



IV. Organization, Format, and Content of Proposal

Please provide responses to the following questions. Responses will be evaluated, in part, on an organization's ability to communicate clearly and succinctly.

4.1 PROPOSAL SUMMARY

Each proposal shall provide a narrative summary of the proposal being submitted. This summary should identify all of the services and work products that are being offered in the proposal and should demonstrate the firm's understanding of the project.

CFGI has reviewed this Request for Proposal and the associated *Section II. Scope of Audit*, as summarized below:

Purpose: CFGI will critically evaluate the risk review, control procedures, and information technology operations of the Ohio Highway Patrol Retirement System (HPRS). CFGI will identify areas of strengths and weaknesses of the HPRS, compare its operations with the best practices of similar organizations, and make recommendations for improvement.

Deliverables: CFGI will provide monthly updates to the HPRS (at a minimum). We will submit a draft report to the HPRS, and to any other designated party, for comments. The final report will include a description of the work performed; an executive summary; findings and recommendations; and specific, concrete proposals to achieve any improvements recommended in the report.

We acknowledge the elements listed in the *Scope of Audit* and confirm CFGI's ability and experience to perform each of the listed elements below. We are in partnership with the experts at RVK, who will address the elements not covered by CFGI's scope. We outline below the key items reflective of the core services of this RFP and the key professionals responsible for leading them:

1. Board Governance and Administration - covered by the experts at RVK
2. Organizational Structure and Staffing - covered by the experts at RVK
3. Investment Policy and Oversight - covered by the experts at RVK
4. Legal Compliance - covered by the experts at RVK
5. Risk Management and Controls – Elaina Coletta, Managing Director, Lead
6. Information Technology Operations – Xavier Sanchez, Managing Director, Lead

CFGI, has a Risk Advisory practice specializing in Enterprise Risk Management, internal controls, IT compliance and IT operations. The proposed leads are Managing Directors in CFGI's Risk Advisory practice. Elaina Coletta has extensive experience in assessing and helping organizations with Risk Management and the development of Internal Control programs. Xavier Sanchez has led numerous engagements assessing and evaluating IT operations and controls.

In addition to the summary, please provide all of the following general information:

- **The firm's primary contact for ORSC staff use and, if different, for HPRS staff use during the audit, including the contact's address, telephone and e-mail address;**



We are proposing the following two professionals to serve as co-leads for this important opportunity.

Elaina Coletta – Managing Director
Role: Risk Management and Controls Lead
340 Madison Ave, FL3
New York, NY 10173
617.875.2554
ecoletta@cfgi.com

Xavier Sanchez - Managing Director
Role: IT Operations Lead
340 Madison Ave, FL3
New York, NY 10173
203.610.2869
xsanchez@cfgi.com

As the Risk Management and Controls Lead, Elaina will be responsible for the work completed by CFGI in this area, coordinating with RVK, and providing ORSC periodic updates.

As the IT Operations Lead, Xavier will be responsible for the work completed by CFGI in this area, coordinating with RVK and providing ORSC periodic updates.

- **General ownership structure of the organization, including subsidiary and affiliated companies, and joint venture relationships;**

CFGI is a standard Corp, with a holding company, US Corp, and UK Corp. The firm is owned 33% by the Carlyle Group and 33% by CVC Capital Partners, and the firm's managing partners hold the remaining ownership. All of the work to be performed by CFGI will be under the CFGI LLC, the US Corp.

- **Information regarding any material change in the firm's structure or ownership within the last eighteen months, or any material change in ownership, staff, or structure currently under review or being contemplated by the firm;**

CVC Capital Partners, acquired its 33% stake in 2021.

- **If available, a third-party assessment or report concerning client satisfaction and measures of the firm's strengths and weaknesses;**

Not applicable - CFGI is not an independent accounting firm that is subject to third-party assessments.

- **Any material litigation which has been threatened against the firm or to which the firm is currently a party;**

No material litigations have been threatened nor is the firm currently a party in any litigations.

- **A list and brief description of litigation brought against the firm by existing or former clients over the last five years; and**

During 2020, the firm was named as part of a bankruptcy filing regarding a former client Starworks, LLC. The client engaged CFGI to perform accounting advisory services, specifically assuming various interim finance and accounting roles on behalf of Starworks' management team. This is a standard co-source

engagement with an accounting advisory client and how CFGI structures the majority of its projects. It is important to note that there were 30 additional defendants named in the litigation proceedings. The filing has since been settled and CFGI was required to payout an immaterial amount to the counterparty.

- **A list of any professional relationships involving the ORSC, the five Ohio public retirement systems, the State of Ohio, or its political subdivisions for the past five years, together with a statement explaining why such relationships do not constitute years, together with a statement explaining why such relationships do not constitute a conflict of interest relative to performing the proposed review. In the event that the firm has had any professional relationships involving the ORSC, the five Ohio public retirement systems, the State of Ohio, or its political subdivisions for the past five years, the firm shall provide a statement explaining why such relationships do not constitute a conflict of interest relative to performing the proposed review, or, if necessary, an explanation of the actions that will be taken to ensure an independent review. Note that any media or social media comments opining on HPRS as an organization, whether positive or negative, may be viewed as pre-judgement of the system and result in disqualification. The firm must also disclose any staff relationships with other entities that evaluate pension systems and include a statement explaining why such relationships do not prevent an independent analysis or, if necessary, an explanation of the actions that will be taken to ensure an independent review.**

CFGI does not currently or has had in the past five years any professional relationships involving the ORSC, the five Ohio public retirement systems, the State of Ohio, or its political subdivisions for the past five years.

4.2 CAPABILITIES AND EXPERIENCE

Each proposal shall describe the firm’s capabilities and recent experience (at least during the last five years) in performing fiduciary audits or studies of public employee retirement systems. The firm should include information on the types and sizes of public employee retirement systems for which past work has been performed, including whether the systems were defined benefit or defined contribution plans, the types and number of participating employers, number of participants, and other relevant indicators of plan type, size, and comparability to HPRS. You may provide a sampling or summary description of the scope of these projects and non-proprietary key findings and recommendations. Sampling of work should be incorporated in the report as an appendix or attachment rather than a web citation. You should include other information you believe may be relevant in demonstrating your capabilities in performing the fiduciary audit, including other professional experience and data processing capabilities. Please include the firm’s experience and capability regarding all of the following:

CFGI is an established leader in accounting advisory services providing technical accounting and operational finance expertise to clients. The Firm was built with the highest quality professionals who are innovative, passionate and work alongside our clients to solve their most complex and critical finance, tax and accounting issues.

Our significant experience servicing the needs of CFOs (Finance), CIOs, CTOs, CISOs (IT), and the CAE (IA) across various industries allows us to assess the control environment against best practices to drive continuous improvement.

CFGI's Risk Advisory practice brings a pragmatic and cost-considerate approach to today's governance, risk, and compliance challenges with a "strategy-first" mindset. We are laser-focused on delivering positive change and meaningful results in the specific areas of need most important to the client and its key stakeholders.

Our Risk Advisory team consists of approximately 95 individuals, all with Big Four backgrounds. Because we do not provide attestation services, we are always independent and free to perform the services you need when you need them. Our Risk Advisory professionals are also 100% dedicated to our practice and service offerings.

Our core competitive strengths position us ahead of our competitors in the industry:

- Operational Risk Management experience ensures our recommendations and enhancements reflect the maturity, trajectory, and corporate culture expectations of our clients.
- Internal Audit experience allows us to simultaneously identify non-financial risk mitigation opportunities.
- External auditor coordination allows us to get ahead of "hot topic" areas.
- Incorporation of IT considerations and other subject matter expertise (e.g., Tax) facilitates delivery of a unified and comprehensive approach to financial risk assessment.
- Continuous collaboration results in ongoing communication.
- Operating as a member of Management ensures business changes impacting the control environment are readily identified and addressed.
- Provides deep expertise in cybersecurity and data privacy, enabling a comprehensive audit universe despite severe talent shortages in these areas.

As a non-audit accounting advisory firm, CFGI's Risk Advisory practice will be responsible for evaluating the adequacy of HPRS' financial controls, current accounting process, and recordkeeping system; the integrity of their financial statements and reports provided to the Board; and the sufficiency of internal and external audit processes. We perform the major deliverables described below:

1. Risk Assessment and Scoping - CFGI professionals, with broad experience in internal controls, financial reporting and financial operations, assist clients with all phases of the planning and scoping of the internal control assessment.
2. Walkthrough, Control Matrices, and Narratives/Flowcharts - Robust documentation of key processes is a vital first step in assessing the effectiveness of a company's control environment. CFGI assists clients with documentation of all financial processes for companies in all industries.
3. Gap Identification and Remediation Plan - CFGI assists clients in all phases of the assessment of control design and operating effectiveness.
4. Reporting to Management and Executive Committees - CFGI drafts and presents recommendations and executive-level presentations providing guidance and methodology that is tailored to the unique needs of the client and scope of the project.

4.3 STAFF QUALIFICATIONS

Each proposal shall, at a minimum, describe the qualifications of all management and lead professional personnel who will participate in the fiduciary audit. Each personnel description shall include: (1) a resume; (2) a summary of experience each has had in performing fiduciary audits or studies of public

employee retirement systems; and (3) a management plan identifying the responsibilities each will have on the audit. The firm must also disclose any staff relationships with other entities that evaluate pension systems and include a statement explaining why such relationships do not prevent an independent analysis or, if necessary, an explanation of the actions that will be taken to ensure an independent review. Each proposal shall also include a description of the firm’s procedures in the event that a key person assigned to this engagement leaves the firm during the engagement.

Services for the fiduciary audit of HPRS will be led by Elaina Coletta, CPA, and Xavier Sanchez, CPA—two risk advisory consulting professionals with nearly 30 years of combined consulting and risk advisory experience across various industries and client types. The two CFGI co-leads, and their respective roles, are described below.

- As co-lead of our firm’s NYC Risk Advisory practice, Elaina Coletta, CPA, has extensive experience conducting the services outlined in this RFP. She has served (or is currently serving) as a key member for similar assignments. Elaina has assumed various roles across her Risk Advisory clients, including Director of Internal Audit and ICFR Program Lead as well as subject matter expert and liaise for management (CFOs/Controllers) regarding all technical matters related to risk management of financial reporting. Her engagements typically entail performing risk and scoping assessments, designing and testing controls, educating control owners on execution best practices, and reporting to management and the Audit Committee. Elaina has extensive experience working closely with all key stakeholders to ensure the internal control program meets the client’s objectives and goals.
- As co-lead of our firm’s NYC Risk Advisory practice, Xavier Sanchez, CPA, has extensive experience conducting the services outlined in this RFP. He specializes in Information Technology audits and the application of IT audit standards. He has served (or is currently serving) as a key member for similar assignments. Xavier has led numerous SOX and Internal Audit engagements for clients ranging from start-ups to Fortune 500 companies throughout his career at CFGI. He focuses on providing his clients with solutions to build strong, efficient internal control systems and practices that support their strategic objectives. Xavier has extensive experience assessing IT systems with varying infrastructures (on-prem, hosted, and cloud). He has direct experience with Microsoft Dynamics, NetSuite, Oracle Fusion and SAP.

Each resume should include information on the current and past positions held with the firm, educational background, relevant credentials, and other relevant information to demonstrate the person’s qualifications.

Please refer to Page 14 for our proposed team lead bios.

The experience summaries should include information on the types and sizes of public employee retirement systems for which the designated staff have completed work, including whether the systems were defined benefit or defined contribution plans, the types and number of participating employers, number of participants, and other relevant indicators of plan type, size, and comparability to HPRS. You may reference, rather than repeat, duplicative information provided in paragraph 4.2, Capabilities and Experience. The experience summaries also should describe the work performed and detail the roles and responsibilities that the individual staff had on the projects.



The following examples detail the type of projects we have conducted within the past two years relevant to this mandate. We believe these are indicative and representative of our vast experience in this arena.

- CFGI has been engaged by hundreds of clients to perform risk advisory services. A short list of these clients is summarized below:
 - CFGI was engaged by a billion-dollar funded government agency construction project to assist with the development of an Internal Audit, Risk and Compliance function. CFGI was initially engaged with the project in 2020 and over the course of two years has established a corporate governance structure, drafted best practice policies and procedures, developed an enterprise risk methodology and program, conducted an annual internal audit plan and executed upon the establishment of the plan, and created a contract reporting process to ensure the agency was compliant with all laws and regulations.
 - CFGI has extensive experience in the Information Technology Risk space. In 2021, the firm was engaged by a life sciences company that produces, distributes, and sells protein research tools for cancer studies with \$300M in revenue annually. The CFGI IT subject matter experts were responsible for the development of an audit plan specifically around user access, change management, computer operations, and entity level controls. This effort required an extensive scoping and risk assessment exercise for all IT applications and systems. The client has numerous proprietary systems that were lacking the proper infrastructure and controls in order to ensure the financial data and reporting was complete and accurate. Over the course of a year, the IT specialists have developed and formalized policies and processes across all systems, tracked and monitored recurring deficiencies, and assisted management with remediation activities in order to lift the material weakness in the control environment.
 - CFGI is engaged by a health insurance company with approximately \$1.7 billion in assets and a recent IPO in 2021. The firm has managed the Internal Control over Financial Reporting (ICFR) implementation project for the past two years. Key tasks include coordination with the various business owners as well as other stakeholders in the process, e.g., conducting walkthroughs, coordinating all phases of internal control testing as well as reliance with external auditor requirements to ensure high standards of quality documentation are met. The material business cycles for this client include Investments, Treasury, Insurance and Actuarial reserves, including claims, premiums, etc.

