BUSINESS CONFIDENTIAL

ZRA
zeichner risk analytics

ZRA CAPABILITIES STATEMENT

2023 - 2025

GSA

CYBERSECURITY & CRITICAL INFRASTRUCTURE

GSA CONTRACT
47QRAA19D003F

TABLE OF CONTENTS

INTRODUCTION

WHO WE ARE

ZRA is passionate about cybersecurity and dedicated to helping Federal Civilian Executive Branch (FCEB) departments and agencies achieve their cyber and infrastructure security missions. With a legacy of over 25 years supporting the Department of Homeland Security (DHS) and critical infrastructure stakeholders, we have earned a reputation as a trusted partner in delivering exceptional services. Our interdisciplinary team brings together innovative cybersecurity experts, leveraging expertise and diverse backgrounds to pioneer solutions that address risk assessment and mitigation, capability-based planning, IT transformation, compliance implementation, education and coaching.

ZRA was launched in conjunction with the President's Commission on Critical Infrastructure Protection in 1996, serving as support for the Commission and the implementation of Presidential Decision Directive 63. Since then, ZRA leaders and staff have supported Cyber & Infrastructure Security Agency's (CISA) predecessors, including the National Cyber Security Division (NCSD) and the National Protection Programs Division (NPPD). ZRA has proven itself integral in developing CISA's major functions, including the United States Computer Emergency Readiness Team (US-CERT), National Security or Emergency Preparedness (NS/EP) communications, mission engineering, and stakeholder engagement.

Our team is driven by a shared mission to empower organizations to effectively navigate the complexities of cybersecurity. We have built enduring relationships with government agencies, providing invaluable guidance and support to ensure the protection of critical infrastructure and sensitive information in a continually evolving landscape.

WHAT WE DO

ZRA surpasses traditional cybersecurity solutions. We actively drive change to guide organizations towards a secure and resilient future. Our team excels in conducting thorough risk assessments, identifying vulnerabilities, and developing effective risk mitigation strategies. We believe in taking a forward-thinking approach to cybersecurity, enabling our clients to stay one step ahead of emerging threats. By leveraging industry-leading frameworks and methodologies, we ensure that our clients meet compliance requirements and adopt tailored best practices.

Our capability-based planning services empower organizations to chart a clear path towards a robust cybersecurity posture. With a deep understanding of the Federal Government landscape, we assist our clients in aligning their cybersecurity initiatives with their overarching strategic objectives. Leveraging our interdisciplinary expertise, we consider technical, operational, and policy perspectives to design comprehensive solutions that withstand the test of time. Our team takes pride in cultivating a culture of security awareness within organizations by providing education and coaching to equip personnel with the knowledge and skills to effectively combat cyber threats.

HOW WE DO IT

ZRA believes collaboration is the key to achieving success. We work side by side with our clients, forging strong partnerships based on trust, transparency, and shared goals.

- Our client-centric approach begins by thoroughly understanding their unique challenges, enabling us to develop tailored solutions that address their specific needs.
- Our comprehensive methodologies cover the entire cybersecurity life cycle, from initial assessment to ongoing monitoring and improvement. We align our practices with the Systems Engineering Life Cycle (SELC), Acquisition Life Cycle Framework (ALF), and other frameworks mandated by Congress and the Administration.
- Our priority is effective communication. We provide regular updates, progress reports, and actionable insights to ensure that our clients are informed and empowered at every step.
- We perpetually stay ahead of the curve, leveraging the latest best practices and industry trends to deliver innovative cybersecurity solutions. Our interdisciplinary team brings together experts from diverse backgrounds to foster a collaborative environment where innovative ideas flourish.
- We understand that cybersecurity encompasses more than just technology—it involves people, processes, and culture. That is why we place a strong emphasis on education and coaching, empowering our clients to become defenders of their own cybersecurity. We equip clients with the knowledge and skills necessary to make informed decisions, strengthen their security posture, and cultivate a culture of cybersecurity excellence within their organizations.

INTRODUCTION

OUR TEAM

ZRA stands at the forefront of our industry thanks to our exceptional team of cybersecurity professionals. Our team has decades of combined experience, a drive for knowledge, and a passion for excellence. We have assembled a diverse group of experts, including seasoned cybersecurity analysts, risk management specialists, compliance experts, and technology architects. Each team member brings a unique set of skills and perspectives, enabling us to provide comprehensive and interdisciplinary solutions to our clients.

Rigorous training and continuous professional development are integral parts of our team's journey to tackle the latest advancements and challenges in cybersecurity. We foster a culture of collaboration to encourage knowledge sharing and the production of new ideas. By leveraging our collective expertise, we approach complex challenges with creativity and precision. This technically-proficient team is deeply committed to client success. We take pride in delivering exceptional service and building long-lasting relationships based on mutual trust and respect.

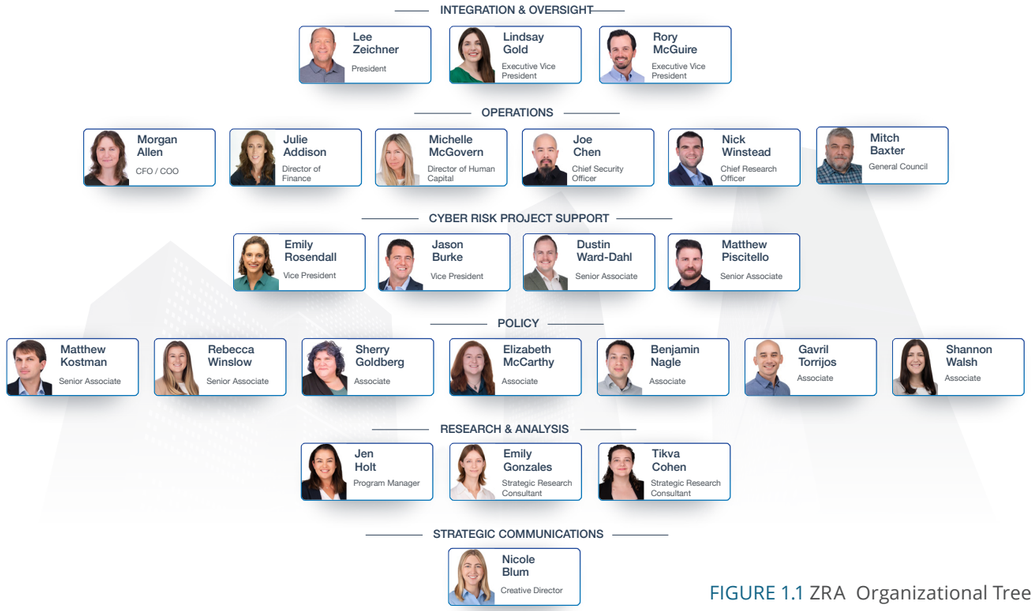


FIGURE 1.1 ZRA Organizational Tree

OUR PAST PERFORMANCE

UNITED STATES DEPARTMENT OF ENERGY (DOE)
SANDIA NATIONAL LABORATORIES (SNL)

Period of Performance:
JUNE 2023 - DECEMBER 2024

Contract Title:
CISA Cyber Support

Customer POC/ Email:
Wendy Dolstra/Wdolstra@sandia.gov

Total Contract Value:
$9,900,000

CPARS Available:
No

- Utilized expertise on Federal Government and DHS policies, directives, and leadership to provide SNL with an understanding of the growing dependence on information infrastructure.
- Provided recommendations on ensuring proper technical deliverables, customer engagements, and strategic planning.
- Conducted analysis on how the Federal Government approaches cybersecurity risk to develop SNL's risk-informed methodologies and metrics for cybersecurity.

