement requirements for the indemnification provision, as well as other provisions of the employment contract, to ensure that they are enforceable and provide adequate protection for the Risk Executive.

This Employment Agreement ("Agreement") is made and entered into by and between [Company Name], a [State of Incorporation] corporation, ("Company") and [CISO Name] ("CISO") (collectively referred to as "Parties").

WHEREAS, the Company desires to employ CISO to provide services to Company in the capacity of Chief Information Security Officer ("CISO").

WHEREAS, CISO desires to accept employment with Company and to provide services in the capacity of CISO.

NOW, THEREFORE, the Parties agree as follows:

EMPLOYMENT

The Company hereby employs CISO, and CISO hereby accepts employment with the Company, on the terms and conditions set forth in this Agreement.

JOB DESCRIPTION

The Company shall provide the CISO with a clear and detailed job description, outlining the CISO's responsibilities, duties, and expectations. The job description shall be agreed upon by the Company and the CISO and shall be attached to this Agreement.

ACCESS TO BOARD AND KEY STAKEHOLDERS

The Company shall provide the CISO with direct access to the Chief Audit Executive, General Counsel, Chief Risk Officer, and/or appropriate Board Risk Oversight Committee for the purpose of reporting on technology risks, reportable incidents, and trends. The Board shall receive regular updates from the CISO on cybersecurity matters, the effectiveness of the Information Security Program, and shall be kept informed of significant risks and incidents in a timely manner. In addition, Management agrees not to place any undue pressure or attempt to influence the CISO in their reporting to the Board and shall not take any retaliatory action against the CISO for reporting technology risks or incidents to the Board or appropriate parties.

COMPLIANCE

The CISO shall be responsible and accountable for defining clear standards for, and ensuring that the Company is made aware of its compliance status with, applicable laws and regulations related to cybersecurity as advised by General Counsel or appropriate parties within the organization. The CISO shall have the authority to assess and report on compliance with these laws and regulations and shall work with relevant stakeholders to implement corrective actions as necessary. The CISO shall be supported by General Counsel or appropriate 3rd party resources and counsel to remain up to date with changes to applicable laws and regulations (and/or evaluation of specific incidents) and is responsible for integration of those requirements into organizational policies and procedures to reflect those changes. The Company shall provide the CISO with the resources, support, and authority necessary to effectively manage compliance with applicable laws and regulations and shall not take any retaliatory action against the CISO for reporting non-compliance or refusing to engage in conduct that violates applicable laws and regulations.

PERFORMANCE

The Company shall establish clear performance objectives and targets for the CISO, which shall be agreed upon by the Company and the CISO. The performance objectives and targets shall be specific, measurable, achievable, relevant, and time-bound (SMART), and shall be designed to assess the CISO's effectiveness in managing cybersecurity risks.

Performance Indicators: The performance objectives and targets shall be based on key performance indicators (KPIs) that reflect the Company's cybersecurity risk management priorities. The KPIs shall be reviewed and updated annually and shall be designed to assess the CISO's performance in key areas, such as reduction of cybersecurity incidents, implementation of effective, testable security controls, compliance with applicable laws and regulations, appropriate response to security incidents, and collaboration with internal and external stakeholders.

Performance Evaluation: The CISO's performance shall be evaluated against the performance objectives and targets on an annual basis. The evaluation shall be based on a review of the CISO's performance against the established KPIs, as well as the CISO's overall contribution to the Company's cybersecurity risk management efforts.

Performance Improvement: If the CISO's performance is found to be below the established performance objectives and targets, the Company shall work with the CISO to develop and implement a performance improvement plan (PIP) that outlines specific actions to be taken to improve the CISO's performance. The PIP shall be agreed upon by the Company and the CISO and shall be reviewed and updated regularly.

LIMITATIONS OF LIABILITY

The CISO shall not be liable for any damages arising from a data security incident, as long as the CISO acted in good faith and in accordance with the Company's cybersecurity policies and procedures. The Company shall indemnify and hold harmless the CISO from any claims, damages, losses, liabilities, expenses (including reasonable legal fees and expenses) and settlements arising out of or in connection with any data security incident, to the fullest extent permitted by law. This limitation of liability shall survive the termination of the CISO's employment with the Company.