The management plan should specify the roles and responsibilities that each of the management and professional staff will have on the fiduciary audit and include an estimated portion of the audit’s time that will be spent by each on the audit and the individual’s hourly billable rate.

CFGI Professional/ Title	Role	Responsibility	Hours Devoted to ORSC	Hourly Billable Rate
Elaina Coletta, CPA Managing Director Finance Risk Advisory	Co-Lead Consultant	Serve as the Finance Risk Advisory Executive Lead tasked with the overall project management of the engagement, strategic direction, and presenting the final	131	\$240

		report in person to both ORSC and HPRS Board of Trustees.		
Xavier Sanchez, CPA Managing Director IT Risk Advisory	Co-Lead Consultant	Serve as the Finance IT Advisory Executive Lead tasked with the overall project management of the engagement, strategic direction, and presenting the final report in person to both ORSC and HPRS Board of Trustees.	110	\$240
Senior Manager, Finance Risk Advisory	Project Lead Consultant	Serve as the Finance Risk Advisory Project Lead tasked with the day-to-day project management of the engagement, and creation and completion of the overall project plan.	328	\$215
Senior Manager, IT Risk Advisory	Project Lead Consultant	Serve as the Finance IT Advisory Project Lead tasked with the day-to-day project management of the engagement, and creation and completion of the overall project plan.	124	\$215
Consultant, Finance Risk Advisory	Delivery Consultant	Serve as the Finance Risk Advisory Delivery Consultant tasked with the day-to-day execution of the deliverables and overall project plan.	289	\$145
Consultant, IT Risk Advisory	Delivery Consultant	Serve as the IT Risk Advisory Delivery Consultant tasked with the day-to-day execution of the deliverables and overall project plan.	326	\$145

Lead professionals included on the project team should, at a minimum, have performed a fiduciary audit or study of a public employee retirement system within the last two years.



Our proposed Engagement Managers and Co-Lead Consultants, Elaina Coletta, CPA, and Xavier Sanchez, CPA, have completed combined more than twenty projects with similar mandates in the risk management and IT operations space within the last two years.

Each proposal shall include the firm’s affiliations with organizations that sponsor and support investment or fiduciary related research.

CFGI is a portfolio company of the Carlyle Group and CVC Capital Partners, 66% owned by these Private Equity Firms and 34% owned by the Partners. There are no affiliates or parent companies.

4.4 REFERENCES

Each proposal must include a list of at least three organizations, but no more than five, that may be used as references for your work on fiduciary audits or studies. References may be contacted to determine the quality of the work performed, personnel assigned to the project, and contract adherence. Firms should ensure the accuracy of contact information and prior work from references cited. The following should be included for the references listed:

- **Date of the fiduciary audit work;**
- **Name and address of client;**
- **Name and telephone number of individual in the client organization who is familiar with the work; and**
- **Description of the work performed.**

As a professional courtesy, we ask that you please notify us prior to contacting the following references so we can provide sufficient notice to our clients, as well as provide them with contact information of the individual from ORSC conducting the reference call.

Reference #1:

- **Date of the fiduciary audit work;**
Please note, this is a client in the financial services industry with material investments and portfolio management processes.
January 2020 - present.

- **Name and address of client;**
Edelman Financial Engines 28 State St 21st Floor, Boston, MA 02109
- **Name and telephone number of individual in the client organization who is familiar with the work; and**

Mark Jankiewicz, VP, Internal Audit
mjankiewicz@edelmanfinancialengines.com
908.803.7078 (cell)

- **Description of the work performed.**
The aforementioned reference engaged CFGI to perform Enterprise Risk Management and Internal Audit Services, specifically the establishment of risk management and operational controls assessments. The

scope of work included performing an initial risk assessment, developing an overall internal audit plan, interviewing management, documenting the end-to-end processes, and executing upon the in-scope internal audit plans. Additionally, deficiencies identified were assessed for severity, assigned a remediation action plan, and communicated to management.

Reference #2:

- **Date of the fiduciary audit work;**

Please note, this is a client in the health insurance industry with material investments and portfolio management processes.

January 2020 - present.

- **Name and address of client;**

Clover Health Insurance Company, 30 Montgomery St Suite 340, Jersey City, NJ 07302

- **Name and telephone number of individual in the client organization who is familiar with the work; and**

Lisa Czerniewski, Senior Manager, SOX Compliance

lisa.czerniewski@cloverhealth.com

(724) 612-8977 (cell)

- **Description of the work performed.**

The aforementioned reference engaged CFGI to perform Internal Control over Financial Reporting program development. The scope of work included performing an initial risk assessment, interviewing key stakeholders and completing walkthroughs, drafting process documentation, including a risk and control matrix, and executing control testing plans. Additionally, deficiencies identified were assessed for severity, assigned a remediation action plan, and communicated to management.

4.5 METHODOLOGY, WORK PRODUCT, AND TIMELINE

Each proposal shall describe the proposed methodology for each element of the components listed in Section II, Scope of Audit. The description should include specific techniques that will be used, including anticipated sampling techniques and sizes, and proposed sources of data and information. You may propose alternative ways of addressing the elements of the audit's scope.

In describing the proposed methodology, also identify the type and level of assistance that you anticipate will be needed from the staff of HPRS, including assistance to understand the operations and records of HPRS and assistance to access, obtain, and analyze information needed for the audit. The description of the proposed methodology shall also identify meetings, interviews, programming support, space needs, etc., that you anticipate needing from HPRS.

Each proposal shall also include one or more examples of work product(s) for fiduciary audits that may help to illustrate the proposed methodology and final work product.

Each proposal shall provide an estimated date that the final report will be submitted and the projected timeline or the anticipated work requirements and milestone dates to reach that date. This may be expressed as time after start of contract (i.e., “1 week after contract start date,” “4 weeks after contract start date”), rather than specific calendar dates.

The general timeline of work can be summarized as follows.

- **Data and Information Requests Sent:** 2 weeks after contract start date
- **Data and Information Request Responses Received and Validated:** 11 weeks after contract start date
- **Discussions and Clarifications on Data/Information Requests:** 13 weeks after contract start date
- **Draft Findings and Recommendations:** 16 weeks after contract start date
- **Feedback Received:** 18 weeks after contract start date
- **Finalized Module Findings and Recommendations:** 20 weeks after contract start date

1. Board Governance and Administration

Please refer to the RVK proposal for details.

2. Organizational Structure and Staffing

Please refer to the RVK proposal for details.

3. Investment Policy and Oversight

Please refer to the RVK proposal for details.

4. Legal Compliance

Please refer to the RVK proposal for details.

5. Risk Management and Controls

Scope item: Conduct a risk review and evaluate control procedures of HPRS.

RVK will coordinate efforts for this scope item to the highly non-audit accounting advisory firm, CFGI. An overview of CFGI is provided on Page 15. They will employ the following steps to perform the services outlined in this section of the scope:

- Conduct interviews of key personnel and supervisors to determine if existing policies and procedures are being followed and identify any internal control deficiencies
- Review and evaluate the policy and procedures manual for internal control weaknesses pertaining to accounting functions
- Identify inconsistencies in internal controls and recommend changes to enhance consistency
- Perform an analysis of selected data on a limited basis for anomalies or unusual transactions
- Test limited accounting documentation (if needed) for any identified areas of concern
- Create a report identifying internal control weaknesses, potential risks, and recommendations to improve internal controls

CFGI will request and review HPRS’ internal control process documentation, including policies, standard operating procedures/desktop procedures, narratives, flowcharts, risk and control matrices, and any deficiency listing from prior reviews or management self assessments. As part of the audit procedures, we will validate that the current internal control processes are consistent with industry and leading best practices by interviewing the key stakeholders responsible for the retirement plan. We will then document our results and findings in a formal Internal Audit Report to management. Where applicable, we will draft recommendations for remediation on the identified deficiencies and the associated action plans to complete these remediation efforts.

We anticipate 1-2 weeks to perform our planning and scoping activities. The audit fieldwork will take approximately 16 weeks to complete. The reporting phase and delivery of the final report to the client will take approximately 2-3 weeks.

Refer to Page 16 for an example work product related to the development of an Enterprise Risk Program and Internal Audit Plan for a government agency.

6. Information Technology Operations

Scope item: Evaluate the control, accuracy, and integrity of the HPRS IT system. Review HPRS data integrity; security and confidentiality of its records system; contingency and continuity planning; and incident management system. Evaluate the overall risk level for HPRS’ IT operations.

CFGI will coordinate efforts with RVK for this scope item. An overview of CFGI is provided in Page 15. CFGI will employ the following steps to perform the services outlined in this section of the scope:

- Interviews with the Chief Information Officer and staff, as well as other key stakeholders.
- Review and evaluate:
 - IT governance processes
 - IT strategy and delivery framework
 - IT planning documents (strategic, operational, network, data security, use of third-party IT services, etc.)
 - Applications systems portfolio
 - Technology platforms
 - Descriptions of program management functions
 - IT risk assessment
 - IT disaster recovery and business continuity plans
 - Sources of reassurance, if any (e.g., penetration testing)
- Identify inconsistencies in IT controls and recommend changes to enhance consistency
- Perform an analysis of selected data on a limited basis for anomalies
- Test IT mitigating (if needed) for areas of high risk
- Create a report identifying internal control weaknesses, potential risks, and

recommendations

CFGI will request and review HPRS' IT process documentation, including policies, standard operating procedures/desktop procedures, narratives, flowcharts, risk and control matrices, and any deficiency listing from prior reviews or management self assessments. As part of the audit procedures, we will validate that the current IT processes are consistent with industry and leading best practices by interviewing the key stakeholders. We will then document our results and findings in a formal Internal Audit Report to management. Where applicable, we will draft recommendations for remediation on the identified deficiencies and the associated action plans to complete these remediation efforts.

We anticipate 1-2 weeks to perform our planning and scoping activities. The audit fieldwork will take approximately 16 weeks to complete. The reporting phase and delivery of the final report to the client will take approximately 2-3 weeks.

Refer to Page 17 for an example work product related to the development of a comprehensive IT policy for a government agency.

4.6 ADDITIONAL INFORMATION

Each proposal shall include any additional information that might be helpful to gain an understanding of the proposal. This may include diagrams, excerpts from reports, or other explanatory documentation that would clarify and/or substantiate the proposal. Any material included here should be specifically referenced elsewhere in the proposal.

Not applicable.

4.7 GLOSSARY

Each proposal shall provide a glossary of all abbreviations, acronyms, and technical terms used to describe the services or products proposed. This glossary should be provided even if the terms are described or defined when first used in the proposal response.

Not applicable.

4.8 COST INFORMATION

The pricing summary should include a breakdown of costs per element, including personnel costs (including hourly rates and estimated hours for professional and clerical staff assigned to the audit); travel and lodging; data processing costs; materials; and any other potential costs. The cost estimates in the pricing summary must include all necessary charges to conduct the audit and must be a “not to exceed” figure.

Please refer to the RVK proposal for details on the cost information.

Elaina Coletta, Finance Risk Advisory Managing Director



Managing Director
NY, NY

e: ecoletta@cfgi.com

m: 617-875-2554

OVERVIEW

Elaina brings over 12 years of experience providing internal and external audit services to clients across various industries, including financial services, biotechnology, manufacturing, and energy. Elaina has supported all Sarbanes-Oxley (SOX) compliance engagements from 404(a) IPO readiness implementations to 404(b) compliance programs for post-IPO companies.

Relevant Skills include:

- SOX Compliance and IPO Readiness
- Process Improvements
- Policy and Procedure Creation
- Control Design and Testing
- Risk Assessments and Scoping
- SOC 1 Type 2 Report Reviews
- Enterprise Risk Management and Internal Audit

Industry experience includes:

- Financial Services - Asset Management/Banking
- Life Sciences
- Manufacturing and Energy

Systems/technology expertise:

- Microsoft Dynamics
- Netsuite
- FloQast

PROFESSIONAL EXPERIENCE

While at CFGI, Elaina has served her clients in many different facets, primarily in lead SOX roles responsible for establishing and overseeing the entire risk management and SOX program. Her engagements typically entail performing risk and scoping assessments, designing and testing controls, educating control owners on execution best practices, and reporting to management and the Audit Committee. Elaina has extensive experience working closely with all key stakeholders to ensure the internal control program meets the client's objectives and goals.

Prior to joining CFGI, Elaina began her career at PwC as an external auditor in the Boston Assurance practice, participating in financial statement audits for financial services and healthcare clients. Elaina has several years of in-house industry experience leading SOX implementations for Fortune 500 financial institutions and managing Internal Audits designed to adhere to Information Technology and banking compliance requirements.

EDUCATION, LICENSES & CERTIFICATIONS

- Bachelor of Science in Business Administration, Accounting, University of New Hampshire
- Master of Science, Accounting, Northeastern University
- Master of Business Administration, Northeastern University
- Certified Public Accountant, State of Massachusetts

Xavier Sanchez, IT Risk Advisory Managing Director



Managing Director
New York, NY
e: xsanchez@cfgi.com
m: 203-610-2869

OVERVIEW

Xavier is a Managing Director and he brings over 16 years of experience, providing clients with business and technology audits, as well as providing control design assessment and process improvement services.

