# **ABC Software Final Security Report**

Morrese Morrison

Peirce College

ISC 325 Access Control, Security Assessment

Professor Patrick Coyle

Date 12/9/2022

## **ABC Software Overview & Introduction**

A broad and meticulous overview is somewhat required in today’s day in age of technology. With the rapid advancement of hacking techniques, now more than ever, it is paramount that organizations focus heavily on the security of their business. This does not mean just hardware, no. This means hardware, software, access to company systems and resources. A meticulous review of each of these components of an organization assures a set standard of security that will protect the organization from various security attacks. As such, after reviewing ABC software, there are several areas where access control is needed. As businesses rely more and more on a hybrid model for employees with regards to remote work and office work, “a renewed shift in attitude toward security and privacy” is needed (Identity and Access Management: Looking Ahead, 2021). There are several individual security recommendation topics that I would like to thoroughly discuss. For starters, I would like to begin with Access Control.

**Access Control Recommendations**

Access control is the hall mark of any organization’s security model. After my review of ABC Software, there are several areas where access control should be implemented to assure a set standard of security throughout the organization. The first area that I would like to discuss is the network. From my review I have discovered that there is a wired network with around 300 users. Each user is segmented into their respective department. This area is strong on security. However further segregation can be utilized to promote healthy IP traffic throughout the network. Also, network policies should also be implemented for better IP traffic control as well.

A major area that requires attention is the company system servers. As you are aware, the data and information on these servers are irreplaceable. I have found that there are different servers with different levels of data on them. For example, there is an “HR Server” that houses sensitive HR related information. There is also a “Business Server” that houses the orders and fulfillment database as well as the customer database. Tighter access controls should be implemented here to ensure that employees have proper access to these severs based on their role. This will prevent the servers from being compromised as well as data being destroyed or stolen.

Devices also require a measure of access control. This mainly applies to employee’s Laptops and Desktops. Access control in the form of password policies and devices policies should be applied. This is mainly to ensure that every device on your domain and network is compliant. This domain also provides additional features regarding remote log in and data recovery.

Another major area that should consider an extensive amount of access control is the ABC Software building itself. From my observation, there are several current issues that should be addressed with the facility. The first issue is how employees enter the building. Entering through a side door in the building that is not monitored introduces a host of potential building breach possibilities. The second issue is that of the parking lot. To my understanding there have been numerous vandalistic activities in the parking lot that ABC Software employee’s use. A lot that is not properly monitored or properly lit with light when the sun goes down. Again, this should be looked at immediately as the safety of employee’s is important.

Access control measures should also be applied with passwords. Specifically credential management. The use of external websites is often used within the company and as such, various passwords and usernames may need to be remembered to get into these websites. I recommend instituting some form of credential management. This improves security due to employees only needing to remember one password that unlocks the credential manager itself. And when that employee visits a site that is synched to that credential management system, their credentials will be synched. This encourages employee’s to not physically write down or store credential information in unsecure places.

As company’s grow with more employees, user account reviews should be conducted. This is another area that requires some form of access control. This is an area that is often overlooked and easy to be a victim of. Access inflation can happen when users continue to gain more and more access as the years go by. If this is not checked, they may gain access to systems and resources that they should not have access to, thus creating a potential intrusion scenario. A regular account review and audit eliminates this issue.

From my research of ABC Software, I notice that various systems are used internally in the company in day-to-day operations. One of the main applications of course is email. Securing this is vital due to the sensitive data that can be held in one’s email account. The area of Multi-Factor Authentication should be explored. This should be explored since when MFA is enabled, it drastically reduces the success rate of a potential attacker due to them having to authenticate multiple avenues simultaneously.

One more key area that should be given more attention to is that of Single Sign On. Single sign on enables users to sign into multiple company systems with their Active Directory Credentials. This creates uniformity with accounts and password throughout the organization. Again, users only must remember one password along with their username. This will encourage them to not write down their passwords on an unsecure medium.