UNITED STATES DEPARTMENT OF ENERGY (DOE)
SANDIA NATIONAL LABORATORIES (SNL)

Period of Performance:
MARCH 2019 - MARCH 2023

Contract Title:
CISA Cyber Support

Customer POC/ Email:
Kayla Terry/KTerry@sandia.gov

Total Contract Value:
$20,000,000

CPARS Available:
No

- Tracked changes to policies, directives, and leadership to provide relevant updates to National Technology & Engineering Solutions of Sandia (NTESS).
- Supported NTESS Program Leadership Team by leveraging environment awareness in oversight programs and providing recommendations for strategic planning, technical and programmatic vision, and strategic engagement efforts.

DEUTSCHE BANK (DB)

Period of Performance:
JULY 2016 - OCTOBER 2020

Contract Title:
Cybersecurity Strategy and Threat Assessment

Customer POC/ Email:
Wade Bicknell/ wade.bicknell@db.com

Total Contract Value:
$874,042.90

CPARS Available:
No

- Assisted in the development of DB's Threat Assessment by identifying major cybersecurity threats and providing key benchmarks and metrics for threat mitigation.
- Responded to DB Chief Information Security Officer (CISO) review of existing capability models by addressing risk environment changes and strategic business and management challenges affecting corporate performance.
- Assessed and mitigated cybersecurity risks, pressures to deliver financial and operating efficiencies across stove-piped IT and engineering, and stakeholder management.

UNITED STATES DEPARTMENT OF ENERGY (DOE)
SANDIA NATIONAL LABORATORIES (SNL)

Period of Performance:
MAY 2012 - APRIL 2019

Contract Title:
CS&C Cyber Program Support

Customer POC/ Email:
Pamela Williams/ pwilli@sandia.gov

Total Contract Value:
$19,000,000.00

CPARS Available:
No

- Leveraged unique industry insights and government perspectives on cyber security and risk management to provide guidance and support on SNL's projects with DHS Cybersecurity and Communication (CS&C) Cyber Programs.
- Provided technical writing, quality control, legislative and policy analysis, risk management support, and process definition for supply chain risk management.

NEW ENVIRONMENTAL FACTORS

DYNAMIC THREATS

Cybersecurity threats have grown exponentially since Congress created DHS. Cybersecurity threat actors have persistently attacked FCEB entities for a myriad of objectives: stealing critical information, gaining national security advantages, or undermining the delivery of essential services to the public. These threat actors monitor DHS, FCEB, and the wider stakeholder community to improve their Tactics, Techniques and Procedures (TTPs). Since 2002, ZRA has supported DHS in assessing and protecting against such threat actors. Our work involves integrating FCEB needs with government stakeholders, including Law Enforcement, the Intelligence Community, and the Defense Industrial Base.

COUNTLESS VULNERABILITIES

Over the past 25 years, threat actors have increasingly capitalized on cyber and infrastructure vulnerabilities, especially as the delivery of essential services now relies on resilient and protected information technology platforms. To ensure the safe and secure delivery of products and services, CISA and its FCEB stakeholders must leverage secure platforms and systems. Although Congress and the Administration have authorized and resourced defenses, the ability to resolve vulnerabilities remains challenging due to a lack of vulnerability assessments and mitigation capabilities. ZRA actively supports CISA and FCEB in understanding attack surfaces, resolving vulnerabilities, and planning architecture and platform resiliency. Our goal is to shift the advantage from the attackers to the defenders.

LACK OF RISK MODELS

Threats and vulnerabilities have swiftly expanded, yet the security community has not kept pace in developing repeatable frameworks to effectively manage risks. Risk models play a crucial role in helping Federal Government managers assess unique risks and make informed decisions to mitigate potential attacks. Frameworks are essential and need to be multi-faceted, especially when considering critical factors such as scarce resources and potential consequences. ZRA has provided risk services since the 9/11 attacks. We have proactively gathered and cataloged best practice approaches across the FCEB and broader stakeholder community, applying those practices to meet client-specific needs. Our skills include scenario design and development, risk quantification, and performance measurement.

ENGINEERING CHALLENGES

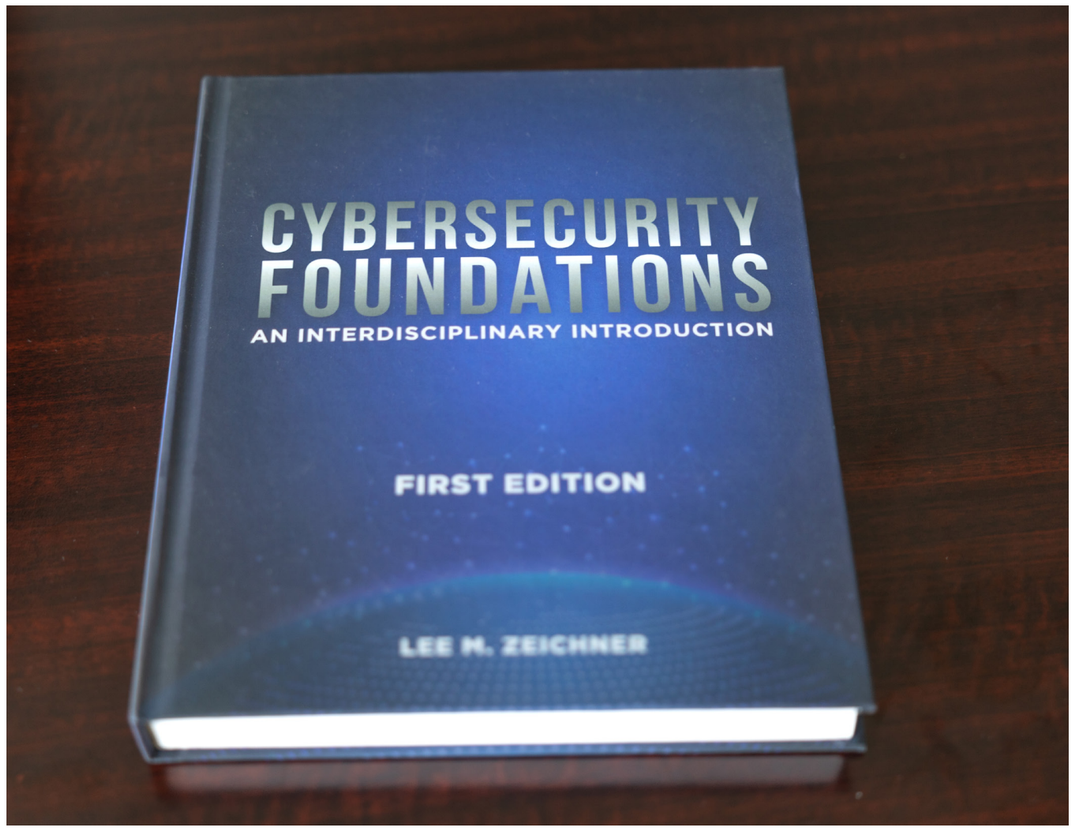
Senior leaders responsible for the nation's cybersecurity increasingly rely on engineering disciplines to design and deploy risk solutions. However, numerous impediments undermine the value and effectiveness of solutions engineering. The complexity of risks, divergent FCEB architectures, and lack of visibility across bureaucratic boundaries pose challenges to DHS and FCEB capabilities. Many of these challenges arise in the initial stages of SELC, necessitating widespread agreement on mission requirements, Needs Analysis, and a well-tailored alternatives analysis. ZRA works to provide solutions by supporting the design and development of key products, including Capability Assessment Reports (CARs), Mission Needs Statements, and a detailed Analysis of Alternatives (AoA).

