What does the CISO role look like now?

Ever since I was asked to take on the responsibilities of a role called the Chief Information Security Officer years ago, I have been asking the question, "Can someone explain this job to me?" I have found that there is no clear and concise answer. I also have discovered it is rapidly changing as fast as it can be defined. There is the EC-Council's Body of Knowledge for their Certified/CISO Certification. It focuses on 5 domains: Governance, Security Risk Management, Controls, and Audit Management, Security Program Management and Operations, Information Security Core Competencies, and Strategic Planning, Financial Management, and Vendor Management. I don't disagree that these high-level areas are very important for success in the CISO role. However, there is a framework out there that really describes the Cybersecurity roles in immense detail: Cybersecurity Workforce Framework (CWF). So, I thought how does CWF describe this elusive role?

Now before we take this journey, I have seen many people and organizations passionately describe the CISO role. So, clearly there are connotations already out in the environment about "what is a CISO". Additionally, where in the organization should the role reside? So, to avoid these prejudices, I will not call it CISO. What is the KEY objective of the CISO (not all the functions, knowledge, skills, abilities, tasks, certifications, experience, education, etc.)? It is to understand and drive their respective organization to inspirationally achieve and maintain Cybersecurity Awareness and Resiliency (CAR) state. This entity accomplishes this analysis of evidence that proves the organization operates in this fluid state of CAR. So, to put it succinctly, this person is the organizational

Cybersecurity Data-Driven Decision Entity (CDDDE)

So, how do we articulate this role? Let's see what CWF says….

Job Title: Cyber Policy, Strategy, Governance, Workforce Development and Executive Leadership

Job Description: Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work for itself or its customers. The CDDDE has many "masters": the CIO, the General Counsel, the Chief Compliance Officer, the Chief Risk Officer, Chief Procurement Officer, Chief of Contracts, the Executive leading the organizational mission/business, the Chief Operating Officer, the CEO and, of course, in a corporate setting, the Board of Directors. In a Public Sector context, the CDDDE reports to the agency leadership or Command in support of this mission function. Develops cyberspace plans, strategy and policy support and align with organizational cyberspace missions and initiatives. Executes decision-making authorities and establishes the vision and direction for an organization's cyber and cyber-related resources and/or operations. While executing this specific mission of "Oversee and Govern," the CDDDE must also be cognizant of all other cyber

categories: Securely Provision, Operate and Maintain, Protect and Defend, Analyze, Collect and Operate, and Investigate.

Primary Responsibilities: Provides legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain. Advocates legal and policy changes and makes a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings. Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers and/or evaluates training courses, methods, and techniques as appropriate. Oversees the cybersecurity program of an information system or network, including managing information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, requirements, policy enforcement, emergency planning, security awareness, and other resources. Develops policies and plans and/or advocates for changes in policy that support organizational cyberspace initiatives or required changes/enhancements. Supervises, manages, and/or leads work and workers performing cyber and cyber-related and/or cyber operations work. Applies knowledge of data, information, processes, organizational interactions, skills, and analytical expertise, as well as systems, networks, and information exchange capabilities to manage acquisition programs. Executes duties governing hardware, software, and information system acquisition programs and other program management policies. Provides direct support for acquisitions that use information technology (IT) (including National Security Systems), applying IT-related laws and policies, and provides IT-related guidance throughout the total acquisition life cycle. Executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations. Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation (CNSSI 4009).

Cyber Security Framework (CSF) Responsibilities and Goals

Identify (ID) - Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; Risk Management Strategy and Cyber Supply Chain Risk Management.

Protect (PR) - Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the

impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

Detect (DE) - Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

Respond (RS) – Oversee and Govern the development and implementation of appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

Recover (RC) - Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.