A dual area that should be focused on is account provisioning and account deprovisioning. Who should be responsible for provisioning? Should this account provisioning be automated? Regarding account deprovisioning, what is the process for deprovisioning? What initializes this process? These questions should be explored to maximize provisioning and deprovisioning in an access-controlled environment. Access control security is paramount; however, authorization and access are just as important. There are various authorization and access recommendations that should be addressed.

## **Authorization & Access Recommendation**

Authorization and access are the foundation for any security implemented plan for an organization. Access to sensitive or crucial information hinges on the proper application of authorization and access methods. If this foundation is not implemented correctly, sensitive, and personal data will be easily accessible by employees thus disregarding any form of data confidentiality in the organization. In the case of ABC Software, there are several authorization and access methods that can be utilized to better enhance the access control within the company.

**Access Control Techniques for Devices**

As the needs of the business constantly change, business require different devices for employees to connect to the internet and to connect company related resources. Everywhere you look, you see a device. An iPhone, and Android Cell Phone, iPads, and Galaxy tablets. As convenient as these devices can be, if proper precautions are not put in place, each of these devices can serve as a point of entry into the network. Essentially increasing the overall liability of the network and company resources.

To address this issue, certain techniques can be implemented to reduce this risk. I suggest the following techniques to be implemented. The first technique is Mac Filtering. Every device has a MAC address burned into the network adapter of that device if that device connects to the internet. Due to this, filtering MAC filtering offers a way to control and monitor a pool of devices. We should implement a set list of approved MAC Addresses to be allowed on to the network. This way only company approved, and security compliant devices can enter the network. If an employee would like to get a device allowed on the network that was not given to them by the IT department, they can submit a request and have that device reviewed by the security team to decide whether it is approved or not. This provides in a way a slimmed down version of a Mobile Device Management system. In addition, certain web filtering features can be applied to stop users from visiting certain sites.

Another technique that should be implemented is to utilize the windows firewall feature on windows 10 (Hoffman C, 2017). Utilizing windows firewall provides additional security without physically installing a firewall. This should mainly be used for employee’s work PC. Mainly when they take their PCs off the secure internal network and work remotely. Yes, a VPN will still be utilized, however, to ensure maximum security on top of the VPN connection, the windows firewall feature should be enabled and set to block certain programs to reaching the internet and to block certain inbound and outbound port connections that could be compromised by hackers to remote connect to employee PC’s.

The last technique that should be implemented is the use of an Access Control System. My recommendation would be a Cisco 1120 Series ACS system (Access Control Options, 2011). This System provides means to set “access policies” for “device administration” for “wireless and wired 802.1x network access scenarios.” This bolsters the overall control of hardware and wireless devices on the network. Thus, increasing security.

**Access Control Employees**

Employees are the life and blood line of an organization. They are the ones who handle day to day business operations. As such they routinely require access to internal company related applications and files. This can pose an issue as their day-to-day interaction with these application and files can cause a security leak. Especially if employees have access to applications and files that they should not have access to. As such proper access control measures should be taken to prevent an incident like this from occurring.

As a whole Role Based Access Control should be instituted as a form of access control throughout the company. Role based access control basses’ access to an object or resource based off an individual’s role in the company. For example, there are multiple HR personnel, accounting personnel as well as IT personnel. Having roles for each department provides a baseline of access for users in that group. This also improves on boarding as new hire’s will only need to be added to their respective group to gain access to the systems that they need.

In conjunction to Role Based Access Control, another technique should also be utilized to further tighten down security. And that is implicit deny. Role based access is efficient and fast, however not everyone in their respective group need access to certain company resources. Take for example the IT department. An IT manager may need access to all the company’s server for troubleshooting and administrative duties. However, an IT Support technician would not need this level of access to complete his job. Implicit deny denies everyone except for users who have been allowed access to said application.