EVER-EVOLVING IT LANDSCAPE

Digital innovation presents exciting possibilities to support customers and deliver essential products and services more efficiently. However, innovative digital platforms also introduce new vulnerabilities and cybersecurity risks that require careful attention. Cybercriminals and threat actors adapt to exploit these vulnerabilities, aiming to compromise the security and integrity of organizational assets, sensitive data, and overall business operations. ZRA actively monitors IT developments and, with each advancement, provides new ways to leverage security solutions. Most recently, ZRA has supported CISA to understand cloud deployments, utilized telemetry for log aggregation, and collaborated with cloud service providers to enhance transparency and visibility.

SIGNIFICANCE OF CUSTOMER SERVICE EXCELLENCE

In today's digital landscape, customers expect seamlessly-functioning technology. Whether accessing online services, conducting financial transactions, or utilizing applications, uninterrupted IT performance is now a fundamental engineering requirement.
ZRA has over two decades of experience in engineering high reliability systems. Our early work with the National Communications System involved designing engineering requirements to support NS/EP communications. Today, our work involves collaborating with Cloud Service Providers (CSPs) and Internet Service Providers (ISPs) to enable cloud application reliability, mobile phone needs, and other essential mission functions.



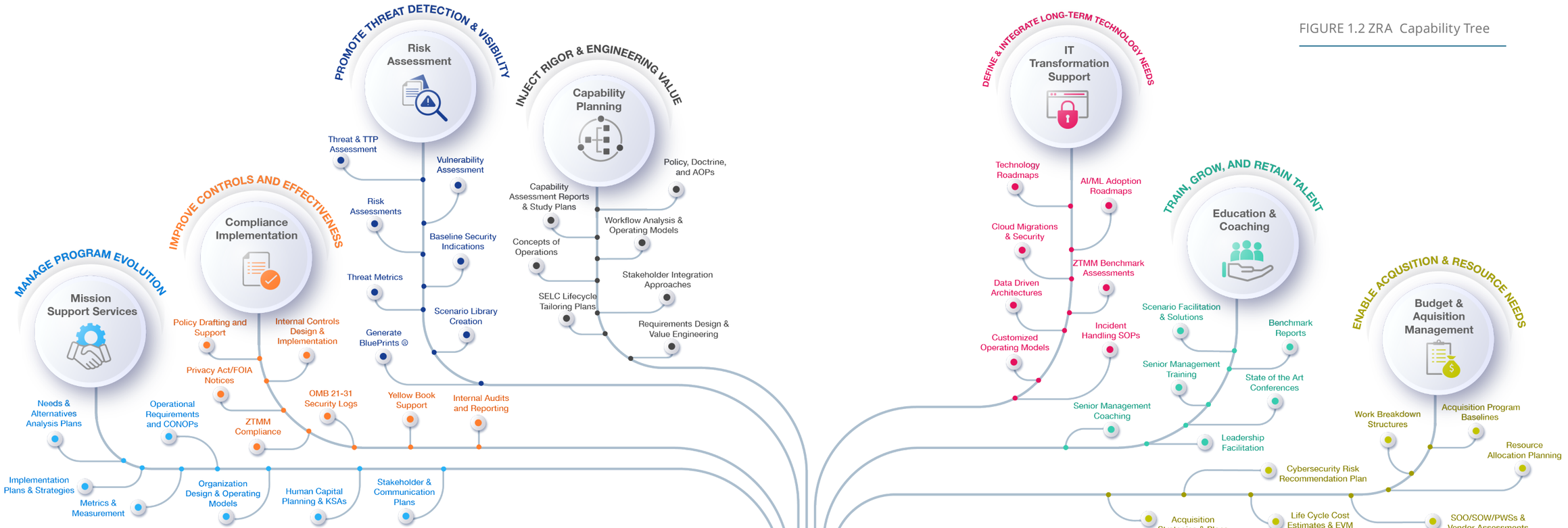
CAPABILITIES

The pursuit of optimal cybersecurity practices requires a comprehensive analysis of an organization's risk profile and the evolving threat landscape. Often limited by the constraints of scarce resources, the ability to make well-informed and effective risk decisions can ensure organizations allocate resources precisely with identified risks, thereby minimizing vulnerabilities and fortifying their cybersecurity posture. ZRA is experienced in helping leaders make smart risk and financial decisions to ensure mission success by offering Mission Support Services, Compliance Implementation, Risk Assessment, Capability Planning, IT Transformation and Support, Education and Coaching, and Budget Acquisition Management.

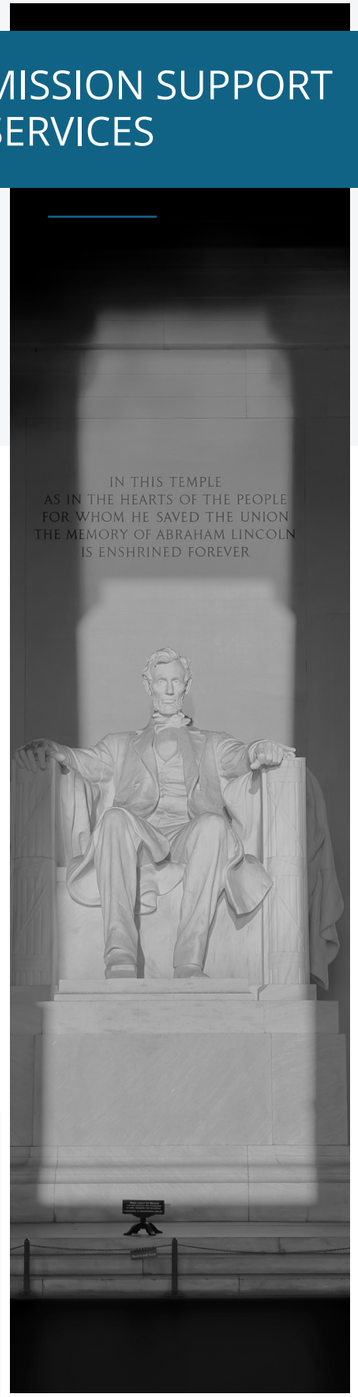
Capabilities Statement

Capabilities

FIGURE 1.2 ZRA Capability Tree



MISSION SUPPORT SERVICES



ZRA specializes in providing comprehensive Mission Support Services for addressing the unique needs of government programs and ensuring successful mission outcomes. With a deep understanding of cybersecurity mission needs and Systems Engineering Life Cycle (SELC) and Acquisition Lifecycle Framework (ALF) approaches, we offer innovative solutions to overcome challenges and optimize program performance. We meticulously analyze client needs, design implementation strategies, and manage program and portfolio risks. We are skilled in addressing operational requirements, establishing organizations, developing Standard Operating Procedures (SOPs), and creating a Concept of Operations (CONOPs) aligned with implementation plans. We measure program progress through metrics and milestones to enable data-driven decision-making. We excel in recommending operating models for efficient communication and collaboration, and we prioritize human capital planning to ensure a skilled workforce. With our expertise, commitment, and proven track record, ZRA is the ideal partner for government entities to achieve their objectives.

Needs & Alternatives Analysis Plans

ZRA specializes in efficiently managing government programs by addressing client needs. Through a formal process, we carefully analyze client requirements to develop alternative models for mission success. Our approach begins with program building, where we identify mission needs and produce detailed Capability Analysis Reports (CARs). This analysis serves as the foundation for understanding client requirements and determining optimal strategies for program implementation.

