IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

DOD Project Part 4: Final Report

Niravkumar K Patel
Dr. Kevin White University of the Cumberlands

List of compliance laws required for DoD contracts.

Access control: In DoD contracts, access control is an access management mechanism that ensures that specific users, groups, programs, or computers have access to a resource. To provide business information to other people and applications, create access control policies to prevent unauthorized people and programs from accessing information or damaging resources (Nash et al., 2021). Access control is a common component in business networks and is implemented with access control policies and rules. The primary mission of Blue Stripe Tech is to work as a professional in access control to provide our valued clients with the highest quality products and services. As part of our service commitment, we offer our clients access control systems and solutions in the area of electronic document imaging and secure electronic processing. The Department of Defense (DoD) employs hundreds of thousands of workers to provide logistical and military support for the armed forces

Awareness and Training : Awareness and Training is a phrase used in DoD contracts to describe several services for which payment is made for a fee in return for providing a training course to an individual or a class. Each training system consists of an instructional package that a provider prepares following an agreed-upon schedule. (Nash et al., 2021).Blue Stripe Tech is a set of rules and procedures developed by the Defense Contract Management Agency. These rules are for Defense Acquisition Regulation and Defense Federal Acquisition Regulation guidance. Awareness and Training refer to two elements in DoD contracts. Awareness helps DoD provide the best possible products and services most cost-effectively. Awareness is defined as the awareness of all aspects of the prime contractor's products and services. It helps DoD provide the best possible products and services most cost-effectively (Nash et al., 2021).

Authentication: In DoD contracts, authentication is typically a one-way or two-way authentication method. One-way authentication is where a user/employee authenticates to the

system. DoD may require a user to enter a username and password or enter a PIN to obtain certain access levels to specific scenarios. DoD may require that a user provide a biometric to the system when logging in and accessing a system. In Blue Stripe Technologies, the authentication process starts with the organization providing data for its users (Nash et al., 2021). It can be as simple as giving every employee a name and an e-mail address. It may not be much, but this simple approach is used today. The authentication process then compares this data to what the user provides. It may compare the user's data with another database that tracks personnel or even reach the user's ID card to a central database of ID cards. In any case, the authentication process has two parts: Comparing the user's data and the organization's data (Nash et al., 2021).

Audit & Accountability: Audit & Accountability is a generic term used by the United States Department of Defense (DoD) in many acquisition contracts such as the blue stripe technology and the military systems. The contract's primary purpose is to ensure the integrity and accuracy of the performance data. (Nash et al., 2021).The Contractor shall use good accounting practices to ensure Accountability and integrity of the Contractor's work. The Contractor shall provide adequate and complete cost and pricing data to substantiate total cost and allow effective contract monitoring. Audit & Accountability is the assurance that the funds received by DoD to provide services or materials are being properly accounted for, delivered, and billed following established contractual terms and conditions. When a DoD contract is initiated, the Contracting Officer requires auditing the Contractor's books and records to verify the accuracy of the information contained in financial statements and records. (Nash et al., 2021).

Configuration management: Configuration management in DoD contracts deals with the processes and practices in controlling a complex set of data elements that can track, monitor, control, validate, assure their consistency, and ensure the integrity and reliability of their content. Configuration Management in DoD Contract Blue Stripe, also known as Blue Striping or Configuration Control, is an integrated set of processes, strategies, and guidelines designed to help manage a contract's configuration of IT and the services provided. When the CM function in DoD Contract Blue Stripe is adequately implemented, it's an excellent management tool that can save significant dollars and reduce the operational cost of IT infrastructure (Nash et al., 2021).

Policy framework(s) used for this project.

Operational view framework

The DoD's operational view framework is used to map its business processes (e.g., human resource management, procurement, finance, personnel, and contract management) to the relevant IT systems and software applications that support those processes. The view will reflect how these systems and software applications execute and perform not how they should be implemented or the way they should organize (Frain, 2018).The framework specifies the activities and associated requirements of the government operation. The activities are further detailed by describing the actions needed to deliver services to the customers and explaining the related conditions, rules, regulations, and processes for accomplishing the activities. The framework defines performance-based targets. As the framework is used to develop and maintain performance metrics, the framework can adapt to incorporate changes in priorities and capabilities of the government operation (Frain, 2018).