Separation of duties from a managerial and executive standpoint should be instituted as well. A manager or an executive should not have the ability to submit and approve a financial related request without that request being approved or not by another individual that is higher than them. A request by a manager would need approval by an executive. A request by an executive would need approval from the CEO. In the case of the CEO, he will not need any approval for his decisions beside the board of directors or shareholders.

I also recommend we utilize data encryption. This is mainly for employee’s work PC’s when files are stored locally on their computer. We strongly recommend that employee’s refrain from storing sensitive files locally on their computer, however there are scenarios where this is necessary. In those scenarios those files should be fully encrypted. This encryption stands as a last line of defense if the employee’s computer is stolen or compromised. Each time a file is used and is no longer needed, that file should be either deleted or moved back into a network folder.

Physical segregation should also be implemented. This is especially important regarding the ABC software’s servers that hold sensitive data. These servers should be moved to a secure, well ventilated and monitored closet or storage room. This room should be monitored 24/7. To get into the room, only the IT Manager, the CEO and a designated keyman should have the door code to access this location. A logbook will also be at the door and requires a detailed log of who is entering the room, their purpose, name, date, and their signature.

Reporting is often needed and as such, content-dependent control is recommended. This mainly deals with various views in the database. These views can query different kind of data depending on the view. For instance, there could be a payroll view, there could be a product view. Regardless, certain views should only be accessible for a select few. Payroll administrators and executives should only have access to the payroll view. The marketing team under no circumstances should have any access to payroll views. Again, this increases security uniformity, instead of outright denying access to the database all together, if content-dependent control is implemented, users can only run views and reports that they need to complete their jobs.

Another highly effective access control technique is that off utilizing constrained interface. Based on a user’s privileged, he or she can only see the screens and data that has been assigned to the role that employee has. For instance, within the HR system, the HR director would have full access to view various data and to preform various functions within that app. The HR recruiter however would have far less access and only have access to the data and functions that she needs to complete her job. This prevents the HR recruiter to view sensitive data as well as prevents the recruiter from filtering false data into the system as well delete data all together.

All these access control methods and techniques boil down to the tried-and-true rule of least privileged. Least privileged emphasizes that employees should only have access to the applications and files that they need to complete their jobs. Noting more nothing less. This ensures that the user does not occur role inflation. This happens when more and more roles are added to the user that is needed, eventually granting that employee’s access to certain company resources that he or she does not need. In addition to access control policies, security assessment and testing will be discussed next for ABC software.

## **Security Assessment & Testing**

Security assessment and testing is an integral part of any organization’s daily operations. Without proper assessments and testing, systems will become faulty or down, increasing the overall business costs due to payment systems not being operatable, customer data being loss or internal systems rendered unusable by employees. As such, proper security assessment and testing should be applied to day-to-day operations to successfully keep the enterprise functional and profitable. In the case of ABC software, there are several security assessment and verification methods that should be implemented to ensure that all systems are available.

**Backup Servers Utilizing Tape Drives & Removable Media**

As company’s collect and analyze more and more data, it is essential that this data is never compromised or lost. Critical information such as company sales, product information and employee records should be routinely backed up. Specifically, data regarding the company’s transaction records and financials. This can be for business reasons as well as audit reasons. A backup verification assessment is recommended for ABC’s Software current back up process. This is to confirm that the data being backed up is accurate and required.

Whether or not that data is required for future purposes such as business analytics regarding sales with certain products, or for audit purposes. Regardless, the current process should be under review to answer these three questions. What exactly is currently being backed up? Is the data that is being backed up necessary for a specific task or purpose? Is the current backup process being backed up off site onto secure servers as a contingency option to limit the possibility of on-site backup data being destroyed in a fire, flood, or supernatural event?