Implementation Plans & Strategies

Our team excels in developing and executing implementation strategies to meet identified needs. We adopt a comprehensive approach by considering our clients' human capital, organization, technology, processes, and stakeholders. Our implementation plans result in detailed road maps that outline necessary steps, timelines, and dependencies. We utilize tools such as Gantt charts to provide a clear visual representation of the project's progression and define stakeholder roles and responsibilities to establish a collaborative environment that facilitates effective communication and coordination.

Human Capital Planning & KSAs

ZRA recognizes the necessity of having the right people with the necessary skills to achieve successful mission delivery. We prioritize human capital planning to ensure that our clients possess the required knowledge, skills, and abilities (KSAs). We guide our clients in attracting, training, and retaining a talented dedicated workforce. To bolster this critical sector, we offer continuous professional development, talent acquisition, and retention strategies, to establish a workforce that is proficient in the latest technologies and possesses a thorough understanding of the government landscape.

Organization Design & Operating Models

We excel in designing operating models that optimize organizational efficiency and effectiveness. Our approach centers around establishing clear lines of communication and collaboration within the organization. We identify key stakeholders, including Deciders, Advisors, and Informers, and define their roles in decision-making processes. By leveraging our expertise in organizational design, we create structures that promote seamless collaboration, knowledge sharing, and agile decision-making.

Operational Requirements & Concept of Operations (CONOPs)

To fulfill operational requirements, we conduct thorough assessments of technical, physical, functional, and security needs. Our expertise lies in developing system-wide solutions by reviewing implementation plans, integrating best practices, and ensuring compliance with standards. We develop SOPs to serve as guidelines for efficient and consistent operations. We create CONOPs documents to provide a framework that aligns clients with implementation plans and strategies.

Metrics & Measurement

ZRA measures progress and milestones to ensure the success of programs. Our team develops metrics that accurately reflect the mission needs outlined in the implementation plan and operational requirements. Through continuous monitoring of these metrics, we assess whether the program is on track and effectively achieving its objectives. This data-driven approach enables us to make informed decisions and timely corrective action to stay aligned with mission objectives.

Stakeholder & Communication Plans

ZRA specializes in fostering channels of communication between and within organizations to ensure client plan success. We assist in opening dialogues and producing artifacts that facilitate information sharing between stakeholders. We begin by determining the proper leader to best communicate with specific groups. We then guide leaders to facilitate connections, exchange collected information, and inform others of duties or opportunities. We leverage our experience with diverse stakeholders across sectors to enable smooth transmission. Our goal is to empower leaders to facilitate discussion and cooperation amongst their own organization.

RISK ASSESSMENT & MITIGATION

ZRA has helped the Federal Government and critical infrastructure stakeholders assess and manage security risks for over a quarter of a century. Since the 9/11 attacks and subsequent creation of DHS, ZRA has designed methodologies to categorize, quantify, and facilitate informed risk-based decisions across the Systems Engineering Life Cycle (SELC). Our approaches are built upon government and industry best practices, data collection, scenario design, and functional approaches. At the end of this process, ZRA delivers clients with risk Blueprints® to reflect capital assets, analyze high-value functions, and provide mappings of an entity's essential services. ZRA has developed Blueprints® to offer long-term resources for assessing and combating risk as changes occur across the operational landscape.

Threat Assessments & Tactics, Techniques, and Procedures (TTPs)

ZRA offers approaches for collecting, analyzing, and sharing valuable threat data. We provide a formal methodology for assessing risk across any landscape that identifies and mitigates attacker TTPs. Our analysis considers threat actor origination and "threat surfaces"—or where attacks occur across the ATT&CK map—as well as a client's IT, functional, and/or operational business processes. This unique method allows us to pinpoint where, how, and why these threats impact an organization.

Vulnerability Frameworks & Mapping

ZRA has continually developed vulnerability assessments for over a quarter of a century by embracing a range of best practices and risk management tools. Our assessments include End point Detection & Response and vulnerability mapping against High-Value Assets (HVAs) and National Critical Functions (NCFs). We support compliance with Office of Management and Budget (OMB) Memorandum 21-31, which aims to improve the Federal Government's investigative and remediation capabilities related to cybersecurity incidents. ZRA is particularly focused on supporting Event Log Management goals and aligning with the Continuous Diagnostics and Mitigation (CDM) Program. Additionally, ZRA focuses on delivering security data as part of the National Cyberspace Protection System (NCPS), including the collection and telemetry of cloud data and associated vulnerability detection.

High-Value Asset (HVA) Blueprints®

ZRA developed functional Blueprints® as a deliverable for all client risk assessments. These Blueprints® — akin to those created in the construction industry — furnish cybersecurity information cruical to critical service delivery, including data storage, IT systems, internal business processes, and key stakeholders. Each Blueprint® is tailor-made to cater to HVAs, essential customer services, and critical infrastructure assurance. These Blueprints® empower clients to make complex decisions by viewing the whole of their operations. In partnering with ZRA, senior leaders, managers, and decision-makers can utilize Blueprints® as a foundation for informed risk decision-making.

Baseline Security Metrics

ZRA boasts a remarkable history of assisting clients in designing and implementing Baseline Security Metrics. These metrics are derived organically from either new risk assessments or pre-existing leadership requirements and expectations. Program managers have the flexibility to incorporate Baseline Security Metrics into Zero Trust Maturity Models (ZTMM) as well as adhere to OMB and CISA Directives, such as Binding Operational Directives, security log reporting, or portfolio risk calculations.

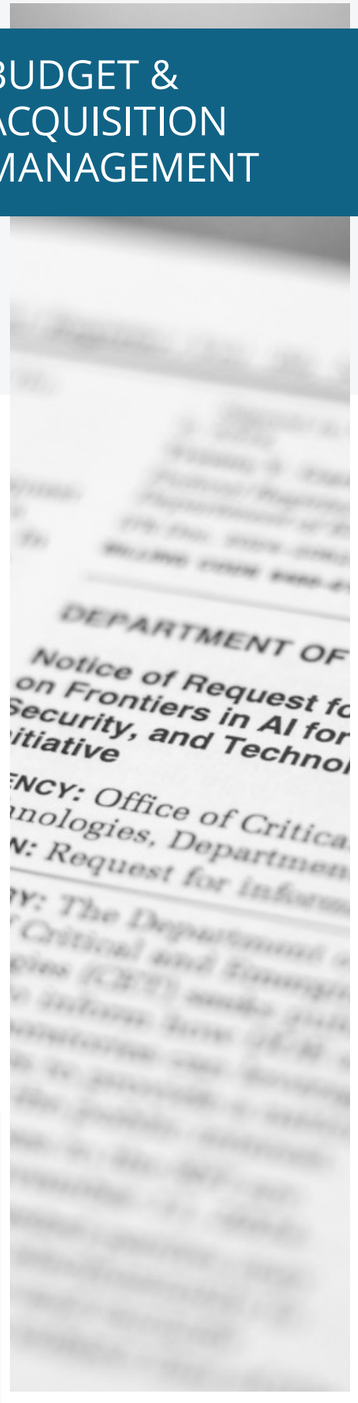
Customized Scenario Library

ZRA excels in creating scenario libraries that facilitate risk assessment, quantification, and management decisions. We have experience tailoring scenarios specifically for FCEB entities by generating a comprehensive set of assumptions and risk data. Our long-established history has allowed us to amass a substantial collection of national security, critical infrastructure, and cybersecurity scenarios. FCEB clients can leverage our Scenario Library to conduct a thorough analysis of portfolio risk and generate valuable qualitative and quantitative data to inform risk decisions. Our methodology is built upon best practices from the Federal Government, industry, and professional associations which address FCEB risk-related needs.