Systems /Services view frameworks

The Systems /Services view frameworks are used in the Department of Defense (DoD) and other public sector organizations where the users have to report their issues and requirements. The use of this framework should not be considered as a replacement for any other tools, processes, or methodologies. The main goal of this report is to help the user understand the benefits and uses of this framework for the users and build their skills to use this framework effectively and use it for the projects in their organizations (Frain, 2018). The Systems

/Services view frameworks used in the Department of Defense (DoD) in Blue Stripe Tech is a large-scale implementation to support the entire Department of protection (DoD) in Blue Stripe Technologies are very well known for their expertise and capability in all sectors of IT. The Systems /Services view frameworks are as such designed to support large scale implementations of data architecture to support the entire DoD in the area of systems services, and it is our specialty in the area of data architecture (Frain, 2018).

Technical Standards view framework

The Technical Standards view frameworks will usein Department of Defense DoD projects to define and document technical and functional requirements for the development of a given project. It can include both systems development manuals and software development manuals. The documentation can also be of a higher level which defines a development environment. It can be delivered as a document and to a software process model (Frain, 2018).The Technical Standards view frameworks will be used in the Department of Defense (DoD) in Blue Stripe Tech to update the technical Standards used in Military aircraft. It is a three-stage project. The blue stripe Technical Standards are the DoD's standards for aircraft and ship systems. Standards are written to reflect the aircraft's actual requirements and ensure interoperability between the equipment (Frain, 2018).

Blue Stripe Tech Security Policies

As a security professional, it is my prime responsibility to tackle each bit of problem from every aspect. Since Blue Stripe Tech wants you to develop a security policy for the project which could match high-security standards and durable measures. Hence below are two main contributions from my side to help and push in developing security policies.

1.List of controls placed on domains in the IT infrastructure.

There is a long list of controls that can be placed on domains in IT infrastructure. These controls can help in making accurate security protocols and policies for better defence. Since Blue Stripe Tech is working on assuring security measures according to the U.S security standards, below are a few security controls that can be placed on different IT infrastructure domains of Blue Stripe Tech.

Digital Security Controls:

Digital security control includes placing security checks on digital information including password, username, authentication, antivirus check, use of firewalls to make your connector and users more secure. Authentication may include two-factor authentication,

fingerprint authentication, and so on. Digital security control is one of the most important security protocols to be implemented in IT infrastructure

Control on Physical Security:

Next security controls can be placed on the physical assets of the system. This includes making your Data Centre secure, use of guards, use of access control, use of fencing, use of CCTV cameras and different detection sensors in order to make the system physically strong.

Internet Security Controls:

Use of Centre for Internet Security control (CIS) its security controls and actions which include a to-do list for making system more secure. A few useful techniques are given by CIS for making the system more secure that include:

- Enforcement of IT security protocols using security controls.
- Educating employees and system users to know more about security guidelines and understand security frauds.
- Meeting compliance regulation and making industry strong both physically and digitally secure.
- Assessing risk on a regular basis to get rid of any broken damage to accidents.

Doing Security Control Assessments:

Security control assessment also helps in making a system of an IT infrastructure strong in terms of user credibility, system utilisation, and getting more of the output from the system. There are different parameters that can be used to check security control assessments. It includes the following things:

- Determination of target system where you check system in terms of physical requirements like IP address checking and physical connection of the system.
- On the second number, it is about the determination of target applications that is all about checking off the services and knowledge about the different databases, third-and party components which can provide you more security.
- Third, it is about checking the report on a regular basis so that you could manipulate whatever you are doing and how far these security protocols will take you to make the best and the strongest security policies.

2.List required standards for common devices, categorized by IT domain.

An IT infrastructure is a combination of different devices and models working in it. IT infrastructure is itself is a combination of huge modelled systems where different subsystems are connected along with different devices. Well-reputed IT infrastructures use different standards in order to make the system more secure and useful that make the system more prominent in terms of tackling different security attacks. Also, it helps systems serve the best services.