Relevant Skills include:

- Implementing SOX Compliance programs
- Performing ICFR Risk Assessments
- Rationalizing SOX controls and controls counts
- Establishing Internal Audit plans/departments
- Evaluating and remediating Material Weaknesses and other deficiencies

Industry experience includes:

- Manufacturing
- Life Sciences, Healthcare & Biotechnology
- Insurance –Life & Health
- Technology & Software

Systems/technology expertise:

- NetSuite
- Sage
- Oracle
- Quickbooks
- SAP
- Workiva
- Microsoft Dynamics

PROFESSIONAL EXPERIENCE

Xavier is a New York Metro Risk Advisory leader and has led numerous SOX and Internal Audit engagements for clients ranging from start-ups to Fortune 500 companies throughout his career at CFGI. He focuses on providing his clients with solutions to build strong, efficient internal control systems and practices that support their strategic objectives. Xavier has extensive experience assessing IT systems with varying infrastructures (on-prem, hosted, and cloud). He has direct experience with Microsoft Dynamics, NetSuite, Oracle Fusion and SAP.

Xavier has a broad skill set built from direct experience with Enterprise Risk Management (ERM), business processes/controls, and IT general controls (ITGCs). With this skill set, Xavier is able to view projects and engagements holistically, ensuring synergies and efficiencies across different workstreams.

Before joining CFGI, Xavier was a Specialist in the M&A and Internal Controls group at Sikorsky Aircraft Corp (A Lockheed Martin company), where he gained first-hand industry experience in implementing and maintaining effective internal controls for both SOX and operational processes. He started his career at Ernst & Young, LLP in Stamford, CT, where he worked on a variety of clients and industries.

EDUCATION, LICENSES & CERTIFICATIONS

- Bachelor of Science in Business Administration, Accounting, Sacred Heart University
- Certified Public Accountant, New Hampshire



CFG I Overview and Risk Advisory: Internal Audit

September 2022

CFG I

TOPIC	
Introduction to CFGI	9
Our Solutions	22
Workiva Partnership	34



CFGI is an established leader in accounting advisory services, providing technical accounting and operational finance expertise to clients.

Our firm was built by dedicated professionals who are innovative, passionate and experts in their field. We work alongside our clients to solve their most complex and critical finance, tax and accounting issues.

About CFGI

CFGI—a portfolio company of Carlyle and CVC—is an established national leader in providing operational finance and technical accounting services. Our clients range from pre-revenue private start-up companies to Fortune 100 public companies, including various private equity firms and their portfolio companies. We work with finance leaders during every stage of the business lifecycle to solve complex business challenges.

Expertise with perspective

CFGI is comprised of professionals with a unique combination of Big Four expertise and first-hand executive-level financial operations experience, allowing us to provide solutions across our clients' business.

Integrated solutions

We collaborate internally and with clients to achieve practical solutions, delivered with boutique firm attentiveness throughout every stage of the business lifecycle.

Collaborative Relationships

Good client relationships are the lifeblood of CFGI. We are committed to working with clients to think strategically, create new ideas, and find better solutions to business issues.





DO IT RIGHT

COMPLIANCE

CFGI's compliance experts deliver Big-Four technical expertise to ensure that every system, process and function adheres to regulatory guidelines and requirements. Our compliance and cybersecurity teams will keep you on the right side of all rules and regulations that apply to your company.



DO IT BETTER

BUSINESS VALUE ENHANCEMENT

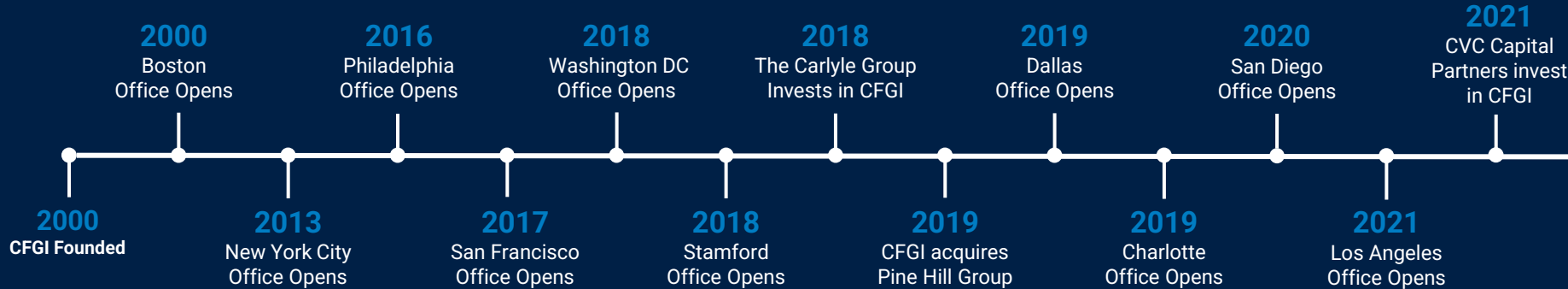
CFGI unearths opportunities to transform business functions and deliver more value to your company. Our experienced business transformation specialists have practical operational experience creating comprehensive roadmaps to drive efficiency, productivity, profitability and value throughout the enterprise.



DO IT NOW

ACCESS TO RESOURCES

CFGI provides the expertise, experience and resources to jumpstart any project without delay. We offer real-time access to the most vital and relevant resources to your company. Our experts can step in and fill empty roles on an interim basis, bridge knowledge gaps and remove barriers to innovation.



Served over
1000
public companies,
including **100s of IPOs**
and many **Fortune 1000**
companies

Over
800
full-time professionals,
all with Big Four accounting,
finance, operational and
business process and
technology backgrounds

Served over
2500
clients since CFGFI was
founded in 2000

Supported
Thousands
of CFOs on high-impact initiatives including
IPOs, SPAC's, accounting standards & Sarbanes-
Oxley 404 implementations, operational process
improvement, automation, restructuring, ERP
implementations and M&A integration

CFGFI HAS SUBJECT MATTER EXPERTS

across all technical accounting, operational finance and finance & digital transformation areas

A history of completing successful projects for the most reputable companies year after year

- Offices in **Austin, Boston, Charlotte, Dallas, Houston, New York, Philadelphia, San Francisco, Stamford and Washington D.C., San Diego and Los Angeles.**
- Over **800 full-time professionals, all** with Big Four accounting backgrounds.
- CFG I has **Subject Matter Experts (SMEs)** across all technical accounting areas including:
 - *Leases, Revenue Recognition, Business Combinations, Share-Based Compensation, Complex Debt/Equity, Warrants, EPS, Derivatives, Consolidation of Variable Interest Entities, SOX, IT Risk Management, SEC Reporting, Reverse Mergers and Pre-Clearance Letters.*
 - *Expertise across all major industry segments.*



A history of completing successful projects for the most reputable companies, year after year

Adecco

ALEXION



AMERESCO
Green • Clean • Sustainable

BAIN & COMPANY



Biogen

Boston Scientific

CDM Smith

communitybrands

COTY



ENDEAVOR

GNC
LIVE WELL

الرجل

Johnson & Johnson

mlbam



PRESIDIO
Future. Built.

Putnam INVESTMENTS

REVLON

Shire



STATE STREET

T-Mobile

TEMPUR + SEALY

Time Inc.

unfi
united natural foods

VICE

wayfair
a zillion things home

wework

We enable your successful achievement of operational, finance, and accounting goals by working as an extension of your management team.

1

Our **team of highly experienced professionals** has years of in-house audit, tax, and Big Four technical public accounting experience to add bandwidth and expertise to our client's finance teams with minimal "ramp-up" time.

2

Our **cost-effective value proposition** means that our clients receive the highest level of talent available in the marketplace at billing rates that are more favorable than Big Four or national consulting firms.

3

Our **flexible service model** enables us to align our resources to meet each client's need, which ensures clients receive the most efficient solution with the necessary expertise and experience required to get the job done.

4

Our **nimble team allows us to be responsive** and rapidly deploy our professionals into nearly any business environment, delivering immediate results to our clients, with an appropriate size team whether large or small.

5

Our firm and team of professionals are **free from independence restrictions** and therefore, can be innovative, strategic, and complete all aspects of the project and provide the most accurate solution to our client's issues.

	Cost-Effective	Technical Expertise	Quick to Respond	Client Control of Project	Resource Availability	Ability to Lead Large Projects	
CFG I	✓	✓	✓	✓	✓	✓	How CFG I Differs
Local Accounting Firm	✓		✓	✓	✓		Technical Competency
Regional Accounting Firm	✓		✓	✓	✓		Quality of Service
Temporary Staffing Firm	✓			✓			Quality of Service and Dedicated team
Internal Resources	✓			✓			Flexibility and Scalability
National Consulting Firm		✓	✓		✓	✓	Cost-effectiveness

How CFG I Differs

CFG I offers a unique solution to the marketplace with its combination of full-time, top-tier professionals dedicated to client service at a very favorable price-point.

Through the years, CFG I has demonstrated this successful model by continually adding to our enviable client roster who rely on CFG I, year after year, for their critical needs.

CFGI supports clients by providing our services across a broad spectrum of industries but have significant concentrations in those listed below.



A broad suite of services and support throughout the corporate lifecycle makes CFGI a value-added and long-term partner to CFOs.

<p>Accounting Advisory</p>	<ul style="list-style-type: none"> Technical accounting assistance Audit readiness and general close support Adoption of new accounting standards Financial Restatements Financial statements and SEC Reporting Carve-out and purchase accounting Complex stock compensation IFRS to GAAP Conversions 	<p>Transaction Advisory</p>	<ul style="list-style-type: none"> Buy-side and sell-side QOE and due diligence Data room preparation and coordination Financial modeling and EBITDA normalization Working capital negotiations
<p>Tax Services</p>	<ul style="list-style-type: none"> Accounting for income tax provisions Federal income tax compliance SALT income tax compliance R&D tax credit compliance IRS audit consulting and defense SALT income tax consulting R&D tax credit analysis 	<p>IT Risk & Cybersecurity Advisory</p>	<ul style="list-style-type: none"> IT risk management Cybersecurity Data privacy compliance (GDPR) IT General controls design and remediation services
<p>Valuation</p>	<ul style="list-style-type: none"> Purchase price allocations 409A valuations Impairment testing Derivative valuations 	<p>Restructuring</p>	<ul style="list-style-type: none"> Company advisory Creditors committee 13-week cash flow modelling Working capital management
<p>Capital Markets</p>	<ul style="list-style-type: none"> Special purpose acquisition companies (SPAC) Initial public offering prep and audit support Registration statement expertise for S-1 (US) and F-1 (foreign filers) Public company readiness compliance and operational implementation 	<p>Business Transformation</p>	<ul style="list-style-type: none"> Insight Into People, Process, Technology, and Data FP&A and other operational finance Post-merger integration Accounting System design and implementation services Digital Transformation - Robotic Process Automation (RPA) Operating model optimization (people/process/technology optimization) Operational finance and staff augmentation (process support) Enterprise Performance Management (PMO & Business Case). Event-led transformation Understanding and enhancing operational processes CFO Vision to Guide Finance Optionality in Path to Future State Understanding & Buy-In From Your Team Future State Design Future State Implementation
<p>Risk Advisory</p>	<ul style="list-style-type: none"> SOX compliance Process controls design and implementation Control design and testing Internal audit 		



CFGI

Risk Advisory and Internal Audit Services and Team

Risk Advisory Practice Overview

Influencing positive change through practical and cost-effective governance, risk and compliance solutions.

Our significant experience servicing the needs of CFOs and Controllers (Finance), CIOs, CTOs, CISOs (IT) and the CAE (IA) across various industries allows us to assess your control environment against best practices to drive continuous improvement.

CFGI's Risk Advisory practice brings a pragmatic and cost-considerate approach to today's governance, risk and compliance challenges with a "strategy-first" mindset. We are laser focused on delivering positive change and meaningful results in the specific areas of need most important to the client and its key stakeholders.