Leadership Decision Briefs & Memorandum

A crucial aspect of ZRA's mission support is helping government leaders comprehend the implications of significant decisions. Our team understands the multifaceted nature of such decisions that involve financial, operational, managerial, and compliance considerations. We assist managers in preparing decision briefs and memorandum that outline various decision options. Our team of experts effectively and clearly communicates complex variables to CISA and DHS leadership. Our formal approaches are based upon our exhaustive understanding of past programs, areas for improvement, and the specific needs of leadership.

BUDGET & ACQUISITION MANAGEMENT



ZRA excels in providing support for cybersecurity program budget and acquisition requirements. In recent years, DHS and CISA have significantly advanced budget and acquisition doctrines. Cybersecurity programs now heavily rely on system engineering disciplines to effectively plan, acquire, deploy, and operate sophisticated cybersecurity and infrastructure protection systems. These programs leverage formal frameworks such as DHS's Systems Engineering Lifecycle (SELC), the Acquisition Lifecycle Framework (ALF), and Planning, Programming, Budget, and Execution (PPBE). ZRA holds a comprehensive understanding of such cybersecurity principles and the essential management frameworks necessary to meet complex mission requirements.

Acquisition Program Baselines (APB)

DHS and leading critical infrastructure companies have designed novel models for acquisition program baselines, many of which ZRA leverages in support of our customers. Since 2002, ZRA has met the requirements of each major APB element, including cost, schedule, and milestones. Our experience within DHS, and particularly with CISA, goes beyond the creation of a single program APB. We ensure traceability across numerous projects and activities that contribute to the overall APB. Our analytics are based on Key Performance Indicators (KPIs) to provide insights for assessing and course correcting as program leaders gain knowledge during the stages of design, deployment, and operations.

Earned Value Management (EVM)

ZRA has developed and utilized EVM models for over 25 years. These models are tailored to address the design and implementation of cybersecurity programs within the Federal Civilian sector, with a focus on performance challenges encountered in government-wide initiatives. Our EVM models and frameworks adhere to the requirements outlined in OMB A-11 and the OMB 300 exhibit. In partnership with DHS, ZRA assisted in the formulation of performance measures, metrics, and cost-based outputs that align with program requirements and expectations. Our unique model integrates cost estimation approaches to ensure a comprehensive view of program outputs and offer CISA leaders valuable innovation for accounting for service-related considerations in program performance.

Acquisition Strategies & Plans

ZRA assists Program Managers and other leaders in preparing Acquisition Strategies and Plans by leveraging a deep understanding of cybersecurity-specific acquisition approaches. ZRA was integral to the original acquisition design team of the NCPS and CDM. With this background and a comprehensive knowledge of emerging trends, ZRA continues to incorporate key elements into acquisition approaches, including IT Modernization, cloud adoption, and increasingly significant, innovative technologies such as Operational Technologies (OT) and cloud telemetry.

Capabilities Statement

ZRA Core Services

Vendor Engagement & Assessments

ZRA provides assistance for vendor-related engagements. As part of our comprehensive service, we work closely to help program leaders understand strategic, functional, operational, technical, and physical requirements. We prepare Requests for Information (RFIs) to reveal ways in which vendors can meet requirements and deliver novel approaches that government customers can leverage. Building on these services, ZRA further aids in the development of Statements of Objectives (SOOs), Statements of Work (SOWs), and Performance Work Statements (PWSs). We conduct Vendor Assessments and other requirement artifacts and are experienced in analyzing vendor capabilities for cloud telemetry, deception, and event log management. Recently, we assisted CISA programs in designing RFIs for Artificial Intelligence (AI), Large Language Models (LLM), and Natural Language Processing (NLP).

Resource Allocation Planning (RAP)

ZRA provides support to CISA leaders by assessing both short-and long-term resource needs, including RAP, Program Decision Options (PDO), and related efforts. We address emerging threats and vulnerabilities, complex IT requirements across FCEB stakeholders, and the expanding mission of CISA in supporting critical infrastructure owners. Our past performance with CISA has proven our understanding of priorities such as Resource Planning Guidance (RPG), identifying mission needs, framing requirements as capabilities, and identifying gaps. We continue to excel in quantification, cost estimation, and the facilitation of engagement across diverse CISA programs. We analyze Capability Assessment Reports (CARs) and Capability Assessment Study Plans (CASPs) and gather input from CONOPs and AoAs. These collective efforts enable us to shape RAP options and propose appropriate solutions.

Work Breakdown Structures (WBS)

ZRA specializes in creating Project Work Breakdown Structures (PWBS) and Contract Work Breakdown Structures (CWBS). Our WBSs deliver valuable insights thanks to our experience in cybersecurity program management and understanding of cybersecurity requirements, cost accounting, and program performance. These deliverables enable CISA leaders to visualize program needs and align them with critical decisions such as resource allocation, capability planning, and long-term acquisition strategies. ZRA has successfully designed PWBS and CWBS for several of CISA's most significant programs, as well as ongoing projects that have the potential to become Programs of Record. In each case, our WBS products adhere to best practices in cost accounting and establish clear traceability from mission needs to program activities by utilizing Integrated Master Schedules and other project artifacts that are central to CISA and DHS program management doctrines.

Life Cycle Cost Estimates (LCCE) & Earned Value Management EVM

ZRA specializes in performing LCCE analysis for cybersecurity and infrastructure security programs. With extensive experience as part of DHS Program Management Offices (PMOs) for over 25 years, ZRA has provided support to government leaders by designing and developing LCCEs. These LCCEs play a crucial role in program planning, including RAP, PDO, decision options, and AoA testing for long-term program planning. ZRA's LCCEs also provide valuable insights for Independent Government Cost Estimates (IGCEs) related to complex cybersecurity and infrastructure security services.

CAPABILITY BASED PLANNING

ZRA applies Capability-Based Planning practices to support CISA by leveraging our expertise in cybersecurity and infrastructure security programs. Our performance encompasses a wide range of products and services that are built upon rigorous Capability-Based Planning methodologies. We have developed formal models and processes that seamlessly integrate CISA policy and doctrine, program artifacts, and stakeholder requirements to ensure alignment with frameworks and mission expectations.

eCapability Assessment Reports (CARs) & Study Plans (CASPs)

ZRA utilizes eCARs and CASPs to support program success at CISA. As mission requirements evolve and new gaps arise, it is imperative to identify and effectively address gaps. ZRA has a long-standing history of assisting cybersecurity program leaders in defining capability gaps and aligning objectives with DHS doctrine. Our CASP approaches are built upon previous decisions, terminologies, and capability methodologies established by CISA and DHS. Through our comprehensive CAR and CASP approaches, CISA managers, technical experts, and leaders can explore diverse options and integrate their decisions into well-rounded CAR and CASP documents.

Requirements Design & Value Engineering

ZRA collaborates closely with requirements engineers to support the production of an Operational Requirements Document (ORD). Our experience designing and producing cybersecurity ORD allows our team to seamlessly manage the transition from CONOPs to ORD design. We have a record of assisting program managers develop comprehensive ORD products that encompass technical, operational, functional, and security requirements. ZRA establishes a formal framework and process for gathering input, exploring different approaches to ORD, and effectively managing teams to deliver high-quality ORD end products that can be utilized throughout SELC and ALF.

Workflow Analysis & Operating Models

Due to CISA's expanding expectations and mission requirements, ZRA has increasingly provided guidance to CISA managers and leaders on workflow and operating models. Our operating model design considers the involvement of new stakeholders, evolving requirements, and the adoption of agile methodologies. Our Operating Models offer reliability and integration across a plethora of mission needs and multiple CISA and FCEB stakeholders. Our workflow analysis offers managers and leaders opportunities to enhance engineering and operational collaboration, which are critical for meeting CISA's evolving mission needs.