Below, different security standards are given but companies are not limited to these only. Different companies use different standards. We get you the best of the standard that we want Blue Stripe Tech to have in it. It includes the following as:

- Use of cabled network
- Use of wireless network

- Telephony: Use of voice over internet protocol (VoIP)
- Telephony: Use of analogue communication system
- Use of the mobile system
- Use of digital media
- Use of CCTV cameras in order to do recordings of the different moments to capture any problem or invalid activity
- Use of different hardware devices like print media
- Use of standard desktop control and alarming methods to tackle any hazardous activity

Also, standards for common devices that are categorised by IT domain include the use of computing hardware which include storage and processing powers along with operating systems utilisation. The database is one of the most important aspects that is considered while working in an IT domain. It helps in doing the settlement of databases and in data management. Database management is also important to consider while talking about the security of devices associated with an IT infrastructure. Last but not least, the security of the system is very important. It is a prime responsibility of security officers of a company to set all the rules for making the system prominent and it could run smoothly.

DoD-compliant policies for the organization's IT infrastructure.

User domains:

Organizations with DoD-compliant user domains can protect their data. They can ensure data security, privacy, user safety, and user comfort. They can also identify the location of the device and the specific access required. The compliance ensures that every device user access is configured with the right policy. This way, the organization complies with the security standards of the federal government. If the organization's IT infrastructure is not DoD- compliant, it can be attacked by the federal government. The federal government can require companies that supply services to comply with specific laws and regulations (Carter, 2016).

Blue Stripe or Blue Stripe is unique and customized. IT support software with specific applications and solutions used by Defense agencies to track and manage various issues and problems related to IT infrastructure. It allows government departments and agencies to find and report potential network infrastructure issues easily. Blue Stripe supports DoD regulations regarding using any information related to its user domains. DoD regulations and policies allow certain agencies to access and share only relevant and directly related to their mission objectives (Carter, 2016).

Workstation Domain

DoD-compliant Workstation Domain is a secure network domain that enables users to connect to the Internet while maintaining their federal networks and systems access. A Secure network domain or network segment is created using a workstation host server and a group of workstations connected to the server. DoD-compliant Workstation Domain is a secure network domain that enables users to connect to the Internet while maintaining their national networks and systems (Carter, 2016).

The DoD-compliant Workstation Domain technology used in Blue Stripe Tech can comply with the security standards and regulations to allow the organization to access classified information for the safety of our country. With Blue Stripe Tech's DoD-compliant Workstation Domain, we provide an easy way to centrally manage the organization's Windows PCs, including network connections, Internet access, and email. Workstation Domain is a secure gateway between client systems and enterprise systems, providing better control of all aspects of the workstation environment, data streams, email, and internet access. Workstation Domain acts like a proxy server and the gateway to the enterprise services and applications. DoD- compliant Workstation Domain will help protect against malware threats, intrusions, network attacks, identity theft, account takeovers, and unauthorized network access (Carter, 2016).

LAN Domain

The DoD-compliant LAN Domain for the organization's IT infrastructure is deployed as an overlay over a physical layer of Cisco Catalyst switches. The DoD-compliant LAN Domain is connected via a firewall-based internet gateway and DoD-compliant web filter. Each physical layer switch provides the access ports to the DoD-compliant LAN Domain and the organization's physical network infrastructure. The DoD-compliant LAN Domain and its controls deliver the data and management paths between the organization's physical network infrastructure and the DoD-compliant web filter for its internet connectivity (Carter, 2016).

In the modern and fast-changing IT infrastructure environment, organizations need to be agile in several ways. As such, our organization uses several practices to ensure that it stays compliant with the Information Assurance requirements of the government. It is essential to the day-to-day activities and operations of Blue Stripes Tech to ensure that our technology solutions are DoD-compliant to guarantee their usefulness to the organization (Carter, 2016).

Blue Stripes Tech's LAN Domain Service helps clients build secure, reliable and interoperable networks to meet federal government mission objectives and help them achieve government compliance. Blue Stripes Tech has provided a comprehensive LAN Domain solution for the defense, federal government, intelligence community, healthcare, public, and non-profit sectors for more than a decade (Carter, 2016).

LAN-to-WAN Domain

LAN-to-WAN Domain in DoD is a concept introduced in the United States Defense Department that was adopted to solve some problems seen on the US Defense Department's infrastructure. The problem that LAN-to-WAN Domain is trained to address was the connectivity problem and the internet connectivity of some DoD systems, including the Internet and Intranets. The LAN-to-WAN Domain for DoD in Blue Stripe Tech covers all information related to DoD's implementation of the IMS in DOD and DoD civilian agencies to facilitate a Single Integrated Operational Picture of operations and intelligence. (Carter, 2016).The LAN- to-WAN Domain results from an initiative taken by the National Defense University's Institute for National Strategic Studies and Analysis. The DoD also launched the Integrated Enterprise Architecture Architecture Roadmap to improve the efficiency and effectiveness of the IT landscape within the DoD. With the support of the National Defense University's Institute for National Strategic Studies and Analysis, the IEAA Roadmap is the culmination of work that has been ongoing since the 2010 NDU-NIAC Report, which also established the Enterprise Architecture Office (Carter, 2016).