As the Cyber Executive Leader of the organization, the CDDDE must communicate the mission priorities, available resources, and overall risk tolerance to the business/process level. The business/process level uses the information as inputs into the risk management process, and then collaborates with the implementation/operations level to communicate business needs and create a Profile. The implementation/operations level communicates the Profile implementation progress to the business/process level. The business/process level uses this information to perform an impact assessment. Business/process level management reports the outcomes of that impact assessment to the executive level to inform the organization's overall risk management process and to the implementation/operations level for awareness of business impact.

A key part of the CDDDE is to understand the organizational vision, mission, objectives, priorities and obligations. Any of these (cyber oriented or not), could wittingly, unwittingly, knowingly or unknowingly affect the security posture of the organization. It is the CDDDE's responsibility to understand the organization's decisions can affect its Cybersecurity Awareness and Resiliency. Additionally, the CDDDE must also understand its Supply Chain and how it wittingly, unwittingly, knowingly or unknowingly affects the security posture of the organization. Supply Chain Risk Management encompasses technology suppliers and buyers, as

well as non-technology suppliers and buyers where technology is minimally composed of information technology (IT), industrial control systems (ICS), Supervisory Control and Data Acquisition (SCADA) systems, cyber-physical systems (CPS), and connected devices more generally, including Internet of Things (IoT).

A new emerging responsibility of this role is not understanding technical security (although this is getting more and more difficult every day), not only is it assessing risk, compliance and security postures (this is also getting more and more difficult by the day), not only is it understanding how to properly assess security postures and risk continuously, but now it all has to be done to a legal evidentiary standard to protect the company, their customers and even the CDDDE itself from legal liabilities.

Qualifications

Education: Master's Degree or Doctorate (Ph.D)

Experience: 7+ years of fulfilling NICE Cybersecurity Journeyman/Intermediate or Master level roles.

Required Skills:

Background in Executive Leadership, Cybersecurity, Forensics, Information Security and Assurance, Program Management, Budget, Legal analysis, Compliance and Risk assessment.

Desired Skills: The list below provides an overall certification choice for policy and strategy development for this position and indicates the diverse needs of this thought leadership role within this organization. The final determination of the organization executive leadership will define which value each suggested certification shall be included in his or her assessment of the candidate skills or amplitude. As the senior most leader for cybersecurity in an organization, it is imperative that the CDDDE be knowledgeable in ALL cybersecurity topics as possible.

What does the CISO role look like now?