Our Risk Advisory team consists of approximately 50 individuals, all with a Big Four background. Because we do not provide attestation services, we are free from many of the independence restrictions our competitors are subject to, and this enables us to perform the services you need when you need them. **Our Risk Advisory professionals are 100% dedicated to our practice and service offerings.**

Risk Advisory Services

SOX / Internal Audit

- SOX Implementation and Ongoing Support
- Outsourced or Co-sourced SOX / Internal Audit Services
- Internal Audit Consulting Engagements

Risk Management

- IT Risk Management
- Enterprise Risk Management
- Financial, IT, Cyber and Fraud Risk Assessments

Interim Management

- Chief Audit Executive
- Director of Internal Audit
- Staff Augmentation (Finance/ITGC/Cybersecurity/Privacy)

Integration Support

- System and Application / Vendor Selection
- System Implementation Support
- Project Management

Governance, Risk and Compliance

- Policies & Procedures Creation (Enterprise, Finance, IT, Cyber)
- COSO Mapping
- Robotics Process Automation (RPA) Compliance

Process Improvements

- Process and Control Assessments
- Enterprise-wide Assessments (people, processes, and technology)
- Segregation of Duties Assessments & Identity Management

Information Technology (IT)

- IT Process & Controls Assessment
- IT Compliance Assessment (e.g. SOX, HIPAA, PCI-DSS, etc.)
- Risk and Control Mapping / Harmonization across Frameworks

SOC 1 and SOC 2 Reports

- SOC 1 Report Review for SOX & CUEC/CSOC Mapping
- SOC 2 Report Review for Vendor Due Diligence
- SOC 1 and SOC 2 Report Readiness / Gap Assessment

Cybersecurity Audit and Regulatory Compliance

- Cybersecurity Risk and Controls Assessment (e.g. NIST CSF)
- Cybersecurity Readiness Services (e.g. ISO 27001, SOC 2, etc.)
- Cybersecurity Regulatory Compliance Advisory (e.g. NYDFS)

Cybersecurity Program, Maturity & Vulnerability

- Cybersecurity Capability Maturity Assessment
- Cybersecurity Awareness & Training
- Vulnerability Scanning and Penetration Testing

Privacy and Data Security

- Privacy Program Implementation (GDPR, CCPA, and other states)
- Data Classification and Governance Design Assessment
- Ongoing Privacy Management Support

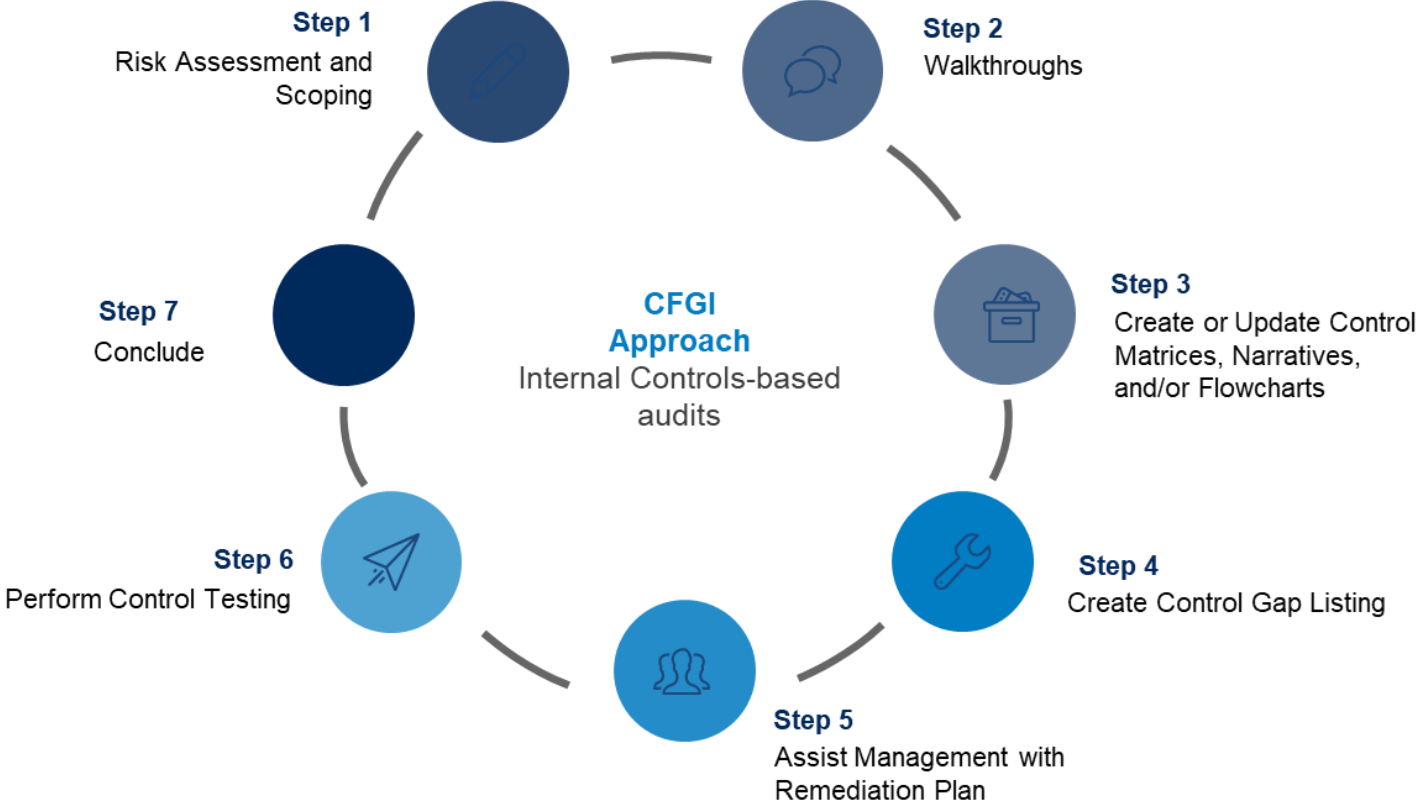
Cybersecurity/Privacy Ancillary Services

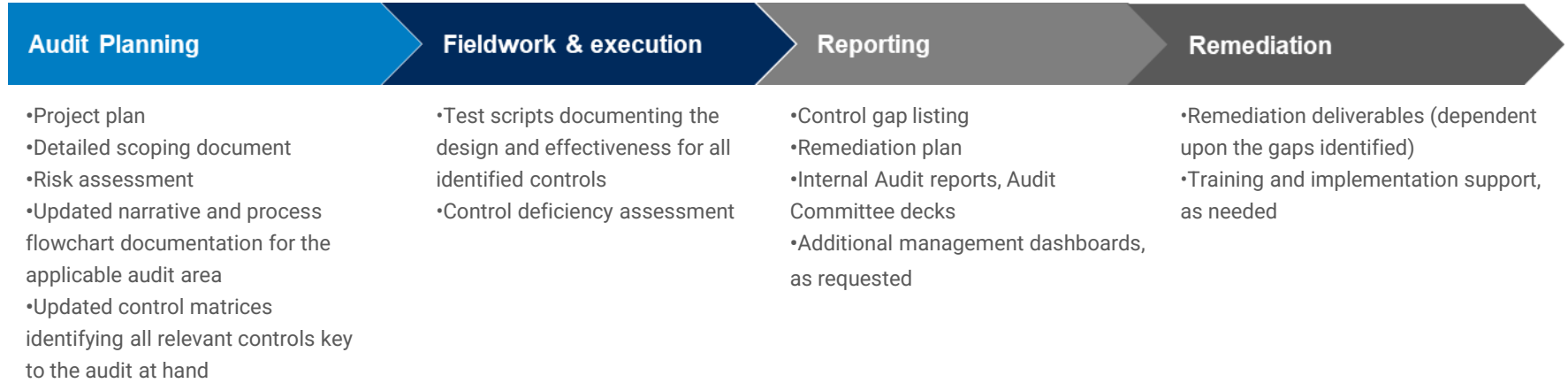
- Incident Response Planning
- Business Continuity Planning & Disaster Recovery
- Vendor Risk Management



CFGI

Internal Audit Methodology and Typical Deliverables





Benefits of Internal Audit Co-Sourcing includes:

- ✓ Practical experience and access to proven leading practice methods / solutions
- ✓ Pay only for time spent on projects / testing, not downtime spent on administrative tasks or calendar delays
- ✓ Flexibility to scale your resources up or down as your business needs warrant
- ✓ Reduce HR / Recruiting challenges typically experienced by smaller IA Departments
- ✓ Subject matter specialists / expertise, whenever you might need it, at reasonable rates
- ✓ Allows management to continually foster positive relationships with business owners, resulting in greater IA execution efficiency
- ✓ Functional ownership / control remains in-house
- ✓ Greater efficiency and overall effectiveness than a purely in-house IA function



CFG I

Sample Case Studies



CHALLENGE

Company A, a publicly-held biopharmaceutical company that received expedited review and approval designation by the FDA for its experimental drug, engaged CFGI to assist it with developing its internal controls (to support commercialization).



CFG I SOLUTION

- Performed a qualitative and quantitative risk assessment to identify applicable current and emerging risks and presented the results to senior management and the Audit Committee for input.
- Designed and implemented internal controls over the Order to Cash and Inventory processes by working closely with different functional groups across the organization.
- Compiled and risk-ranked significant third-party vendors. Worked with management to implement appropriate third-party vendor monitoring controls.
- Identified and ranked internal control gaps (SOX and operational deficiencies) and worked with management to develop remediation plans for each gap. Worked closely with management throughout the year to ensure that remediation plans were being executed upon.
- Met with the external auditors throughout the project to ensure alignment on end deliverables (flowcharts and control matrices).

OUTCOME

- The Company was able to develop efficient and effective processes which allowed it to simultaneously meet its commercialization and SOX goals.



CHALLENGE

Company B, a publicly-held fully integrated biopharmaceutical company, engaged CFGI to assist with a system implementation.



CFGI SOLUTION

- Completed qualitative and quantitative risk assessments to understand the IT environment, and the risks associated with both the technology and the Finance function's intended use cases and complexity of operations. Presented the results to senior management and the Audit Committee.
- Designed and implemented internal controls over the system development lifecycle. In addition, performed a deep dive review into system access and provided recommendations on access provisioning pre- and post-implementation to ensure that failures of access provisioning do not undermine successes in other areas of implementation.
- Provided guidance on documentation and best practices related to project initiation, planning, execution, implementation, reconciliation and testing of converted data, the go-live decision, and closure/post implementation.
- Provided support to Management to understand external auditors' requests and ensure that sufficient documentation retained throughout the process was collected to meet the requirements.
- Mapped existing controls to an internally-developed financial statement risk universe, and subsequently developed and executed a SOX 404 internal control testing program.



OUTCOME

- The system implementation was well-controlled, resulting in data integrity and reliable financial reporting.



CHALLENGE

Company C, a life science company, engaged CFGI to assist with the remediation of a material weakness relating to Income Taxes.



CFGI SOLUTION

- Coordinated multiple walkthrough meetings with the tax team, documenting the process for preparing the tax provision in a narrative-format.
- Identified key risks (“what could go wrong”) associated with the process.
- Identified the non-key and key controls in place to address these risks.
- Compiled a listing of control gaps and worked with the tax team to implement controls to address these gaps.
- Coordinated meetings between the client’s tax team and CFGI’s tax team in order to ensure that all relevant, technical tax matters and considerations were appropriately addressed.
- Provided the client with suggestions on process improvement and guidance on industry best practices.
- Worked with the client’s external auditors to resolve control design questions and facilitate design sign-off.
- Performed control testing over the newly-implemented tax controls in order to ensure that the controls were being executed appropriately (at the right level of precision) and were sufficiently evidenced.



OUTCOME

- The Company was able to successfully remediate its material weakness.



CHALLENGE

Company D, an energy company, engaged CFGI to perform an internal audit over its Procurement function.



CFG I SOLUTION

- Reviewed existing PTOp policies and standard operating procedures (SOPs).
- Interviewed key personnel in order to understand differences in policies and procedures across the Company and to gain an understanding over various procurement to pay sub-processes including, but not limited to, vendor and sub-contractor selection and performance; compliance; Request for Proposal (RFP), contract and PO review, etc.
- Assessed the Company's PTOp process against industry best practices to identify areas for improvement.
- Performed testing over certain aspects of the PTOp process. For example, reviewed a selection of contracts to ensure they were approved in accordance with the Company's pre-established authority matrix; performed trend analyses to identify favoritism towards a particular contractor or sub-contractor, etc.
- Provided management with a report highlighting our findings and recommendations for improvement. Worked with management to develop a roadmap to resolving report findings.

OUTCOME

- Management was able to implement process and policy changes that helped mitigate its operational and strategic risks.
- Management was able to improve cost savings by implementing Procurement best practices.



Partnering with you to address your most important transaction, accounting and finance needs.