The policies, standards, and controls in DoD

The DoD issued logical access policies with policies requiring the use of multifactor and other authentications. A logical access controls require user to validate their identity through the personal identification number to identify the user. There is other way to identify user via biometric system or security token provided by the unique application, device. The control limits the files and resources users can access the system action they can perform. The DoD policies specifically describe the logical access requirements related to identity authentication via public key infrastructure and securing the unclassified, classified, and protected health information.

DoD health care program is used to personnel clearance before accessing protected health information of the employee. DoD cybersecurity program to be used to identify the authentication including public key infrastructure to be used for accessing DoD information systems. DoD security of unclassified information on non DoD information system to be protected at least one physical or electronic barrier such as logical authentication. DoD Staff Instructions policies for information assurance and support to the DoD computer network defense, which includes implementing security mechanisms to protect the DoD computing environments. The instruction required using public key infrastructure to authenticate identities, control access to DoD information systems.

Public key infrastructure and public enabling instruction to require public key infrastructure to be implemented to control access to networks and systems using common access cards. The use of the strong authentication by using common access cards helps to prevent unauthorized user from outside.

All DoD system to be mangling the different level of the security with network and application level of the securities. The security to be achieved via high level of the encrypted algorithms to encrypt the data with complex authentication algorithms to access the data or applications. There are several networking mechanisms to be used to protected data with network secure protocol to identify the IP address or Mac address of the all the request. All the request to be monitored in the efficient application in high level with all the description of the data and measured to be graphical view to see the reports. There are several compliances in DOD.

There is SSL authentication to be used to verify the third party's application for correct request and response from outside of the network infrastructure. All the deployment process of the application to be test in Development's environment with all software development life cycle steps and complete the process of the single task in deeply to verify and access. The application design is basic process to design the application for user views and write the code as per the components. Each component is working separately to write the code, test specific process and deploy on the server efficiently. If there are an issue in the component, then it should be changes as per the requirements without affecting any other applications. There are code vulnerabilities and securities to be measure of the application. The deployment process has different types of the release plan to deploy the application. All the applications to be maintained in high level of security with data security. The disaster planning techniques to be implemented in high level to maintain all IT infrastructure in very short time to get receiver all the data efficiently.

There is the mechanism to be implemented to check the user entry at workplace via figure print and eyeballs verification techniques to use for few of the important applications. It is required to monitor all the activities via video surveillance to check the moments of the activity in while 24/7.

References

Carter, A. (2016). DoD Cybersecurity Discipline Implementation Plan. Department of Defense Washington United States.

Frain, S. C. (2018). (Inter) national legal frameworks in the Marianas Archipelago: The right to self-determination and the National Environmental Policy Act. JOURNAL OF SOUTH PACIFIC LAW, 2018(2018), 1-22.

Nash, R. C., Schooner, S. L., O'Brien-DeBakey, K. R., & Edwards, V. J. (2021). The government contracts reference book: A comprehensive guide to the language of procurement.

IBM Cloud Education (2019). What are Security Controls? [Online] www.ibm.com. Available at: https://www.ibm.com/cloud/learn/security-controls.

Stevevincent.info. (2019). Chapter 4, Business Challenges Within the Seven Domains of IT Responsibility Chapter 5, Information Security Policy Implementation Issues. [Online] Available at: https://stevevincent.info/ITS305_2016_2.htm.

www.redhat.com. (n.d.). What is IT infrastructure? [online] Available at: https://www.redhat.com/en/topics/cloud-computing/what-is-it-infrastructure.

[NIST7657] NIST/NSA Privilege (Access) Management Workshop Collaboration Team, "A Report on the Privilege (Access) Management Workshop," NIST IR 7657, 2010.

[NIST7665] "Proceedings of the Privilege Management Workshop", NIST IR 7665, September 1-3, 2009.

[NIST7874] Hu, V., and Scarfone, K., "Guidelines for Access Contol System Evaluation Metrics", NIST IR 7874, 2012. 1685 [TCSEC] Trusted C