Ultimately, when backing up data and even before the backup, the focus points should be data consistency, data integrity, data privacy and data security. (Data Protection, 2016). The expected outcome from this assessment is to improve the overall efficiency of the current data backup process regarding overall data size as well as recovery options. If less data needs to be backed up, then there is less time and resources being spent on that process. Regarding recovery options, if data is being backed up on a cloud infrastructure as well as physical media, that increases redundancy regarding recovery options.

**Online Sales to Customers**

Another critical operation of this company, Online sales to customers is crucial. This is how revenue is brought into the company. Any issues with the site itself will cause customers to be impatient and possibly search elsewhere for products. For this component of the organization, I recommend a Protocol Conformance Test (Risked-Based and Functional Security Testing, 2005). The goal of this test is twofold. On one side, the longer the site is down, the more potential customers ABC Software is potentially losing. On the other hand, due to customer information being entered onto the site, security is of upmost importance.

With this test, various web-based protocols will be analyzed and tested. This is to minimize and ultimately avoid any potential hackers from accessing the web site. This is the usual method and as such should be focused on. The desired outcome is to confirm that the website is using the latest web security protocols to ensure security when customers access the site to purchase products. This in turn will ensure trust with the customer and can encourage the customer to return if they feel as though the site is safe.

**Fulfillment Order System**

Another crucial part of ABC software operations infrastructure is indeed the back-end system. With any company or enterprise, the back-end system is pivotal to accurately recording sales as well as orders that need to be shipped along with the meta data per order. As such, if this back-end system is not configured correctly, this will affect the overall efficiency of orders being received, recorded, and completed after shipping. I recommend a Load and Performance Testing assessment on the fulfillment order system.

The goal of this is to assess the scalability, fault tolerance and the overall load that this system can handle. Again, up time is of crucial importance. Any issues with this system will affect revenue coming to the company that can lead to lawsuits regarding certain businesses not receiving their specific order based off a contractual agreement. This test will see how much pressure this system can take regarding overall orders being submitted and processed in a certain interval of time. Also, how fast can one order move throughout the system based on its fulfillment status. Are there any bottle necks in the system? Can the system handle a high volume of orders and meta data being processed simultaneously? The desired outcome of this test is to ensure uptime in cases of high-volume orders as well as ensuring the performance of the system does not degrade depending on the volume.

**Payroll System**

Arguably the single most important part of any organization or company is its payroll system. This system can never be down no matter what, especially on pay disbursement days. When employees must wonder whether they will get paid or not this week is only inviting future issues for the company in forms of lawsuits and ultimately employees leaving. Again, due to this, this systems’ uptime is top priority and requires a close examination to confirm usability in all circumstances.

I propose a mixture of Safe-Base and Use-Case testing for this system. This hybrid test will assess the system under certain scenarios. One pro is that payroll systems essentially do not change, the weekly or biweekly process for the most part stays the same. There are rarely any major changes that would compromise the system. Regardless, certain use cases may arise. These use cases should be identified, explored, and tested to see how the system may react. With this focus, there is also a possibility of software threats against ABC Software. These threats can pose a major hinderance to daily operations. This will be discussed in detail next.

## **Ever Looming Possible Software Threats**

The core business focus of ABC software is the development and the sale of various software products. As such, proper attention to possible software security threats should be reinforced during development and post release to assure that software cannot be compromised. These threats do not only have the possibility to compromise the software that is sold and released but can also affect ABC’s software industry credibility and ultimately its bottom line. The meticulous examination of the following possible threats is indispensable to the current and future state of ABC Software.

**Compromising Threats**

To ensure secure development of software systems by ABC software, the following threats should be considered. The first threat is of not validating inputs into a program. In modern day software systems, input from users is often received and processed for the user to interact with the program for a desired outcome. There can be an input field prompt where the user may need to enter a value. It can be an integer or a string. But what happens if the user enters a special character? Or white spaces? This could compromise the program as it is accepting values that cannot be translated once processed. This could potentially open the program wide open. To mitigate this, proper input validation should be applied to any input variables on the back end of the program. That way, when an undesired input is entered, that code function can disregard that input and prompt the user to enter the value in the desired data type.