Certifications		
Level	Type	Course
Advanced/Master	Certificataion	Board Certified Cyber Intelligence Professional (CCIP)
Advanced/Master	Certificataion	Board Certified Executive Leader (CEL)
Advanced/Master	Certificataion	Board Certified Cyber Threat Analyst (CCTA)
Advanced/Master	Certificataion	Board Certified Forensic HITECH Investigator (CFHI)
Advanced/Master	Certificataion	Board Certified Social Media Intelligence Analyst (SMIA)
Advanced/Master	Certificataion	Board Certified Cyber Intelligence Investigator (CCII)
Advanced/Master	Certificataion	Board Certified Cyber Threat Forensic Investigator (CTFI)
Advanced/Master	Certificataion	Board Certified Expert in Cyber Investigations (CECI)
Advanced/Master	Certificataion	Board Certified Social Media Intelligence Expert (CSMIE)
Advanced/Master	Certificataion	Board Certified Professional Criminal Investigator (CPCI)
Advanced/Master	Certificataion	Board Certified Social Media Intelligence Analyst (SMIA)
Advanced/Master	Certificataion	Certified Chief Information Security Officer (CCISO)
Advanced/Master	Certificataion	Certified Information Security Manager (CISM)
Advanced/Master	Certificataion	Certified Information Systems Security Professional (CISSP)
Advanced/Master	Certificataion	Certified HIPAA Privacy Security Expert (CHPSE)
Advanced/Master	Certificataion	Certified Hacking Forensic Investigator (CHFI)
Advanced/Master	Certificataion	Information Systems Security Management Professional (ISSMP)
Advanced/Master	Certificataion	Certified Risk and Information System Control Certification (CRISC)
Advanced/Master	Certificataion	Health Care Information Security and Privacy Practitioner (HCISPP)
Advanced/Master	Certificataion	Certified Professional in Electronic Health Care Records (CPEHR)
Advanced/Master	Certificataion	Certified Prrofessional and Health Information Exchange Certification (CPHIE)
Advanced/Master	Certificataion	Certificate of Cloud Security Knowledge (CCSK)
Advanced/Master	Certificataion	Certified Cloud Security Professional (CCSP)
Advanced/Master	Certificataion	Certified Professional in Healthcare Information Management Systems (CPHIMS)
Advanced/Master	Certificataion	Certified Professional Health Information Technology Certification (CPHIT)
Advanced/Master	Certificataion	Certified Professional Operating Rules Administration Certification (CPORA)
Advanced/Master	Certificataion	Certified Fraud Examiner (CFE)
Advanced/Master	Certificataion	CompTIA Advanced Security Practitioner (CASP)
Advanced/Master	Certificataion	GIAC Security Leadership Certification (GSLC)
Advanced/Master	Education	NCSF-Practicitoner
Advanced/Master	Education	CNSSI 4012-Senior Systems Managers
Advanced/Master	Education	CNSSI 4014-Information Systems Secuity Officers (ISSO)
Advanced/Master	Education	CNSSI/NTSSI 4015 - Systems Certifiers
Advanced/Master	Education	CNSSI/NTSSI 4016 - Risk Analysts
Advanced/Master	Education	Qualified - Information Security Professional (Q/ISP)
Advanced/Master	Education	Qualified - Information Assurance Professional (Q/IAP)
Advanced/Master	Education	Qualified - Certification and Assessment (Q/CA)
Advanced/Master	Education	NDU CIO certifiecate-Chief Information Officer (CIO)
Advanced/Master	Education	AQD GA8-Information Dominance Warfare - Chief Information Officer
Advanced/Master	OJT	IP O4-5, NAVEDTRA 43360-3 - Information Professional (IP) Intermediate

Security Clearance: Ability to obtain and maintain organization security needs. Top Secret (TS).

What does the CISO role look like now?

Other Skills:

Working understanding of the applicable NIST, and associated industry standards required for thought leadership development. Strong working knowledge of analytical and method analysis required for scientific measurement and quantification. Possesses subject matter expertise and the ability to blend various ideas together to achieve desired outcomes to move the needle of progress and growth in work portfolio area. Ability to manage programs in vision, direction, execution, staffing, resources, budget with competence. PMI certification a plus.

What does the CISO role look like now?

Knowledge, Skills, Abilities and Tasks		
KSAT	**Unique Identifier**	**Description**
Knowledge	K0001	Knowledge of computer networking concepts and protocols and network security methodologies.
Knowledge	K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
Knowledge	K0003	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
Knowledge	K0004	Knowledge of cybersecurity and privacy principles.
Knowledge	K0005	Knowledge of cyber threats and vulnerabilities.
Knowledge	K0006	Knowledge of specific operational impacts of cybersecurity lapses.
Knowledge	K0009	Knowledge of application vulnerabilities
Knowledge	K0013	Knowledge of cyber defense and vulnerability assessment tools and their capabilities.
Knowledge	K0019	Knowledge of cryptography and cryptographic key management concepts
Knowledge	K0028	Knowledge of organization's evaluation and validation requirements
Knowledge	K0037	Knowledge of Security Assessment and Authorization process
Knowledge	K0038	Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.
Knowledge	K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).
Knowledge	K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).

What does the CISO role look like now?

Knowledge	K0048	Knowledge of Risk Management Framework (RMF) requirements.
Knowledge	K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).
Knowledge	K0054	Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures utilizing standards-based concepts and capabilities.
Knowledge	K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.
Knowledge	K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
Knowledge	K0084	Knowledge of structured analysis principles and methods.
Knowledge	K0089	Knowledge of systems diagnostic tools and fault identification techniques.
Knowledge	K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.
Knowledge	K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.
Knowledge	K0126	Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161).
Knowledge	K0146	Knowledge of the organization's core business/mission processes.
Knowledge	K0147	Knowledge of emerging security issues, risks, and vulnerabilities.
Knowledge	K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.