Concepts of Operations (CONOPS)

Along side CAR and CASP support, ZRA has developed management frameworks to design program and organizational CONOPs. Our processes prioritize a deliberate and incremental analysis of needs to incorporate concepts that operationalize CISA priorities into manageable activities. ZRA has developed CONOPS capable of meeting the requirements of the Cyber Incident Reporting for migration for the NCPS, CDM, and Incident Handling. ZRA bolsters its catalog by transforming threat analysis into existing CONOPS-related products. Our Operating Models are derived from industry and government best practices to facilitate the definition of roles and responsibilities, ensure the successful development of systems, and integrate diverse capabilities from CISA stakeholders.

Systems Engineering Life Cycle (SELC) & Solutions Engineering

ZRA provides comprehensive support across all phases of SELC. We bring expertise to solutions engineering and play a crucial role in supporting the production of a SELC Tailoring Plan. Our portfolio highlights an emphasis on program planning and design phases, including Study Plan Reviews, Solution Engineering Reviews, Project Planning Reviews, and Systems Definition Reviews. Throughout the Design phase, ZRA continues to support similar work products and present compliance and oversight materials to senior leaders at CISA and DHS. We draw on our expertise in producing APB, ORD, and EVM offerings to contribute to operational readiness reviews.

Policy, Doctrine, and Annual Operating Plans (AOPs)

ZRA's Operating Models offer unique expertise in the development of Policy, Doctrine, and AOPs. We have collaborated closely with DHS and CISA to support program leaders in the implementation of new and innovative programs. Our AOP support is particularly valuable as CISA expands its mission and seeks to incorporate innovative technology and security solutions. Leveraging our expertise in CISA policy, we assist in integrating policy requirements into AOP language and approaches. Our support for CISA managers extends beyond AOP design to encompass the integration of stakeholder contributions, alignment with RAP and PDO, and utilization of policy priorities, such as those outlined in the RPG.

Stakeholder Integration Approaches

ZRA actively supports the design and facilitation of stakeholder integration. Our Operating Models and Workflow Analysis enable us to identify gaps, address needs, and capitalize on opportunities to meet the unification expectations of CISA. We have successfully implemented manager directives and met expectations through our comprehensive stakeholder engagement support services. Our frameworks and approaches prioritize engineering and operational collaboration. We highlight the significance of enhancing technical collaboration within CISA and fostering partnerships with other DHS entities, such as Science & Technology, the Intelligence Community, Federally Funded Research and Development Centers (FFRDCs), and University Affiliated Research Centers (UARCs). To facilitate technical deliberations, discussions, and outputs for CISA leaders, we employ various planning options, including forward-leaning conferences and other interactive events. Recently, we have supported stakeholder engagements in cyber-tool development, software design, and climate risk.

IT TRANSFORMATION

ZRA specializes in assisting departments and agencies within FCEB to harness innovative cybersecurity technologies. The rapid pace of digital innovation, especially in cybersecurity, presents significant challenges. While it is essential to conduct thorough needs analysis, define requirements, and carefully plan resource distribution, they alone are not sufficient. ZRA takes a comprehensive approach to emphasize active engagement to refine user needs. We tailor roadmaps that align with each organization's unique culture and existing investments, incorporating Agile methodology, SELC, and ALF processes. Our consultancy and deliverables focus on supporting initiatives such as NCPS, CDM, cloud migrations, and incident handling. With ZRA as a trusted partner, clients can confidently navigate the complexities of digital innovation and achieve cybersecurity goals with optimal efficiency and effectiveness.

Technology Roadmaps

ZRA specializes in crafting technology roadmaps that seamlessly incorporate and integrate new and innovative solutions. Our expertise lies in designing roadmaps that consider diverse perspectives, ranging from user needs to the objectives of executive officers, including Chief Information Officer (CIO), Chief Technology Officer (CTO), Chief Financial Officer (CFO), Chief Audit Executive (CAE), and Chief Human Resources Officer (CHRO). We ensure that our roadmaps align with an organization's existing technology architectures while also considering future-forward investments. By leveraging our experience and knowledge, we can assist in charting a clear and strategic path towards achieving technology objectives.

Cloud Migrations & Security

ZRA has dedicated critical time and resources to support FCEB entities in migrating to the cloud. ZRA has extensive involvement in implementing Federal Risk and Authorization Management Program (FedRAMP) requirements including requirement formulation, design of data architectures, and collaboration with leading cloud service providers to streamline data sharing and Request for Proposals (RFPs). ZRA's current focus is on identifying critical security data requirements and devising strategies to leverage telemetry for comprehensive analysis, seamless sharing, and streamlined reporting.

AI/ML Adoption Roadmaps

ZRA collaborates with FCEB agencies to thoroughly comprehend specific requirements on adopting and harnessing Artificial Intelligence (AI) and Machine Learning (ML) technologies. Our ongoing initiatives involve conducting comprehensive needs analysis, exploring the distinctive capabilities of Large Language Modeling (LLM) and Natural Language Processing (NLP), and devising intelligent contracting strategies to engage with a diverse array of providers.

Zero Trust Maturity Model (ZTMM) Assessments

ZRA offers invaluable assistance to FCEB agencies in conducting benchmark assessments for Zero Trust Maturity Models (ZTMM). Our expertise lies in guiding organizations through the evaluation process, assessing Zero Trust maturity, and identifying areas for improvement. We work closely with FCEB entities to evaluate various aspects of their security posture, including network architecture, access controls, identity management, data protection, and monitoring. Our comprehensive approach incorporates factors such as visibility, automation, analytics, and governance to provide a holistic assessment of Zero Trust implementation. Through our guidance, FCEB entities gain insight into their strengths and weaknesses, develop a roadmap for advancing Zero Trust maturity, and enhance overall cybersecurity resilience objectives.

Data Driven Architectures

ZRA closely collaborates with FCEB entities to facilitate the implementation of robust and effective Data-Driven architectures. Leveraging our expertise and industry best practices, we guide agencies through the entire process, starting with the initial assessment of data needs and requirements. Our approach includes designing and deploying scalable data integration frameworks, establishing secure and efficient data storage solutions, implementing advanced analytics capabilities, and ensuring comprehensive data governance and security measures. We work collaboratively with FCEB entities to customize data-driven architectures for their specific organizational needs, leveraging emerging technologies and data-driven insights to drive informed decision-making and strategic outcomes. Through partnership with ZRA, FCEB entities can harness the power of their data assets to foster a culture of data-driven innovation for achieving tangible results.

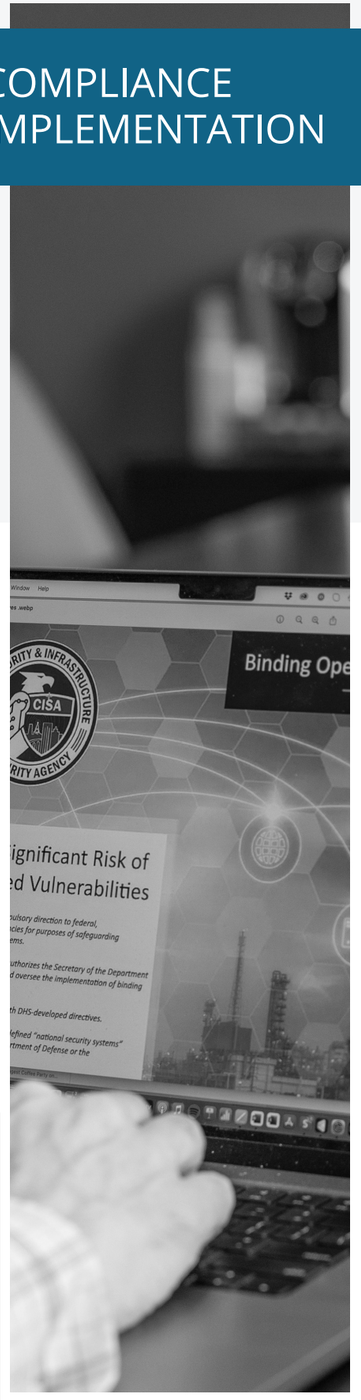
Customized Operating Models

As a trusted management and engineering consulting firm, ZRA is dedicated to assisting FCEB entities negotiate customized Operating Models to drive operational excellence. Seamless collaboration across various organizations is critical to designing any cybersecurity support function. We guide FCEB entities in evaluating stakeholder requirements and exploring optimal strategies to achieve engineering value and operational efficiencies. Our well-established model has undergone rigorous testing and proven effective in both public and private sectors, affirming an ability to deliver remarkable results. ZRA provides comprehensive support in crafting tailored Operating Models that meet the unique needs of client organizations to foster success.