The second threat relates to authentication and session management. This mainly applies to web applications as the internet web browser is the main interface the user is interacting with. On the authentication side of this threat, improper authentication can allow a user to gain a higher-level of access to the application that they should not have. To combat this, ABC’s software developers should integrate user authentication with the current authentication system. This produces less technical debt and eliminates the necessity to create an authentication system from scratch. On the session management front, if web cookies are not sent over secure channels, this opens the possibility of an attacker to be able to “hijack a session” (Session Hijacking Attack, n.d). To prevent this from occurring, sessions cookies should be randomly generated, long and should also expire after an extended period, prompting the user to reauthenticate themselves once the cookies are expired. These sessions should also be encrypted as well.

Another potential threat that I feel as though does not get enough attention that can affect the overall security of a program is Error Handling. “Error handling refers to the response and recovery procedures from error conditions present in a software application” (What Is Error Handling, n.d). The main thing with this threat is that if Error Handling messages are displayed, those messages can expose sensitive internal information. This can range from databases to servers. This information can give a potential attacker all the ammo he needs to compromise the program. To stop this from happening, any error handling messages should be disabled from any publicly accessible servers or applications.

The fourth potential threat is the improper utilization of a failure secure or fail open state lock on a program. The reality of software development is that software will be used in unconventional ways. Contrary to what the developers have intended. How the program reacts when this occurs is unpredictable. If proper failure measures are not put in place, this unconventional use could crack the program open for hackers. However, this can be avoided by developers programing the software to either lock out completely or allow the software to operate in a high-level secure state, locking certain functions of the program from the user.

The fifth potential threat that that can compromise ABCs’ Software is the use of API’s. The advent of API’s has made web applications extremely robust and has introduced new possibilities to the industry for customers and consumers. With API’s, systems can talk to one another and exchange information in real time. This completely opens the door of possibilities for web development. However, caution should be applied when using API’s. API’s that deal with financial transactions or the action of deleting, adding, or modifying data should be backed behind API key authentication. Anytime an API call is initiated between two systems, this encrypted key will be authorized once it reaches its designated server. If API keys are not used, a hacker can manipulate an API call to gain access to a backend system. Along with various software security threats, it is also paramount to focus in on the software development environment as well regarding ABC software. There are various threats against this environment that should be analyzed.

## **Software Development Environment**

In modern day times, the development of software requires an environment that is safe and secured. Most notably but not limited to a production environment. “Production environment is a term used mostly by developers to describe the setting where software and other products are actually put into operation for their intended uses by end users” (What Is a Production Environment, n.d). Security in this environment is paramount since live applications are being run while users are interacting and using said programs. However, these threats can also affect the development side of the environment. “A development environment is a collection of procedures and tools for developing, testing and debugging an application or a program” (What Is a Development Environment, n.d). Regardless if the environment is production or development, ABC software should take heed to the following potential environment threats.

**Development Environment Threats**

The first development environment threat that requires a considerable amount of attention is SQL Injection Attacks. With an SQL injection attack, an attacker would have the ability to directly run SQL queries against the underlying database. For obvious reasons this could be disastrous. As a counter measure, pre prepared SQL statements such as parametrized queries and stored procedures should be utilized. This way queries can only be run if called by a function. This eliminates the possibility of the application executing code that is inserted by an attacker. This threat mainly applies to the production environment.

The second development environment threat that can occur is if an attacker utilizes various vulnerability scans. An attacker would initially choose a potentially vulnerability system and commence various scans against that system. Various scans such as port scans, application scans or network-based scans. Once these scans come back to the hacker, they can then exploit that vulnerability and attempt to attack the system A simple counter measure to this is to perform these same scans on the system. Turn off any open ports that the application server does not need to run the application. Utilize proper firewall rules on the network where the production or development servers are held, and frequently review all server security logs. This is a threat that can be easily mitigated, but it is also a threat that is often overlooked.