What does the CISO role look like now?

Knowledge	K0169	Knowledge of information technology (IT) supply chain security and supply chain risk management policies, requirements, and procedures.
Knowledge	K0170	Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations.
Knowledge	K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
Knowledge	K0199	Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zachman, Federal Enterprise Architecture [FEA]).
Knowledge	K0203	Knowledge of security models (e.g. Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).
Knowledge	K0260	Knowledge of Personally Identifiable Information (PII) data security standards.
Knowledge	K0261	Knowledge of Payment Card Industry (PCI) data security standards.
Knowledge	K0262	Knowledge of Personal Health Information (PHI) data security standards.
Knowledge	K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.
Knowledge	K0295	Knowledge of confidentiality, integrity, and availability principles.
Knowledge	K0296	Knowledge of capabilities, ,applications, and potential vulnerabilities of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware.
Knowledge	K0314	Knowledge of industry technologies' potential cybersecurity vulnerabilities.
Knowledge	K0322	Knowledge of embedded systems.
Knowledge	K0342	Knowledge of penetration testing principles, tools, and techniques.
Knowledge	K0622	Knowledge of controls related to the use, processing, storage, and transmission of data.

What does the CISO role look like now?

Knowledge	K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list).
Knowledge	K0628	Knowledge of cyber competitions as a way of developing skills by providing hands-on experience in simulated, real-world situations.
Skill	S0018	Skill in creating policies that reflect system security objectives.
Skill	S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.
Skill	S0356	Skill in communicating with all levels of management including Board members (e.g., interpersonal skills, approachability, effective listening skills, appropriate use of style and language for the audience).
Skill	S0357	Skill to anticipate new security threats.
Skill	S0358	Skill to remain aware of evolving technical infrastructures.
Skill	S0359	Skill to use critical thinking to analyze organizational patterns and relationships.
Skill	S0367	Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
Abilities	A0028	Ability to assess and forecast manpower requirements to meet organizational objectives.
Abilities	A0033	Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities.
Abilities	A0070	Ability to apply critical reading/thinking skills.
Abilities	A0077	Ability to coordinate cyber operations with other organization functions or support activities.
Abilities	A0085	Ability to exercise judgment when policies are not well-defined.
Abilities	A0090	Ability to identify external partners with common cyber operations interests.

What does the CISO role look like now?

Abilities	A0094	Ability to interpret and apply laws, regulations, policies, and guidance relevant to organization cyber objectives.
Abilities	A0105	Ability to tailor technical and planning information to a customer's level of understanding.
Abilities	A0106	Ability to think critically.
Abilities	A0111	Ability to work across departments and business units to implement organization's privacy principles and programs, and align privacy objectives with security objectives.
Abilities	A0116	Ability to prioritize and allocate cybersecurity resources correctly and efficiently.
Abilities	A0117	Ability to relate strategy, business, and technology in the context of organizational dynamics.
Abilities	A0118	Ability to understand technology, management, and leadership issues related to organization processes and problem solving.
Abilities	A0119	Ability to understand the basic concepts and issues related to cyber and its organizational impact.
Abilities	A0123	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
Abilities	A0129	Ability to ensure information security management processes are integrated with strategic and operational planning processes.
Abilities	A0130	Ability to ensure that senior officials within the organization provide information security for the information and systems that support the operations and assets under their control.
Abilities	A0170	Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations.
Task	T0001	Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology (IT) security and objectives and reduce overall organizational risk.

What does the CISO role look like now?