Incident Handling Standard Operating Procedures (SOPs)

For over 25 years, ZRA has been at the forefront of assisting organizations in the development of comprehensive incident handling SOPs. Our expertise extends to significant entity-establishing initiatives, such as our instrumental role in creating US-CERT, the National Cybersecurity and Communications Integration Center (NCCIC), and new operating entities at CISA, including threat hunting. Leveraging our deep understanding of incident handling best practices and industry standards, we closely collaborate with organizations to design tailored SOPs. These SOPs empower organizations to respond to security incidents, minimize the impact of breaches, and enhance overall cybersecurity resilience proactively and efficiently. With ZRA as a partner, clients benefit from our experience, proven methodologies, and unwavering commitment to helping develop SOPs which meet the highest standards of incident handling.

COMPLIANCE IMPLEMENTATION



Efficient compliance implementation is vital for organizations across both the government and private sectors to ensure strict adherence to statutory, administrative, and regulatory requirements. ZRA specializes in providing comprehensive support and expertise in seamless compliance implementation. We understand the intricacies involved in translating complex regulatory mandates into practical and actionable measures that harmonize with an organization's unique operations and objectives. Collaborating closely with clients, our seasoned experts conduct thorough assessments of existing processes to pinpoint gaps and devise customized strategies for achieving and sustaining compliance. We guide clients through every step by assisting in designing and implementing the necessary controls, policies, and procedures. We also deliver comprehensive training and ongoing support to guarantee a thorough understanding and steadfast adherence to the compliance framework. By partnering with ZRA, clients can streamline compliance efforts, minimize risk, and cultivate a pervasive culture of unwavering compliance throughout an organization. Whether in the public or private sector, our unwavering goal is to empower organizations to meet regulatory obligations while optimizing operational efficiency, bolstering reputation, and inspiring unwavering trust among stakeholders.

Policy Drafting & Support

ZRA specializes in providing comprehensive policy drafting and support services designed to meet the needs of both government entities and the private sector. We understand the distinct requirements and compliance standards of both sectors, enabling us to develop policies that align with respective goals and regulations. Our team of experts closely collaborates with clients from government agencies and private organizations to ensure the policies we create are tailored to their specific needs. Whether clients require policies related to security, data privacy, human resources, or any other area, ZRA customizes these policies to address the unique challenges and compliance obligations you face. Our goal is to support clients in establishing and maintaining effective policies that enhance operational efficiency, mitigate risks, and ensure compliance with applicable laws and regulations in the public and private spheres. With ZRA's ongoing support, client policies will remain current and relevant, enabling clients to navigate the dynamic landscape of government and private sector operations with confidence.

Privacy Act/Freedom of Information Act (FOIA) Notices

ZRA specializes in providing comprehensive Privacy Act/FOIA notice services to help organizations adhere to privacy regulations and maintain transparency while protecting sensitive information. We understand the complexities of privacy laws and the critical importance of providing clear and accurate notices to individuals whose data is collected. Our team collaborates with clients to assess data practices, identify relevant legal requirements, and develop tailored Privacy Act/FOIA notices. With ZRA's expertise, clients can enhance transparency within their organization, build trust with stakeholders, and ensure compliance with applicable privacy regulations.

Internal Audits and Reporting

Effective internal audits play a crucial role in providing organizations with insights into operations, identifying areas for improvement, and ensuring compliance with regulatory requirements. ZRA offers comprehensive internal audit and reporting services tailored to client needs. Our experienced auditors conduct thorough assessments of client processes, controls, and systems to provide objective and independent evaluations. We deliver detailed reports that highlight areas of strength and opportunities for enhancement alongside actionable recommendations to drive positive change. By partnering with ZRA for internal audits and reporting, clients can enhance their organization's governance, risk management, and overall operational effectiveness.

Zero Trust Maturity Model (ZTMM) Compliance

ZRA specializes in providing comprehensive ZTMM compliance services to help organizations from both the public and private sectors establish and maintain robust security measures. Navigating complex ZTMM compliance measures can be a daunting task, but our team of experts is well-versed in the principles and requirements outlined in the ZTMM framework. We guide clients through each stage of the compliance journey, ensuring that the organization meets the rigorous standards set forth by ZTMM. From assessing current security posture to designing and implementing necessary controls and processes, we collaborate closely with clients to strengthen cybersecurity defenses. By partnering with ZRA, clients can minimize risk, enhance their organization's resilience against cyberthreats, and demonstrate an unwavering commitment to protecting sensitive data and systems. Our goal is to empower organizations to achieve and maintain ZTMM compliance, enabling clients to navigate the ever-evolving cybersecurity landscape with confidence and peace of mind.

Office of Management and Budget (OMB) 21-31 Security Logs

ZRA specializes in providing comprehensive Zero Compliance with OMB Memorandum 21-31, which outlines new requirements for federal agencies' security logging practices and is of paramount importance for organizations operating in both public and private sectors. We understand the intricacies involved in implementing robust security logging practices and the necessity of accurate and thorough record-keeping. Our team collaborates closely with clients to assess current security logging capabilities, identify gaps, and develop and implement strategies to align with the requirements specified in OMB Memorandum 21-31. By partnering with ZRA, clients can ensure that security logs are compliant and able to effectively monitor and respond to security incidents. With ZRA, clients can enhance their organization's cybersecurity posture, bolster incident response capabilities, and demonstrate commitment to maintaining the highest level of data security and integrity.

Internal Controls Design & Implementation

Establishing strong internal controls is crucial for organizations in both the government and private sectors to help mitigate risks, ensure compliance, and optimize operational efficiency. ZRA specializes in providing expert services for designing and implementing tailored internal controls for an organization's specific needs and objectives. Our experienced team conducts a comprehensive assessment of business processes, identifies areas of vulnerability, and designs robust controls to address those risks. We collaborate closely with clients to seamlessly integrate controls into existing operations, providing training and ongoing support to ensure effective implementation. With ZRA's expertise, clients can enhance the integrity of their operations, safeguard assets, and promote a culture of compliance and accountability. Our goal is to assist organizations in establishing effective internal controls that support strategic objectives while mitigating risks and ensuring regulatory compliance.

Yellow Book Support

Compliance with the Generally Accepted Government Auditing Standards, commonly referred to as the Yellow Book, is essential. ZRA specializes in providing comprehensive support and expertise to ensure clients meet the rigorous requirements of the Yellow Book. Our team of experts hold a complete understanding of the principles and guidelines outlined in the Yellow Book to guide clients through the entire compliance process. We work closely with organizations to assess current practices and develop tailored remediation strategies that align auditing and reporting processes with Yellow Book standards. Whether clients operate in the government or private sector, ZRA can enhance the quality and credibility of audits, strengthen accountability, and demonstrate an unwavering commitment to upholding the highest professional standards. Our goal is to support clients in achieving Yellow Book compliance to instill confidence during audits, enable transparency, and boost integrity to financial operations and reporting practices.