The third development environment threat is session hijacking. This is a more sophisticated attack that deals with the interception of communication between a user and their desired resource. An attacker has various techniques at his or her disposal to make this happen. The attacker can take advantage of the user’s cookie data, replicating that data and thus acting like the user. Or the authentication details between a user and the server could be copied and used by the attacker. Regardless of the method, the result could mean the attacker gaining access to the resource acting like the user. If this user has administrative access to the web application, the attacker can inflict even more damage. Developers at ABC software should confirm that all authentication channels are secured, and that cookie data expires after a certain period.

The fourth development environment threat is buffer overflowing. This occurs when software developers fail to properly validate user input in an application. With this vulnerability, attackers can input large values that can cause the backend form processor to offload this input data into other memory mediums. This could in fact open the application up to the hacker to run commands on the underlying server. ABC software developers should take heed and make sure proper input validation is applied to all variables that are expected to receive input from a user. This decreases the likelihood of a buffer overflow. This is especially dangerous in the production environment.

The final development threat is the possibility of cross site request forgery. This attack works by the user thinking he or she is connected to their desired site. But it is a second website set up by an attacker to mimic the desired site. The user would then enter confidential information thinking they are signing into their desired site, however that information is now being received by the attacker which can then use this information. A simple solution to this is for ABC software developers to utilize secure web tokens embedded in their links. Attackers would not have this token; thus, they would not be able initiate their XSRF attack.

## **Summary**

As a whole ABC software is secure in some areas, however in other areas, more attention is needed. The one security area that needs significant improvement is the physical security of the building. This is an area that is often overlooked, but with the recent incident reports, this should be resolved immediately. Following physical security, the reliability of ABC software’s development environment is crucial as well. As this is the main driver for the company, this should be top priority. All in all, with my above recommendations, ABC software can expect an overall decline in security related incidents. Allowing the company to focus on business development and innovation within their industry.

## **References**

Goldfarb, J. (2022, June 13). *In security, less is more*. Dark Reading.

https://www.darkreading.com/edge-articles/in-security-less-is-more

Staff, D. R. (2020, December 14). *Identity and Access Management: Looking Ahead to 2021*.

Dark Reading.https://www.darkreading.com/operations/identity-and-access-management-

looking-ahead-to-2021

Hoffman, C. (2017, July 8). *How to create Advanced Firewall Rules in the windows firewall*.

How to Create Advanced Firewall Rules in the Windows Firewall. Retrieved November

21, 2022, from <https://www.howtogeek.com/112564/how-to-create-advanced-firewall->

rules-in-the-windows-firewall/

Barr, J. G. (2011, August). *Access Control Options*.

Data protection. (2016). In A. Burdett, & D. Bowen, *BCS glossary of computing* (14th ed.). BCS, The

Chartered Institute for IT.

Michael, C. C., Wyk, K. V., & Radosevich, W. (2005, September 23). *Risk-based and functional*

*security testing*. CISA.

Session hijacking attack. Session hijacking attack | OWASP Foundation. (n.d.)

<https://owasp.org/www-community/attacks/Session_hijacking_attack>

*What is error handling? - definition from Techopedia*. Techopedia.com. (n.d.).

<https://www.techopedia.com/definition/16626/errorhandling#:~:text=Explains%20Error%2>

0HandlingWhat%20Does%20Error%20Handling%20Mean%3F,programming%20errors%

20or%20communication%20errors.

What is production environment? - definition from Techopedia. Techopedia.com. (n.d.)

<https://www.techopedia.com/definition/8989/production-environment>

*What is development environment? - definition from Techopedia*. Techopedia.com. (n.d.)

<https://www.techopedia.com/definition/16376/developmentenvironment#:~:text=A%20dev>

elopment%20environment%20is%20a,debugging%20an%20application%20or%20program.