BOSTON

1 Lincoln Street, Suite 1301
Boston, MA 02111
Phone 617.531.8270

NEW YORK

340 Madison Avenue, 3rd Floor
New York, NY 10173
Phone 646.360.2850

PHILADELPHIA

1835 Market Street, Suite 910
Philadelphia, PA 19103
Phone 215.558.2850

SAN FRANCISCO

Two Embarcadero Center, Suite 450
San Francisco, CA 94111

SAN DIEGO

8910 University Center Lane
San Diego, CA 92122

HOUSTON

2700 Post Oak Blvd
Galleria Office Tower,
Houston, TX 77056

WASHINGTON DC

1775 Tysons Blvd, 5th Floor
Tysons, VA 22102
Phone 703.338.3585

DALLAS

3090 Olive Street
Dallas, TX 75219
Phone 617.531.8270

STAMFORD

263 Tresser Boulevard
Stamford, CT 06901
Phone 646.360.2850

LOS ANGELES

C/O Los Angeles Office
Two Embarcadero Center, Suite 450
San Francisco, CA 94111

CHARLOTTE

615 S College St
Charlotte, NC 28202
Phone 617.531.8270

AUSTIN

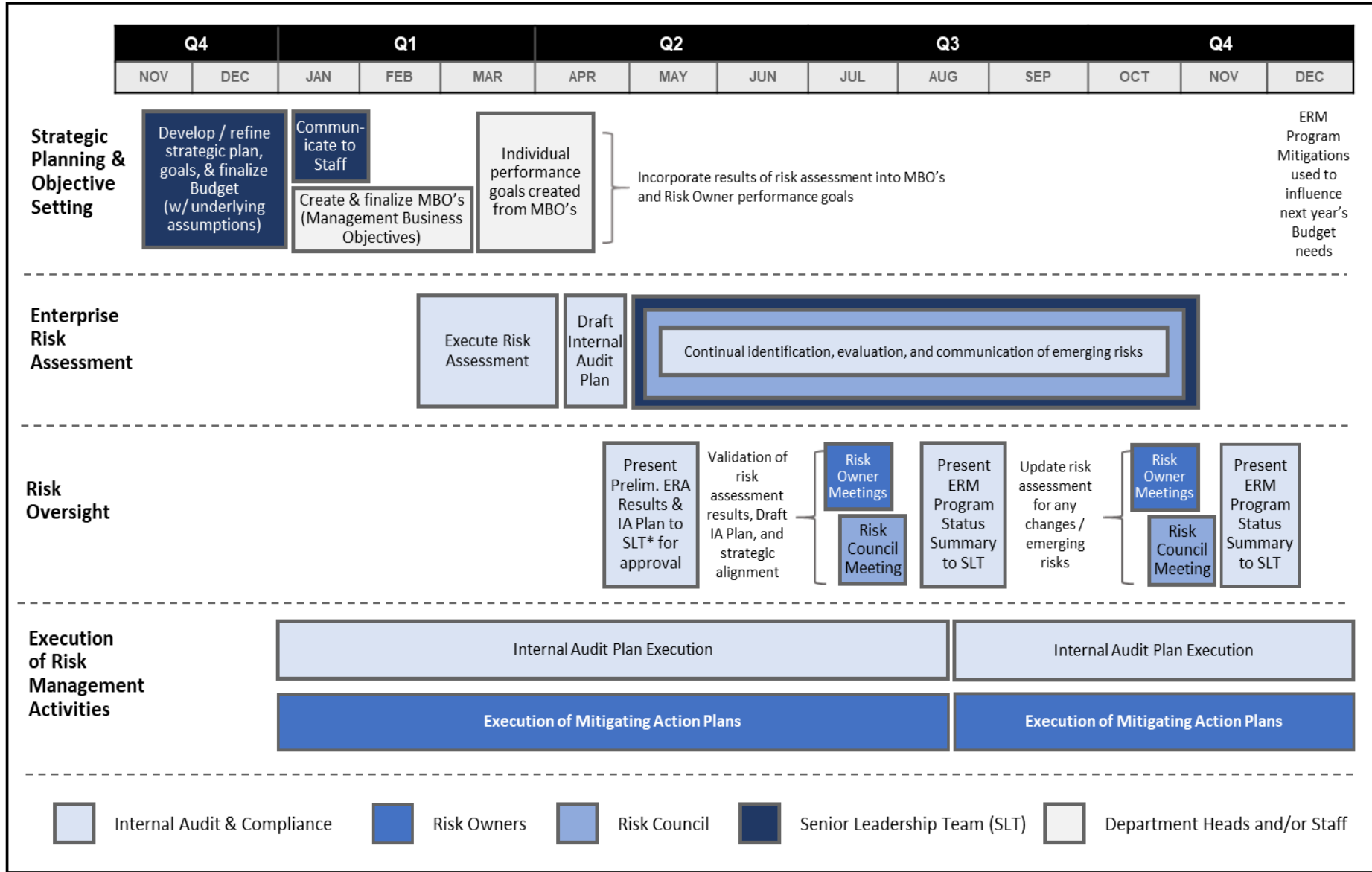
600 Congress St
Austin, TX 78701

Enterprise Risk Management (ERM) Program – Plan & Status

Deliverables & Milestones	Status
Enterprise Risk Assessment Results Summary, ERM Framework / Approach, & Draft 2020-21 Internal Audit Plan	
A) Develop and Present the ERM Methodology & Risk Universe	Completed
B) Send Enterprise Risk Assessment (ERA) Surveys to Stakeholders	Completed
C) Map ERA Survey Results to Risk Universe and Generate List of Top Risks	Completed
D) Conduct Follow-up Interviews on ERA Surveys with All Respondents	Completed
E) Generate Draft 2020-21 Internal Audit Plan & Suggested Projects to Mitigate Top Risks	Completed
Validated ERM Program Status Summary (Initial Baseline)	
A) Develop ERM “One Pagers” for each Top Risk Identified	Completed
B) Conduct Validation Meetings with Designated Risk Owners; Refine / Update Accordingly	Completed
C) Distribute ERM “One Pagers” for Risk Owner Approval; Finalize Accordingly	Completed
D) Present ERM Status Summary to Risk Council for Discussion; Refine / Update Accordingly	Not Started
E) Present ERM Status Summary to Senior Leadership Team; Refine / Update Accordingly	Not Started
F) Distribute “Final” ERM Status Summary to Risk Council & Senior Leadership Team for Execution	Not Started
G) Conduct Ongoing Meetings with Risk Owners to Refresh Top Risks & Mitigations	Not Started
Approved Internal Audit Plan	
A) Obtain Executive Chair and/or Senior Leadership team Approval of 2020-21 IA Plan	Not Started

Ongoing ERM Program & IA Plan Execution will occur in accordance with the Calendar of Events provided on the next slide

ERM Program – Annual Life Cycle & Calendar of Events

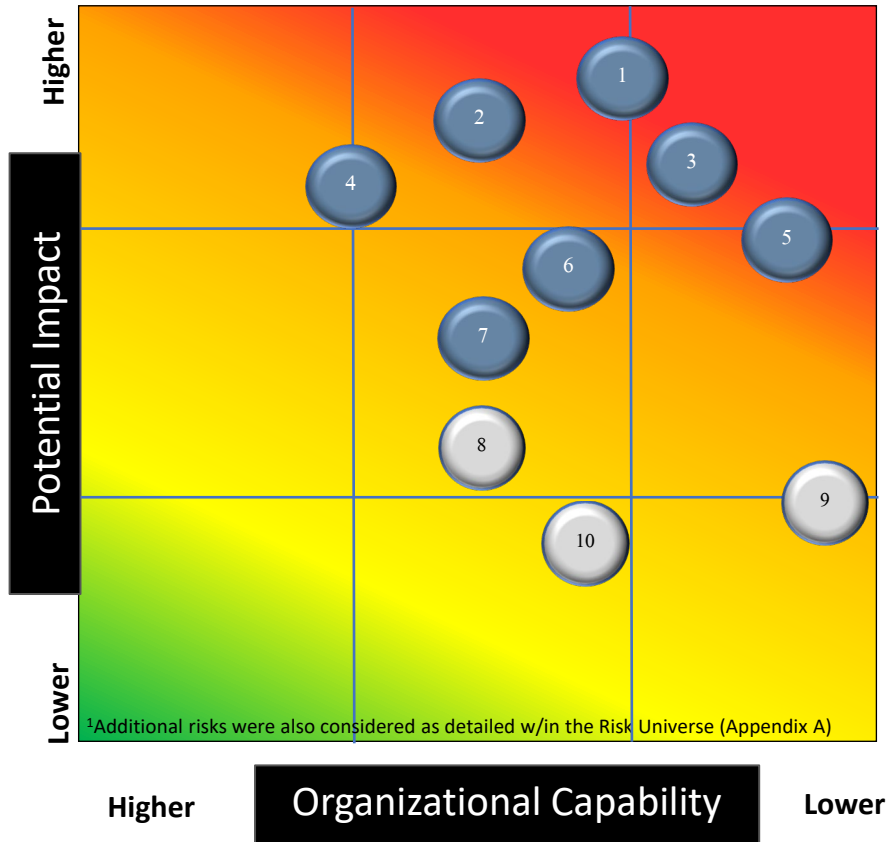


* Involved Executive Chair & Chief of Staff only in May 2020

Enterprise Risk Assessment – Results Summary

Preliminary Risk Priorities

The graph below depicts those risks / opportunities¹ most frequently cited as a result of the ERA process, plotted based on potential impact / significance and organizational capability. Based on such positioning, each risk has been classified as either Top Risk or Watchlist Risk. This list is *meant to provide a basis for further discussion and alignment of risk management priorities*.













#	Risk / Opportunity
TOP RISKS	1 Port Authority Relations & Interdependencies
	2 Project Costing & General Contractor Interdependencies
	3 MWBE Execution, Compliance & Reporting
	4 Governance & Internal Controls Readiness
	5 Procurement / Bid Process & Vendor Selection
	6 Anti-Fraud Posture & Incident Response
	7 Contract Management
WATCH LIST RISKS	8 Regulatory & Contract Compliance (non-MWBE)
	9 Staff Engagement, Retention, & Morale
	10 Quality Control & Inspections (Project Build)

Based on surveys received and/or Interviews held with: Askew, Brathwaite, Choudri, Clarke, Garzon, Hardy, Ohm/Voyer, Moussallieh, Petroff, Read, Stickelman, Sumwalt

Enterprise Risk Management

Risk Prioritization Summary

	Risk Description <i>(see details on subsequent pages)</i>	Executive Owner(s)	Current Health Assessment
TOP RISKS	Port Authority Relations & Interdependencies	Askew / Stickelman	
	Project Costing & General Contractor Interdependencies	Smyth	
	MWBE Execution, Compliance & Reporting	Hardy	
	Governance & Internal Controls Readiness	Barcelos	
	Procurement / Bid Process & Vendor Selection	Garzon	
	Anti-Fraud Posture & Incident Response	Barcelos	
	Contract Management	Okoye / Read / Garzon	
WATCH LIST	Regulatory & Contract Compliance (non-MWBE)	Okoye / Read / Barcelos	
	Staff Engagement, Retention, & Morale	Petroff	
	Quality Control & Inspections (Project Build)	Smyth	

RISK MANAGEMENT STATUS LEGEND

Current Health Assessment



: Effectively Managed



: Treatment Plan(s) Identified and In Process



: Further Treatment(s) Required

Trend Since Last Update (future)



: Improving

: Unchanged

: Deteriorating

Project Costing & General Contractor Interdependencies

THREAT	EVENT	POTENTIAL IMPACT(s)
The organization struggles to manage the General Contractor relationship. Specifically identifying decision makers at General Contractor who are able and authorized to execute decisions in a timely manner. The organization is also facing risks related to project costing specifically, finalizing the GMP and how change orders, allowances and contingencies will be managed and controlled.	The Project Management team and General Contractor struggle to finalize a GMP or identify key decision makers able to do so in a timely manner. Cost reporting by General Contractor in the required format are not transparent enough to meet and Financial sponsor objectives/goals.	<ul style="list-style-type: none"> Excessive / unjustified project costs Delays to project execution Failure to achieve build design parameters Loss of financial sponsor confidence / funding

CURRENT STATE SUMMARY	KEY ACCOMPLISHMENTS TO DATE
Positive progress has been made in terms of implementing the proper internal control environment through the System Portal. However, Project Management is still in the process of finalizing the GMP as well as implementing and testing the proper Cost Coding structure from General Contractor to allow transparency in reporting. Testing of the proper cost code structure, data integrity and reporting requirements are paramount.	<ul style="list-style-type: none"> Performed an end to end process flow of with the Project Management Team and General Contractor that identifies each step of the monthly base contract General Contractor payment process, the process owner and timeline. Developed a risk and control matrix that identifies inherent risks to the General Contractor payment process, the controls in place and the control owners. Project Management efforts to develop and finalize a Cost Coding structure with General Contractor that allows transparency in to construction costs and reporting to the project's sponsors. Work flow captured in the System Portal that documents along each step the action, review and approver before routing the next level of the work flow process.

MITIGATION OBJECTIVE	ACTION PLAN(s)	OWNER(S)	TARGET DATE	STATUS
Assess the efficacy of the General Contractor payment process	Procedural walk-throughs. Sample testing of data from the System Portal / JD Edwards	Smyth	2/28/21	TBD
	Cost and spend data reconciliations between JDE/NetSuite/ACCONEX	Smyth	2/28/21	TBD
	Monthly reporting to the Executive Chair highlighting milestones achieved, budget tracking and percentage completion.	Smyth	2/28/21	TBD
Testing of the General Contractor payment processes and control environment.	Quarterly audits utilizing sampling techniques to assess effectiveness of the control environment, identify control weaknesses and propose remediation steps, as needed.	Barcelos / Ibrahim	2/28/21	TBD

Governance & Internal Controls

Barcelos – Updated

CURRENT
HEALTH:

THREAT	EVENT	POTENTIAL IMPACT(S)
The organization may not have the proper governance, risk management, and/or internal control environment to support its needs as a standalone entity. Lack of formalized and approved policies and procedures governing business activities and transactions, including the relevant IT systems to support such needs. Lack of clearly defined roles / responsibilities and approval requirements to provide proper oversight, management, and controls.	Governance and risk management practices do not effectively support the achievement of the organization's objectives. Staffing, processes, controls, and/or systems are not sufficient to meet the needs of the organization nor satisfy regulatory / compliance requirements.	<ul style="list-style-type: none"> Strategic objectives are not met nor supported Inefficient / ineffective policies, procedures, and/or controls Lack of ownership or staffing of key processes Financial reporting and/or transactional processing errors


CURRENT STATE SUMMARY	KEY ACCOMPLISHMENTS TO DATE
A Governance, Risk, & Controls (GRC) Checklist has been created and prioritized with Management to help guide the tactical build-out of internal control environment. The GRC Checklist includes defined objectives and owners against which Internal Audit & Compliance monitors progress and objectively reviews proposed process and control design. While much progress has been made, there is still much to do in order for the organization to be fully ready on "Day One" of standalone operations.	<ul style="list-style-type: none"> Developed Code of Conduct & Complaint Handling & Incident Response Protocols Engaged NAVEX Global to maintain Compliance Hotline Developed / communicated / implemented baseline Authorization Policy, inclusive of vendors System Portal developed with documented workflows to facilitate approval requirements Completed Internal Audit assessment of IT General Controls; Management Action Plans in process Key business processes / controls have been defined, socialized, presented to Executive Chair, including: General Contractor Payments and Vendor / Commitment Approval Established ERM Approach, draft governance structure, and performed Risk Assessment to influence IA Plan Established Internal Audit & Compliance structure and go-forward plan / budget