Task	T0002	Acquire necessary resources, including financial resources, to conduct an effective enterprise continuity of operations program.
Task	T0003	Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture.
Task	T0004	Advise senior management (e.g., CIO) on cost/benefit analysis of information security posture.
Task	T0006	Advocate organization's offical position in legal and legislative proceedings.
Task	T0025	Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders.
Task	T0066	Develop and maintain strategic plans.
Task	T0130	Interface with external organizations (e.g., public affairs, law enforcement, Command or Component Inspector General) to ensure appropriate and accurate dissemination of incident and other Computer Network Defense Information.
Task	T0134	Lead and align information technology (IT) security priorities with the security strategy.
Task	T0135	Lead and oversee information security budget, staffing, and contracting.
Task	T0145	Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2).
Task	T0148	Manage the publishing of Computer Network Defense guidance (e.g., TCNOs, Concept of Operations, Net Analyst Reports, NTSM, MTOs) for the enterprise constituency.
Task	T0151	Monitor and evaluate the effectiveness of the enterprise's cybersecurity safeguards to ensure that they provide the intended level of protection.
Task	T0221	Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network.
Task	T0227	Recommend policy and coordinate review and approval.

What does the CISO role look like now?

Task	T0229	Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.
Task	T0248	Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals.
Task	T0254	Oversee policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies.
Task	T0263	Identify security requirements specific to an information technology (IT) system in all phases of the system life cycle.
Task	T0264	Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.
Task	T0282	Define and/or implement policies and procedures to ensure protection of critical infrastructure as appropriate.
Task	T0337	Supervise and assign work to programmers, designers, technologists and technicians, and other engineering and scientific personnel.
Task	T0356	Coordinate with organizational manpower stakeholders to ensure appropriate allocation and distribution of human capital assets.
Task	T0371	Establish acceptable limits for the software application, network, or system.
Task	T0429	Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities.
Task	T0445	Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization's strategic plan.
Task	T0509	Perform an information security risk assessment.
Task	T0763	Conduct long-range, strategic planning efforts with internal and external partners in cyber activities.
Task	T0871	Collaborate on cyber privacy and security policies and procedures.

Task	T0872	Collaborate with cybersecurity personnel on the security risk assessment process to address privacy compliance and risk mitigation.
Task	T0927	Appoint and guide a team of IT security experts.
Task	T0928	Collaborate with key stakeholders to establish a cybersecurity risk management program.

Afterward

I have chosen to stop the analysis at this point. It is logical to continue this analysis to provide even more detail below the functional level (at the sub-function, category, sub-category) per the CSF. The frameworks even cite supportive and informative references by these levels that could be leveraged. Since the CWF is aligned with the CSF, and the CSF has assigned security controls that aligns with these constructs, we could even populate from these references a security control index scientifically aligning and, therefore, assigning, security controls to this CDDDE role. This would provide quite the detailed assigned requirements, tasks, knowledge, abilities, certifications, education, experience, etc. required to properly be prepared to execute this very daunting role called, CDDDE. Logic continues in that if you have all these defined tasks, knowledge, skills and abilities well-articulated, then you could create a matching set of questions for recruiters and interviewers (as well as auditors and investigators) to assess if the CDDDE (or their staff) truly have the requisite capabilities and competencies.

Reference(s)

Newhouse, W., Keith, S., Scribner, B. & Witte, G. (2017). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (CWF). NIST SP 800-181. Retrieved February 22, 2018 from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

National Institute of Standards and Technology (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 Draft 2. Retrieved February 22, 2018 from https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_without-markup.pdf

Department of the Navy, Chief Information Officer. (2016). Cyberspace Information Technology and Cybersecurity Workforce Management and Qualification Manual. SECNAV M-5239.2 June 2016. Retrieved February 22, 2018 from www.doncio.navy.mil/ContentView.aspx?id=7991

EC-Council, Certified CISO website. Retrieved February 22, 2018 from https://ciso.eccouncil.org/cciso-certification/cciso-domain-details/

For Additional Information Contact:

Eigenspace
312 Main Street, Suite 300
Gaithersburg, MD 20878
240-654-4097
www.eigenspace.us