EDUCATION & COACHING

ZRA is a leader in providing management consulting services to enable security leadership, with expertise trained through close collaboration with CISA and DHS managers. We have a history of over 25 years in contractual work with critical infrastructure owners and operators, including the design of leadership facilitation and training programs that specifically address security challenges. Our Education & Coaching support services therefore recognize the complex missions that CISA and its stakeholders must fulfill by incorporating exceptional management, operational, and engineering practices essential for CISA's missions.

Leadership Facilitation

ZRA offers Leadership Facilitation support services which directly address management challenges faced by leaders and senior managers. These scenarios encompass those encountered at CISA and throughout the broader stakeholder community and put management practices and leadership values to the test. Our programs not only facilitate discussions on best practices in security leadership but also provide management frameworks applicable to daily experiences at CISA. Our approaches incorporate policies and practices specific to cybersecurity and infrastructure security scenarios, including strategic risk management, long-term portfolio risk, and strategies for garnering trust and engagement on complex cybersecurity issues. CISA leaders can utilize ZRA's facilitation sessions to tackle both short-term operational issues and strategic problems.

Senior Management Training

ZRA's Senior Management Training focuses on addressing the unique challenges faced by mid- and senior-level managers across CISA portfolios. Our programs for senior managers, such as Leadership Facilitation, emphasize both daily and strategic challenges common throughout CISA's mission and stakeholder community. These programs include designing program fundamentals, exploring operating models for stakeholder engagement, and enhancing communication with leaders, managers, and the broader workforce. Our scenario facilitation sessions further underscore the significance of CISA doctrine, culture, and mission priorities. Additionally, ZRA administers the Insights Discovery Test, enabling participants to gain deeper insights into themselves and their crucial job functions.

Senior Management Coaching

ZRA provides professional coaching experiences to cyber and infrastructure security leaders and managers. We collaborate with International Coaching Federation (ICF) certified coaches to deliver programs that offer coaching support while incorporating a deep understanding of the unique challenges faced by CISA and the stakeholder community. Our programs leverage the expertise of ICF certified coaches to provide effective coaching support by introducing real-world scenarios and best practices. ZRA enhances the abilities of individual Senior Managers by guiding them through their Insight Discovery Test as it applies to real-world scenarios.

Capabilities Statement

ZRA Core Services

Literature & Benchmark Reports

ZRA's Education & Coaching support programs include focused sessions on designing and delivering cybersecurity literature reviews and benchmark assessments. As the field of cybersecurity research is relatively new, newcomers may face challenges in navigating this practice. ZRA provides detailed processes and frameworks to help managers learn essential practices related to cybersecurity research, including the ability to utilize efficient methodologies to draw defensible and relevant conclusions for senior managers.

State of the Art Facilitation & Workshops

ZRA designs and implements state-of-the-art workshops that delve into relevant cybersecurity areas of concern. ZRA's state-of-the-art approach involves designing workshops that uncover critical findings and foster stakeholder cohesion and long-term collaboration on the given topic. Our background features a diverse range of experiences, including cybersecurity risk underwriting, software engineering for critical missions, and cybersecurity tool development. Our facilitation and workshops include pre-workshop white papers, facilitation materials, and post-workshop findings and conclusions.

Scenario Facilitation & Solutions

ZRA has over a quarter of a century of experience providing scenario facilitation and support services. Our Scenario Library consists of over one hundred scenarios that cover a wide range of topics, including cybersecurity, infrastructure security, NS/EP Communications, epidemiological surveillance, and operational preparedness, response, and restoration activities across critical infrastructure sectors. When facilitating scenarios, ZRA applies best practices for facilitation, drawing on our extensive knowledge of cybersecurity practices. We incorporate tools such as Insight Testing to support the continual growth and development of our clients.

Management Best Practice Roundtables

ZRA has extensive experience designing and implementing roundtables dedicated to exploring best practices in the field of homeland security. Management Best Practices roundtables organized by ZRA involve locating, convening, and facilitating discussions among diverse stakeholders. ZRA's expertise provides models for conducting multiple roundtables in areas that require the identification of best practices and stakeholder awareness and engagement. ZRA has designed roundtables on best practices, methodologies for deriving critical findings, and approaches to involving stakeholders. Our roundtables cover diverse topics, including CEO risk management approaches, board of director risk oversight practices, and financial practices for resourcing large-scale cybersecurity programs.

ACRONYMS

ALF: Acquisition Lifecycle Framework

AI: Artificial Intelligence

AOA: Analysis of Alternatives

AOPs: Annual Operating Plans

APB: Acquisition Program Baselines

CAE: Chief Audit Executive

CARs: Capability Assessment Reports

CASPs: Capability Assessment Study Plans

CDM: Continuous Diagnostics and Mitigation

CFO: Chief Financial Officer

CHRO: Chief Human Resources Officer

CISA: Cyber & Infrastructure Security Agency

CIO: Chief Information Officer

CISO: Chief Information Security Officer

CONOPS: Concept of Operations

CS&C: Cybersecurity and Communication

CSPs: Cloud Service Providers

CTO: Chief Technology Officer

CWBS: Contract Work Breakdown Structures

DB: Deutsche Bank

DHS: Department of Homeland Security

DHS CS&C: Department of Homeland Security Cybersecurity and Communication

DOE: Department of Energy

EVM: Earned Value Management

FCEB: Federal Civilian Executive Branch

FEDRAMP: Federal Risk and Authorization Management Program

FFRDCs: Federally Funded Research and Development Centers

FOIA: Freedom of Information Act

HVA: High-Value Asset

ICF: International Coaching Federation

IGCEs: Independent Government Cost Estimates

ISPs: Internet Service Providers

KPI: Key Performance Indicator

KSAs: knowledge, skills, and abilities

LCCE: Life Cycle Cost Estimates

LLM: Language Modeling

ML: Machine Learning

NCCIC: National Cybersecurity and Communications Integration Center

NCF: National Critical Function

NCPS: National Cyberspace Protection System

NCSD: National Cyber Security Division

NLP: Natural Language Processing

NPPD: National Protection Programs Division

NS/EP: National Security or Emergency Preparedness

NTESS: National Technology & Engineering Solutions of Sandia

OMB: Office of Management & Budget

ORD: Operational Requirements Document

OT: Operational Technologies

PDO: Program Decision Options

PMOs: Program Management Offices

PPBE: Planning, Programming, Budget, and Execution

PWBS: Project Work Breakdown Structures

PWSs: Performance Work Statements

RAP: Resource Allocation Planning

RFI: Request for Information

RFPs: Request for Proposals

RPG: Resource Planning Guidance

SELC: Systems Engineering Life Cycle

SNL: Sandia National Laboratories

SOOs: Statements of Objectives

SOPs: Standard Operating Procedures

SOWs: Statements of Work

TTPs: Tactics, Techniques and Procedures

UARCs: University-Affiliated Research Centers

US-CERT: United States Computer Emergency Readiness Team

WBS: Work Breakdown Structures

ZTMM: Zero Trust Maturity Model

Address
4601 Fairfax Drive
Suite 1130
Arlington, VA 22203

General Inquiry
contact@zra.com
Phone: (703) 351-1101
Fax: (703)-351-1109

Contract Management
Morgan Allen
mallen@zra.com
Phone: 703-351-1101