MITIGATION OBJECTIVE	ACTION PLAN(S)	OWNER(S)	TARGET DATE	STATUS
Define Organizational Roles & Responsibilities	Establish Organization Structure to support standalone needs, including defined roles and responsibilities	Petroff	8/31/20	
	Develop Centralized Compliance Tracker (CCT), establish ownership for key compliance elements, and operationalize accordingly	Barone / Leavitt	9/30/20	
Implement Enterprise Risk Management (ERM) Program	Execute ERM Program approach and finalize ERM governance model	Barone / Ibrahim	9/30/20	
Develop / implement key business processes & controls	Finalize policies / procedures / controls for the following business areas: Budgeting & Analysis, Monthly Close & Financial Reporting, MWBE, Contingencies & Change Orders, Treasury & Cash Management, Procurement (non-project), and Travel Expenses	Various (Barone / Ibrahim to facilitate)	9/30/20	
Establish 3 rd Line of Defense to continually assess effectiveness of internal controls	Develop and obtain approval for Internal Audit Charter, 2020-21 IA Plan, & execute accordingly	Barone / Ibrahim	10/31/20	



Procurement / Bid Process & Vendor Selection

Garzon – Pending Update

CURRENT HEALTH:


THREAT	EVENT	POTENTIAL IMPACT(S)
The organization does not effectively balance the need for strategic sourcing and adequate alternatives when making procurement decisions / selecting vendors. The selection of vendors is not tied to a formalized RFP / bidding process.	Vendor sourcing, procurement functions are not fully optimized. Need for procurement and sourcing various vendors, designed to meet dynamic project/ schedule needs, budget and objectives	<ul style="list-style-type: none"> Excessive or unnecessary costs Preferential vendor treatment Reputational damage, if unable to effectively substantiate final purchase / vendor decisions

CURRENT STATE SUMMARY	KEY ACCOMPLISHMENTS TO DATE
Positive progress has been made in terms of establishing, communicating, and implementing new authorization requirements for new vendors, commitments, and invoices. However, attention still needs to be given to the actual procurement / vendor selection process from a competitive bid and cost management perspective.	<ul style="list-style-type: none"> Developed / communicated / implemented baseline Authorization Policy Developed / communicated / implemented Commitment Approval Request (CAR) process Developed / communicated / implemented Invoice Approval Request (IAR) process Developed system Portal workflows to facilitate approval requirements Established new Procurement inbox to centrally manage vendor communications

MITIGATION OBJECTIVE	ACTION PLAN(S)	OWNER(S)	TARGET DATE	STATUS
Develop robust procurement policy and tools to execute	Establish procurement, RFP / tender / bid requirement policy, including threshold requirements. Communicate, socialize and implement policy	Nifenecker	TBD	TBD
	Configure / develop tools to facilitate policy and documentation requirements	Vanhorne	TBD	TBD
Assess and seize additional cost saving opportunities	Identify opportunities and areas for cost savings across legacy and/or prospective needs	???	TBD	TBD
	Execute procurement policy for identified areas of opportunity	???	TBD	TBD

Anti-Fraud Program & Incident Response

Barcelos – Updated



THREAT	EVENT	POTENTIAL IMPACT(S)
The organization does not establish, communicate, nor promote standards for how it expects representatives to conduct business on its behalf and in an ethical manner. There is no mechanism or process in place to report, investigate, respond to, and/or resolve reported concerns / allegations of misconduct.	A violation of policies / procedures, financial malfeasance, health / safety / workplace harassment, etc. occurs and is not properly reported, investigated, nor resolved.	<ul style="list-style-type: none"> • Damage to reputation • Legal exposure • Fines or penalties • Loss of investor confidence / funding

CURRENT STATE SUMMARY	KEY ACCOMPLISHMENTS TO DATE
Positive progress has been made establishing, communicating, and implementing a Code of Conduct (CoC), Compliance Hotline, and Incident Response Protocols. Efforts continue to increase awareness of the CoC and Compliance Hotline through promotional materials, periodic reminder communications, and employee trainings.	<ul style="list-style-type: none"> • Code of Conduct (CoC) has been developed, communicated, and implemented • Complaint Handling & Incident Response Protocols have been developed, approved, and are in place • Engaged NAVEX Global to provide 3rd Party Compliance Hotline intake and support services • Established fully functional Compliance Hotline website and capabilities, as referenced within the CoC • Responsible parties for monitoring the Compliance Hotline have been trained • A test case has been run to validate the established process and protocols are operating effectively

MITIGATION OBJECTIVE	ACTION PLAN(S)	OWNER(S)	TARGET DATE	STATUS
Expand promotion / awareness of Compliance Hotline	Finalize promotional materials with NAVEX Global	Ibrahim	7/31/20	
	Position promotional posters in strategic project and office locations	Ibrahim	8/31/20	
	Include promotional pamphlets and/or wallet cards with new employee and vendor onboarding materials	D'Oliveira (employees) Nifenecker (vendors)	9/30/20	
	Develop / implement annual Executive Chair communication strategy to establish appropriate "Tone-from-the-Top"	Ibrahim / Petroff	1/31/21	
	Develop / launch annual training materials (with acknowledgements) to all employees and contractors	Ibrahim	3/31/21	

2020/21 Internal Audit Plan Considerations

Potential Projects (Top Recommendations)

Category / Audit Name	Project Goals / Objectives
Corporate & Back-Office	
Financial Close & Reporting	Design & operating effectiveness testing / assessment of key internal controls over financial accounting & reporting activities including proper journal entry recording, account reconciliation, close timeline, and financial statement & disclosure preparation, review, and approval to all relevant stakeholders.
Investigations & Special Projects	Ad hoc projects requested by management and/or required as a result of incoming Compliance Hotline activity
MWBE Compliance	Ensure a rigorous process is in place to vet, verify, and qualify MWBE subcontractors / suppliers / vendors. Conduct substantive testing to verify new and current partners are (or remain) MWBE compliant. Verify MWBE payments are properly made to qualified parties.
Office Health & Safety	Provide substantiation of COVID-19 risk management protocols / procedures in the office environment. Conduct testing to ensure such procedures are consistently maintained and any incidents are effectively managed.
NTO Procurement, Vendor Set-up & Payments	Provide assurance to management that a comprehensive process is in place when sourcing suppliers, inclusive of an RFP / tender / bidding process. Ensure sufficient internal controls are in place for managing vendor contracts, processing payments, and monitoring actual vendor budgets / spend.
Treasury & Cash Management	Design & operating effectiveness testing / assessment of key internal controls over treasury management that includes required capitalization, bank functions, and financial disclosures to relevant stakeholders.
Project & Construction Related	
Construction Quality Control & Inspections	Provide assurance to management on the scopes of work and project milestones, ensuring deliverables are being met and project costs and schedule remain on track and on budget.
Construction / Contractor Payments	Provide assurance to management on the efficacy of internal controls surrounding monthly General Contractor progress invoices, change orders, and use of allowances and contingencies.
Construction / Contractor Contract Compliance	Provide assurance to management on the accuracy / appropriateness of construction practices and accounting, including an evaluation of potential recoveries due from subcontractors / suppliers for non-compliance with contract terms.
Construction Site Health & Safety	Provide project assurance over the health and safety of the construction environment by conducting periodic site visits, reviewing incident logs, ensuring proper insurance requirements are maintained, etc.



**INFORMATION SYSTEMS
USER POLICY**

Risk Advisory Department
9.6.2022

Table of Contents

- 1. Purpose & Scope 5
 - 1.1 Acknowledgement and Acceptance5
 - 1.2 Periodic Training.....5
- 2. Policy 6
 - 2.1 Acceptable Use of Systems6
 - 2.1.1 Email Usage at the Company.....6
 - 2.1.2 Internet Usage7
 - 2.1.3 Software Access and Usage7
 - 2.1.4 Data Storage, Disposal, and Transmission/Exchange.....7
 - 2.1.5 Unacceptable Use of Systems8
 - 2.2 Devices and Support.....9
 - 2.2.1 Remote Access, Portable Devices/Media10
 - 2.2.2 IT Support10
 - 2.2.4 Personal Mobile Devices10
 - 2.2.4 Lost or Stolen Devices10
 - 2.2.5 Separation Procedures.....11
 - 2.3 Minimum Security Requirements11
 - 2.3.1 Passwords.....12
 - 2.3.2 Network Security12
 - 2.3.3 Physical Security.....13
 - 2.4 Confidentiality/Non-Disclosure13
 - 2.4.1 Protected/Confidential Information13
 - 2.4.2 Privacy/Personal Identifiable Information.....13
 - 2.4.4 Unauthorized Disclosures14
 - 2.4.5 NDAs14
 - 2.5 Risks/Liabilities/Disclaimers15
 - 2.5.1 Court Orders and Other Legal Processes15
- 3. Incident Management..... 15
 - 3.1 Incident Monitoring15
 - 3.2 Incident Communicating & Reporting.....15
- 4. Policy Enforcement 16
 - 4.1 Responsibilities15

4.2 Consequences of Violation15

1. Purpose & Scope

- a) This Information Systems Use Policy (“Policy”) governs the use of all information systems (“Systems”) developed and employed by THE COMPANY, LLC (“THE COMPANY LLC” or “the Company”). Subject to the agreement between THE COMPANY LLC and each of its partner organizations (collectively “Partner Organizations” and each a “Partner Organization”), each Partner Organization and its personnel assigned to work on THE COMPANY LLC project (the “Project”) and any personnel hired or contracted by THE COMPANY LLC (collectively “Personnel”) shall be bound by this Policy. The Policy shall be provided by each Partner Organization to its Personnel; however, each Partner Organization shall be responsible for the compliance of its Personnel with this Policy.
- b) THE COMPANY LLC reserves the right to revoke access to any or all Systems if any Personnel, person or organization accessing and using such Systems (“Users”) does not abide by the policies and procedures outlined below. This Policy is intended to protect the security and integrity of THE COMPANY LLC’s Data (as defined below) and its Systems.
- c) All data and other information that relates to THE COMPANY LLC or the Project (collectively, the “Data”) shall be owned by, and treated as the Confidential Information, as defined herein, of THE COMPANY LLC.

1.1 Acknowledgement and Acceptance

Each User shall acknowledge receipt and acceptance of the Policy and any updated acknowledgements as shall be required. If a User fails to acknowledge and accept the Policy, THE COMPANY LLC, in its sole discretion, may temporarily or permanently revoke access to any or all Systems and Data. Users may not use Data, nor any information accessed through any System for any reason whatsoever other than work or services as defined in the agreements between THE COMPANY LLC and any Partner Organization (“Services”). User acknowledges that User may, in the course of performing its responsibilities, be exposed to, or acquire, information which is proprietary or confidential, to PANYNJ and/or THE COMPANY LLC, its affiliated companies, or third parties to whom THE COMPANY LLC owes a duty of confidentiality. Any and all non-public information of any form accessed by User in the performance of Services shall be deemed to be confidential and proprietary information (“Confidential Information”). Partner Organizations and Users agree to hold, and require Personnel to hold, such information in strict confidence and not copy, reproduce, sell, assign, license, market, transfer, or otherwise dispose of, give, or disclose any Confidential Information to third parties or to use any Confidential Information for any purpose whatsoever other than the performance of Services and to advise all Personnel and Users who may be exposed to the Confidential Information of their obligations to keep such information confidential.

1.2 Confidentiality/Non-Disclosure.

Users may not use Data, nor any information accessed through any System for any reason whatsoever other than work or services as defined in the agreements between THE COMPANY LLC and any Partner Organization (“Services”). Please refer to Section 1.1 ‘Acknowledgement and Acceptance’ for details on Confidential Information

1.2.1 Protected/Confidential Information

If a Partner Organization or a User’s Services are terminated or expire, each User shall, as directed by THE COMPANY LLC, promptly deliver to THE COMPANY LLC all Confidential Information, together with all copies thereof, in the possession, custody or control of User or, alternatively, with the written consent of THE COMPANY LLC destroy all such Confidential Information and certify in writing to THE COMPANY LLC that all such Confidential Information has been delivered or destroyed.

1.2.2 Privacy/ Personal Identifying (Identifiable) Information

Privacy is a subset of Confidential Information. It concerns information about an entity and assures that this information is not made public or accessible by unauthorized parties or entities, or individuals. Personal Identifying (Identifiable) Information (“PII”) is information which can be used to distinguish or trace an individual’s identity, which may include their name, social security number, driver’s license, fingerprints, biometric records, etc. which alone, or when combined with other personal or identifying information may be used to link or is linkable to a specific individual (such as date and place of birth, mother’s maiden name, etc.)

Such information should not be used or exchanged within the Company for purposes other than those stated, for legitimate purposes that would be reasonably expected, or where the information exchanged does not identify any individual, such as with aggregated data.

- a) PII should only be sent through secure/encrypted protocols cleared by THE COMPANY.
- b) Individuals requiring access to Confidential Privileged Information must have a need to know consistent with the creation and preservation of the privilege attached to the Protected Information. An individual will be given access privileges to the Confidential Privileged information only to the extent that it is necessary and/or is required by the individual to fulfil and/or carry out his/her duties, obligations and responsibilities.