INDEMNIFICATION

The Company shall indemnify and hold harmless the CISO from any and all claims, damages, losses, liabilities, expenses (including reasonable legal fees and expenses) and settlements arising out of or in connection with the CISO's employment with the Company, to the fullest extent permitted by law. The Company shall maintain Director's & Officer's (D&O), and Errors and Omissions (E&O) liability insurance coverage that includes the CISO as an insured party, to the fullest extent permitted by law. The CISO shall be entitled to the benefits of such insurance coverage, subject to the terms and conditions of the policy. The Company shall promptly provide the CISO with a copy of the D&O liability insurance policy upon request, or notify of any changes.

In the event that the liability insurance policy does not fully cover the CISO's liability, or has exclusions in connection with any claims, damages, losses, liabilities, expenses, or settlements arising out of or in connection with the CISO's employment with the Company, the Company shall provide gap coverage for any such liability. Such gap coverage shall be subject to the terms and conditions of the policy and shall be in an amount that is reasonable and customary for similar coverage for individuals in similar positions.

The Company shall advance all reasonable legal expenses and fees incurred by the CISO in defending any claim, action or proceeding related to the CISO's employment with the Company, subject to the CISO's agreement to repay such advances if it is ultimately determined that the CISO is not entitled to indemnification. In addition, the Company shall pay for independent legal representation of the CISO's choice to defend the CISO personally, both during employment and following separation, in the event that the CISO is named in any claim, action or proceeding arising out of or in connection with the CISO's employment with the Company, subject to the Company's agreement that such legal expenses and fees are reasonable and customary. The CISO shall cooperate with the Company in the defense of any such claim, action or proceeding. Invocation of this section may arise from the initiation of a government investigation, declaration of a data security incident, or a pending public data security incident notification.

TERMINATION

For purposes of this Agreement, 'cause' shall mean the CISO's material breach of this Agreement: i. material violation of the Company's policies, procedures, or regulations, including without limitation those related to cybersecurity, ii. failure to perform duties or obligations in a competent and professional manner, iii. including lack of accountability or questioned authority, or any regulatory action or proceeding against the CISO or the Company that would materially and adversely affect the Company's business or reputation. Notwithstanding the foregoing, if the CISO's breach, violation, or failure is capable of being cured, the Company shall provide written notice thereof to the CISO and the CISO shall have 30 days from receipt of such notice to cure the breach, violation, or failure. If the breach, violation, or failure is not cured within such a 30-day period, it shall constitute 'cause' for termination under this Agreement.

In the event that the CISO resigns from employment with the Company due to the Company's failure to fund or address technology risk concerns raised by the CISO, and the CISO has attempted to escalate such concerns to the Company's management and/or Board of Directors in writing, and has given the Company a reasonable opportunity to address such concerns, the Company shall provide the CISO with a mutual separation agreement that includes accelerated vesting of all outstanding stock, stock options, restricted stock or other incentive compensation that would have vested within 12 months following the date of separation if the CISO had remained employed by the Company during such period. The mutual separation agreement shall include all other protections set forth in this Agreement, including without limitation the indemnification and advancement of legal expenses provisions.

OUTSIDE ACTIVITIES

The CISO may engage in outside activities, including but not limited to serving on advisory boards, consulting, or teaching, provided that such activities do not interfere with the CISO's duties and obligations to the Company or create a conflict of interest. The CISO shall promptly notify the Company of any such outside activities and shall not engage in any such activities that may be harmful to the Company's interests. The Company may require the CISO to terminate or modify any such outside activities if the Company determines, in its sole discretion, that such activities create a conflict of interest or otherwise interfere with the CISO's duties and obligations to the Company.

DISPUTE RESOLUTION

In the event of any dispute arising out of or related to this employment agreement, including but not limited to any claims arising out of or related to the CISO's employment, termination of employment, or compensation, the parties agree to first attempt to resolve the dispute through good faith negotiations. If the dispute cannot be resolved through negotiations within a reasonable period of time, the parties agree to submit the dispute to binding arbitration in accordance with the rules of the American Arbitration Association.

This Agreement represents the entire understanding of the parties with respect to the employment of the CISO and supersedes all prior negotiations, discussions, and understandings. This Agreement may not be amended or modified except in writing signed by both the Company and the CISO. This Agreement shall be binding upon and inure to the benefit of the parties hereto, their respective heirs, executors, administrators, successors, and assigns. This Agreement shall be governed by and construed in accordance with the laws of the jurisdiction in which the Company is located.

IN WITNESS WHEREOF, the parties have executed this Agreement as of the date and year first above written.

[Insert Company Name]

By: _____

Title: _____

Date: _____

[Insert Name]

By: _____

Date: _____