1.2.3 Unauthorized Disclosure

If THE COMPANY LLC Personnel, consultants, third-party contractors, or other individuals and/or entities with authorized access to Protected Information become aware that Protected Information has been released to unauthorized persons, or has been lost, stolen or compromised, they are required to immediately notify helpdesk@oneTHE.com.

1.2.4 NDA’s

Requirements must be included in procurement documents in order to help reduce potential disclosure of Protected Information and to provide bidders with certain security requirements in

advance. They must also be included in contract awards to ensure information protection practices, procedures, and protocols are included in each project's lifecycle phase. The typical requirements are:

- a) Requires prospective consultants, prime vendors, general contractors, or commercial enterprises to enter iCompany an NDA with the Port Authority before obtaining a copy of an RFP for projects that may contain Protected Information.
- b) NDAs should be project and procurement specific and should be completed in a timely manner for specific types of procurements or projects. A broad or generic NDA should not normally be utilized to cover all procurements and projects under contract to a particular consultant, prime vendor, general contractor or commercial enterprise over a long period of time; however, it may be appropriate in certain situations to utilize such an NDA, if approved by management.
- c) Consultants, Prime Vendors, General Contractors, or Commercial Enterprises should contact the Port Authority to request authority prior to releasing RFP Protected Information to a subcontractor. The sub-contractor should execute the appropriate Acknowledgement that it will comply with the terms of any NDA that the successful bidder has executed.

1.3 Periodic Training

IT security awareness training is a formal process for educating Personnel about computer security. All Personnel with access to THE COMPANY LLC network and Information Resources must complete security awareness training within the first 30 days from date of hire. Information Security Refresher Training must be completed annually, within 60 days of the anniversary of the previous instance of such training.

2. Policy

2.1 Acceptable Use of Systems.

- a) Acceptable business uses of Systems are activities that directly or indirectly support THE COMPANY LLC or any work associated with the Project. Users shall:
 - i. exercise due care and adhere to all policies, rules and regulations of THE COMPANY LLC and the Port Authority of New York and New Jersey ("PANYNJ") including without limitation adherence to the PANYNJ Information Security Handbook when accessing transmitting and processing information;
 - ii. not share passwords, copies or links to any Systems or Data to any unauthorized user;
 - iii. complete the PANYNJ training module, which supplements the PANYNJ Information Security; and
 - iv. not, at any time, use any System to:
 - o Store or transmit illicit materials,
 - o Store or transmit proprietary information belonging to another company,
 - o Harass others, and
 - o Engage in outside business activities.

- b) The use of any photographic, video, audio or other recording capabilities at any Project office or site must be solely related to Services (as defined above) and must be governed with a reasonable expectation of privacy. **Use of any device's photographic, video, audio, or other recording capabilities at any Project site or office not related to Services is strictly prohibited unless approved in advanced by THE COMPANY LLC in writing in each instance.** All photographs, video, audio, or other recordings taken at any Project site or office shall be the property of THE COMPANY LLC and shall be treated as Confidential Information as defined and set forth in Section 3 of this Information Systems Use Policy.

2.1.1 Email Usage at the Company

Email is to be used for THE COMPANY LLC business only. Confidential Company information must not be shared outside of THE COMPANY LLC, without authorization, at any time. Personnel also are to minimize personal business using THE COMPANY LLC computer or email. Any email content that discriminates against any of the previously mentioned protected classifications is prohibited. Any Personnel who sends an email that violates this Policy will be dealt with according to the anti-harassment policy. These mails are prohibited at THE COMPANY LLC. Sending or forwarding discriminatory emails will result in disciplinary action that may lead to employment termination.

Keep in mind that THE COMPANY LLC owns any communication sent via email or that is stored on Company Equipment. Company Equipment includes company-issued phones, laptops, tablets and any other electronic equipment, and belongs to THE COMPANY LLC. Management and other authorized staff have the right to access any material in Personnel email or on their computers at any time. Personnel should not consider their electronic communication, storage, or access to be private if it is created or stored on work systems.

2.1.2 Internet Usage

This Internet usage policy applies to all Personnel of THE COMPANY LLC who have access to computers and the Internet to be used in the performance of their work. Use of the Internet by Personnel is permitted and encouraged where such use supports the goals and objectives of the business. However, access to the Internet through THE COMPANY LLC's systems is a privilege and all Personnel must adhere to the policy requirements concerning device, email and Internet usage. Violation of these requirements could result in disciplinary and/or legal action leading up to and including termination of employment. Personnel may also be held personally liable for damages caused by any violations of this policy. All Personnel are required to acknowledge receipt and confirm that they have understood and agree to abide by the rules hereunder.

- a.) Job-related activities include research and educational tasks that may be found via the Internet that would help in an employee's role;
- b.) All Internet data that is composed, transmitted and/or received by the Company's computer systems is considered to belong to the Company and is recognized as part of its official Data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties;

- c.) The equipment, services and technology used to access the Internet are the property of the Company and the Company reserves the right to monitor Internet traffic and monitor and access data that is composed, sent or received through its online connections;
- d.) All sites and downloads may be monitored and/or blocked by the Company if they are deemed to be harmful and/or not productive to business

2.1.3 Software Access Procedure

Software needed in addition to the Microsoft Office suite of products must be authorized by a supervisor and downloaded by the Director of Technology or their designate. If you need access to software or websites not currently on the company network, Personnel should discuss this with their supervisor and consult with the IT department to explain the reason for this request. All reasonable requests that are not considered a network risk will be considered. The purpose of this Policy is not to restrict Personnel's access to products that will make them more productive. Rather, the goal is to minimize the risk to the organization's network.

The installation of unapproved software, such as instant messaging technology, is strictly prohibited.

2.1.4 Data storage, Disposal, and Transmission/Exchange

Access to information system media is permitted only for Authorized Users. Authorized Users are any personnel or contractor who has permission to use THE COMPANY LLC's computing systems and network.

Approved Cryptographic Mechanisms or other alternative physical safeguards should be used during transmission in order to prevent unauthorized disclosure of information. Cryptographic Mechanisms are encryption tools used for protecting confidentiality, integrity, authenticity and non-repudiation of information. Media containing sensitive or highly sensitive data or information that is transported outside of controlled areas needs to be strictly monitored to control access and to form accountability. Sensitive data is broadly defined as information that must be protected against unwarranted disclosure. Access to sensitive data must be safeguarded in accordance with legal and regulatory standards, IT best practices, and organizational policy. The local storage of sensitive data on mobile devices should be minimized or risk managed in accordance with the employee's duty requirements. Mobile devices are to include any mobile phone, smartphone, tablet or hybrid device. Some examples of sensitive data include information on research subjects, protected health information, financial data, employee records, grants, contracts, and intellectual property.

Approved backups and cryptographic mechanisms or other alternative physical safeguards should be implemented to protect the integrity and confidentiality of information stored on digital media during transport. Backups, or backup programs, can be defined as the process of copying data oCompany electronic storage media (i.e., backing up) that may then be used to restore the data to its original form after the occurrence of a data loss event or data file corruption. All data should be

disposed of when it is no longer necessary for business use, provided that the disposal does not conflict with our data retention policies, a court order, or any of our regulatory obligations.

- a) All THE COMPANY LLC personnel, clients, vendors, and contractors are instructed to not use the following media to store confidential information.
 - i. paper-based media
 - ii. USB Drives or external backup programs
 - iii. CD ROM drives.
- b) All cloud-based storage media being decommissioned should be sanitized when it is no longer necessary, provided that there is a backup of third-party data on production systems to comply with our data retention and contractual obligations.
- c) Laptop based storage media may not be donated or sold. All laptop-based storage media should be sanitized prior to transfer of ownership to a co-worker or prior to destruction.

2.1.5 Unacceptable Use of the Information Technology Network

The following activities are prohibited, although Personnel who are Authorized Users may be exempted from these restrictions during the performance of their legitimate job responsibilities. Under no circumstances is an Authorized User permitted to engage in any activity that is illegal under local, state, federal or international law while utilizing the Information Technology Network.

Regarding Security and Proprietary Information, the following activities are strictly prohibited, with no exceptions:

- a) Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of copyrighted or other software products that are not licensed for use by the company.
- b) Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Company or the Authorized User does not have an active license is strictly prohibited.
- c) Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. Management must be consulted prior to export of any material that is in question.
- d) Introduction of malicious software to the Information Technology Network (e.g., viruses, worms, trojan horses, e-mail bombs, etc.).
- e) An Authorized User's revelation of that person's account password to others or allowing use of an Authorized User's account by others, including family and other household members when an Authorized User's computer is connected to the Information Technology Network from home or other non-locations.
- f) The use of a component of the Information Technology Network or other computing asset to actively engage in procuring or transmitting material that violate sexual harassment or hostile workplace laws or that violates any policy. Pornographic material is a violation of sexual harassment policies.

- g) Making fraudulent offers of products, items, or services originating from any account or otherwise made from a computer connected to the Information Technology Network.
- h) Causing security breaches or disruptions of communication over the Information Technology Network. Security breaches include, but are not limited to, accessing data or other communications of which the Authorized User is not an intended recipient or logging iCompany an account that the Authorized User is not expressly authorized to access. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, traffic floods, packet spoofing, denial of service, etc.
- i) Executing any form of network monitoring which will intercept data not intended for the Authorized User is expressly prohibited, unless this activity is a part of the Authorized User's normal job/duty.
- j) Circumventing user authentication or security of any device, Network, or account.
- k) Using any Program/script/command, or sending messages of any kind, with the intent to interfere with or disable a user's terminal session, via any means locally or remotely.
- l) Providing information about, or lists of, Personnel.

Regarding Email and Communications Activities, the following activities are strictly prohibited, with no exceptions:

- a) Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (Email spam).
- b) Any form of harassment via email, instant messenger, telephone, or pager, whether through language, frequency, or size of messages.
- c) Unauthorized use, or forging, of email header information.
- d) Solicitation of Email for any other Email address, other than that of the Authorized User's own account, with the intent to harass or to collect replies.
- e) Creating or forwarding chain email, phishing, or other scams of any type.
- f) Use of the 's company's name in any unsolicited email on behalf of, or to advertise, any service or product without the explicit written permission of the company.

2.2 Devices and Support.

THE COMPANY LLC expects its personnel to respect and protect the Company's equipment.

2.2.1 Remote Access, Portable Media and Devices

For all remote access, it's strongly recommended to use a Virtual Private Network ("VPN"). A VPN provides remote access to company network services from any computer, on or off site, and offers safe, secure sign-in to the company's network.

- a) Portable media and mobile devices shall implement full disk encryption solutions to safeguard Company information in case of loss.
- b) All Protected Information stored on portable devices shall be password protected at the document level or protected using the Company's information protection solution.
- c) Mobile laptop computers, tablets, cell phones, other devices, computer media and any other forms of removable storage must be handled in a prudent and responsible manner.

A mobile device displaying sensitive information being used in a public place (e.g., train, aircraft or coffee shop) must be positioned so that the screen cannot be viewed by others, thus protecting THE COMPANY LLC information. A tinted/polarized screen guard may be used to decrease the viewing angles of any mobile device.

- a) Mobile devices must not be left unsecured or unattended, even for a short period of time.
- b) Mobile devices must not be left in a vehicle overnight.

2.2.2 IT Support

Connectivity issues while at any Project site or office operated by THE COMPANY LLC and application issues are supported by THE COMPANY LLC. Please contact helpdesk@oneTHE.com for emergencies or access to applications.

2.2.3 Personal Mobile Devices

A Personal Mobile Device (Personal Device) is broadly defined as any laptop computer, smartphone, tablet, etc. that is purchased and maintained by an individual and is used for business purposes. Users are required to enroll their device(s) iCompany the mobile device manager environment in use by IT and maintain their devices in compliance in order to access enterprise systems hosted or contracted by IT.

Users must maintain a device compatible with the organization's published technical specifications. IT will periodically review the suggested specifications and, based upon security and support requirements, make modifications. All modifications will be communicated to the intended audience if the modification affects a number of devices currently in use. These modifications could result in a decrease in functionality or support until the device is upgraded or updated. In rare cases, extreme security flaws or findings may dictate a total loss of access until the device again meets standards.

2.2.4 Lost or Stolen Devices

In the event the device with company Data is lost or stolen, an employee should:

- a) Immediately report the theft/loss of a mobile device to your supervisor and department/division leadership.
- b) If PII is stored or is otherwise accessible on or through the mobile device, report the theft/loss to the applicable privacy officer.
- c) Report the theft and details of the incident to the appropriate law enforcement.
- d) Upon loss or theft of a device, Authorized Users must submit a report to the Help Desk - helpdesk@oneTHE.com. This allows the device to be remotely wiped over the network before cancelling any mobile operator services. The act of remotely wiping data from the device does not cancel the service in effect for the device. It shall be the Authorized User's responsibility to contact their carrier and cancel any individual voice and data services after the remote wipe of the device is completed.

- e) IT support will work closely with the individual to minimize the potential exposure and disclosure of sensitive business and/or personal data that might be on a stolen/lost mobile device.

2.2.5 Separation Procedures

Return all Company Property:

- a) Keys/Access Cards (building, office, desk, files, vehicles, lockers, etc.).
- b) Company Equipment including computers/laptops/iPads or other peripheral equipment (e.g., printers, cameras) cellular phones, etc.
- c) Records (documents, files, correspondence, etc.).

Electronic Records:

- a) Retrieve or delete any personal files/information on an employee's office/home PC, office/department server, lab server, central file space, etc.
- b) Retrieve any email files, or files on other email servers and systems, that an employee wishes to retain:
 - i. Employee must have the permission of the appropriate supervisor to copy any Company files or records.
 - ii. Files are purged when an email account is closed.
- c) Return (transfer, copy, etc.) to the appropriate unit and/or administrator(s) any unit or company data files, electronic documents and records, etc. that are stored on a personal work PC or in personal server file spaces.
- d) If an employee possesses sole access rights to an administrative database, software application, information system, etc., that is necessary for operations, transfer the passwords to the appropriate administrator, or arrange for an administrator to be given the access needed to assure continued operations.
- e) Delete or return any Company owned/licensed software that is contained on a home computer. For assistance please contact the Help Desk.

2.3 Minimum Security Requirements.

Adherence to these standards is an essential safeguard for the protection of electronic company data and systems. However, compliance does not assure complete security. These standards should be incorporated into a comprehensive security plan. Additional policies and laws may also apply.

2.3.1 Passwords

User must obtain a personal password to access any System. Authorized users shall keep such personal password(s) and User ID confidential and shall not share, transfer, sublicense, or otherwise make it available to any other Authorized user, person, or entity. Passwords should never contain security-sensitive information, such as an employee's social security number or date of birth. They also should not include public information related to an employee's personal life, such as the names of their children, hobbies, favorite sports team, etc.

Personnel must configure their laptops with a password that meets the following standards for password length, complexity, history, expiration, and lockout.

Password length: Password must be between 8-64 characters long.

Password complexity: Password must contain a mixture of special characters, alphanumeric characters, and lower- and upper-case letters. Dictionary words should never be used as a password but are acceptable as part of a longer passphrase (16 characters and longer).

Password history: Password must be different from the previous last three passwords used.

Password expiration: Passwords are required to change every 90 days. Employee laptops will require a password change every 180 days.

Password logout: Users must re-enter their password after 60 minutes of inactivity.

Passwords should be considered confidential data and treated with the same discretion as any of the organization's proprietary information. The following guidelines apply to the confidentiality of passwords:

- a) Users must not disclose their passwords to anyone
- b) Users must not share their passwords with others (co-workers, supervisors, family, etc.)
- c) Users must not write down their passwords and leave them unsecured
- d) Users must not use the same password for different systems and/or accounts
- e) Users must not reuse passwords upon expiration of the old password

2.3.2 Network Security

All information traveling over THE COMPANY LLC computer networks that has not been specifically identified as the property of other parties will be treated as though it is a THE COMPANY LLC asset. It is the policy of the Company to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information. Users are responsible for complying with this and all other company policies defining computer and network security measures. Users also are responsible for bringing all known information security vulnerabilities and violations that they notice to the attention of the Information Technology department.

Network-connected, single-user systems must employ Company approved hardware or software controls that prevent unauthorized access.

2.3.3 Physical Security

Protect and monitor the physical facility where data and information are stored and support infrastructure for those information systems.

Any device (including smartphones and tablets) accessing any System must lock itself with a password or PIN if the device is idle for five minutes. Where feasible, devices should also have virus protection installed and run-on schedule or on Authorized User demand.

Encryption of information must be used in compliance with the Policy. Encryption includes any process of converting information iCompany an unintelligible form except to holders of a specific cryptographic key.

Authorized Users are required to exercise special care to protect laptop computers that are part of or connected to Network

2.4 Risks/Liabilities/Disclaimers

IT related risks are the probability that a particular vulnerability or vulnerabilities in the THE COMPANY LLC information system will be intentionally or unintentionally exploited by a threat which may result in the loss of confidentiality, integrity, or availability, along with the potential impact such a loss of confidentiality, integrity, or availability would have on THE COMPANY LLC operations, assets, or individuals. Lost or stolen devices with copies of Data must be immediately reported to THE COMPANY LLC within 24 hours by contacting helpdesk@oneTHE.com. Passwords should be changed immediately by Authorized Users. Users should take every precaution to safeguard their passwords.

2.4.1 Court Orders and Other Legal Processes

In the case of court orders or other legal process (including subpoenas or agency requests for information) that require release of information about THE COMPANY LLC Personnel, that individual should ordinarily be notified of the request as soon as possible. Notification will not be made, however, where such notification is specifically prohibited by the law or where the request for information asks for nondisclosure and such nondisclosure is, in the judgment of management, appropriate under the circumstances (for example, where notification might interfere with a criminal investigation). The requested information should be released only by an authorized officer of the Company after consultation with the General Counsel.

3. Incident Management

3.1 Incident Monitoring

Types of security incidents to monitor: Any security event believed to be suspicious or considered an unauthorized attempt to access, use, steal, or damage the company's electronic information, information systems, or information technology infrastructure. This includes anomalous computer activity, missing computer equipment, etc.

Failure to report or respond to an event or incident can expose the company to regulatory and/or statutory penalties, costly litigation, and undermine its mission and standing in the community. Violations of this policy may subject the violator to disciplinary actions up to or including termination of employment

3.2 Incident Communicating & Reporting

All personnel are required to report any disruptive incidents in the following manner:

- a) IT-related incidents, such as a data breach, should be immediately communicated to senior management.
- b) The communication must summarize the incident and procedures that will be taken to contain the incident from escalating.
- c) All IT-related incidents (e.g., phishing attacks, connectivity issues, etc.) must be reported by telephone or email to the management and the Helpdesk.

4. Policy Enforcement

4.1 Responsibilities

Any Authorized User found to be in violation of this Policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Policy Enforcement section of the Policy.

4.2 Consequences of Violation

Repeated failure or refusal to comply with any principles of this policy will result in the following disciplinary actions:

1. First violation: The employee and the employee's manager are notified.
2. Second violation: Senior management and Human Resources are notified of the violation.
3. Third violation: Potential cause for termination. Depending on the severity of the violation (e.g., deliberate breach of data), an employee may be terminated for a first violation.

Summary of Fees

Audit Workstreams	Proposed Total Hours	Proposed Cost	
Section 2.5 - Risk Management and Controls	748	\$ 144,000	
Proposed Fees		\$ 144,000	
Expenses (Local + Travel)		\$ 14,000	
Section 2.6 - IT Operations	560	\$ 110,000	
Proposed Fees		\$ 110,000	
Expenses (Local + Travel)		\$ 11,000	
		\$ 279,000	Fee with Travel
		\$ 254,000	Fee to Client

*Note, we will absorb the \$25K for travel to the client site as a good faith effort.

Role	CFG rates	
	Standard Rate	
Partner	\$	300
Managing Director / Director	\$	240
Senior Manager	\$	215
Manager	\$	170
Consultant	\$	145

Section 2.5 Risk Management and Controls: An evaluation of the adequacy of financial controls and integrity of the financial statements of HPRS overall and its investment program.

3.1.1 Proposed Discount --> 0.0%

3.1.2 Internal Audit Activities		Proposed Hours	Proposed Cost
1	Audit Planning	40	\$ 8,360
2	Audit	491	\$ 92,880
3	Project Management	120	\$ 23,040
4	Stakeholder Reporting	97	\$ 20,065
EXP1	Local resources expense NOT TO EXCEED this % of fee -->	0.00%	\$ -
EXP2	Travel resources expense NOT TO EXCEED this % of fee -->	10.00%	\$ 14,435
Total proposed cost		748	\$ 144,345

3.1.3	Module Activity	Resource Role	Type of rate	Local/Travel	Proposed rate	Proposed Hours	Proposed Fees
1	Audit Planning	Partner	Standard rate	Travel	\$ 300	2	\$ 600
2	Audit Planning	Managing Director / Director	Standard rate	Travel	\$ 240	6	\$ 1,440
3	Audit Planning	Senior Manager	Standard rate	Travel	\$ 215	24	\$ 5,160
4	Audit Planning	Consultant	Standard rate	Travel	\$ 145	8	\$ 1,160
5	Audit	Partner	Standard rate	Travel	\$ 300	0	
6	Audit	Managing Director / Director	Standard rate	Travel	\$ 240	75	\$ 18,000
7	Audit	Senior Manager	Standard rate	Travel	\$ 215	208	\$ 44,720
8	Audit	Consultant	Standard rate	Travel	\$ 145	208	\$ 30,160
9	Project Management	Partner	Standard rate	Travel	\$ 300	0	
10	Project Management	Managing Director / Director	Standard rate	Travel	\$ 240	24	\$ 5,760
11	Project Management	Senior Manager	Standard rate	Travel	\$ 215	48	\$ 10,320
12	Project Management	Consultant	Standard rate	Travel	\$ 145	48	\$ 6,960
13	Stakeholder Reporting	Partner	Standard rate	Travel	\$ 300	6	\$ 1,800
14	Stakeholder Reporting	Managing Director / Director	Standard rate	Travel	\$ 240	18	\$ 4,320
15	Stakeholder Reporting	Senior Manager	Standard rate	Travel	\$ 215	48	\$ 10,320
16	Stakeholder Reporting	Consultant	Standard rate	Travel	\$ 145	25	\$ 3,625

3.1.5 INSERT Resource Hours by Month (consider 8 hours per day and 21 working days per month) -->

Total hours	Month 1	Month 2	Month 3	Month 4	Month 5
2	2				
6	6				
24	24				
8	8				
75		25	25	25	
208		104	84	20	
208		104	84	20	
24	5	5	5	5	5
48	10	10	10	10	10
48	10	10	10	10	10
6					6
18					18
48					48
25					25

Key Audit Areas:	Planning (1 wk)	Audit Fieldwork (16 wks)	Reporting (3 wks)	PM (20 wks)		
Interviews with key stakeholders	40	100				
Review of current documentation		240	40	40		
Benchmarking to leading practice guidance		100	40	40		
Follow up questions to management		80	40	40		
	40	520	120	120	800	check
	0	0	0	0		0

Section 2.5 IT Operations: An evaluation of data integrity; security and confidentiality of its records system; contingency and continuity planning; and incident management of HPRS overall and its investment program.

4.1.1 Proposed Discount --> 0.0%

4.1.2 Internal Audit Activities		Proposed Hours	Proposed Cost
1	Audit Planning	40	\$ 8,560
2	Audit	385	\$ 70,700
3	Project Management	55	\$ 12,300
4	Stakeholder Reporting	80	\$ 18,120
EXP1	Local resources expense NOT TO EXCEED this % of fee -->	0.00%	\$ -
EXP2	Travel resources expense NOT TO EXCEED this % of fee -->	10.00%	\$ 10,968
Total proposed cost		560	\$ 109,680

4.1.3	Module Activity	Resource Role	Type of rate	Local/Travel	Proposed rate	Proposed Hours	Proposed Fees
1	Audit Planning	Partner	Standard rate	Travel	\$ 300	2	\$ 600
2	Audit Planning	Managing Director / Director	Standard rate	Travel	\$ 240	6	\$ 1,440
3	Audit Planning	Senior Manager	Standard rate	Travel	\$ 215	24	\$ 5,160
4	Audit Planning	Manager	Standard rate	Travel	\$ 170	8	\$ 1,360
5	Audit	Partner	Standard rate	Travel	\$ 300	5	\$ 1,500
6	Audit	Managing Director / Director	Standard rate	Travel	\$ 240	40	\$ 9,600
7	Audit	Senior Manager	Standard rate	Travel	\$ 215	40	\$ 8,600
8	Audit	Manager	Standard rate	Travel	\$ 170	300	\$ 51,000
9	Project Management	Partner	Standard rate	Travel	\$ 300	5	\$ 1,500
10	Project Management	Managing Director / Director	Standard rate	Travel	\$ 240	20	\$ 4,800
11	Project Management	Senior Manager	Standard rate	Travel	\$ 215	20	\$ 4,300
12	Project Management	Manager	Standard rate	Travel	\$ 170	10	\$ 1,700
13	Stakeholder Reporting	Partner	Standard rate	Travel	\$ 300	8	\$ 2,400
14	Stakeholder Reporting	Managing Director / Director	Standard rate	Travel	\$ 240	24	\$ 5,760
15	Stakeholder Reporting	Senior Manager	Standard rate	Travel	\$ 215	40	\$ 8,600
16	Stakeholder Reporting	Manager	Standard rate	Travel	\$ 170	8	\$ 1,360

4.1.5 INSERT Resource Hours by Month (consider 8 hours per day and 21 working days per month) -->

Total hours	Month 1	Month 2	Month 3	Month 4	Month 5
2	2				
6	6				
24	24				
8	8				
5		1	2	2	
40	4	12	12	12	0
40	4	12	12	12	0
300	40	120	120	20	
5		1	1	1	2
20	0	5	5	5	5
20		5	5	5	5
10		3	3	2	2
8		2	2	2	2
24		4	4	4	12
40		4	4	4	28
8		2	2	2	2

Key Audit Areas:

	Planning (1 wk)	Audit Fieldwork (16 wks)	Reporting (3 wks)	PM (20 wks)	
6.1 IT operations and governance	4	25	8	6	
6.2 IT project and portfolio management	4	25	8	6	
6.3 Data management	4	60	8	6	
6.4 Application development and maintenance	4	60	8	6	
6.5 Local area network (LAN) infrastructure	4	25	8	6	
6.6 Data integrity	4	60	8	5	
6.7 Security	4	25	8	5	
6.8 IT disaster recovery and business continuity planning	4	40	8	5	
6.9 Incident management	4	25	8	5	
6.10 Areas of high risk and mitigating controls	4	40	8	5	check
	40	385	80	55	560
	0	0	0	0	-