

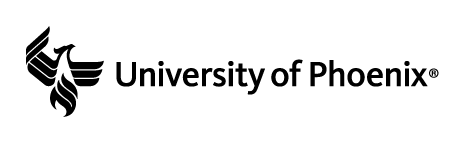
Secuirty Assessment Plan



July 27, 2020

Shane Ẽire Byrne

CYB407



Week 3 – Assignment Template

**Security Assessment Plan Worksheet**

Using the Assignment Scenario, **complete** the following worksheet.

| **Description of Vulnerability** | **Security Control Number and Name** | **Security Control Type** | **System Categorization for Risk Level Impact** | **Last Assessment Information** | **Asset** | **Assessment Method** | **Policy Alignment** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Broken Authentication: Successful: This being the occupation of a user’s account by an outside party. | Access Control (AC-2, 3, 5, 6, 7, 10, 11, 12)  Identification and Authentication (IA-2, 1, 4, 3, 5) | Hybrid. Physical and Technical | High | Adaptation to password and/or passphrase policy. Continued employee training to mitigate such things from happening. | System Access; Specifically, user access and groups as well as permissions. | Brute force, dictionary attacks, mask attack, Rainbow table attack, Shoulder surfing | Password/Passphrase: establishment of password or passphrase rules for every user. Proper expiration of access forcing the user to change passwords or pass phrases during allotted periods of time (90 days). Multifactor identification on possibly based on the user’s permissions (implicitly to be initiated for Administration level accounts). |
| Misconfiguration (Security): Simply failing to properly implement security controls for an asset. | System and Information Integrity (SI-2, 3, 4, 11, 10) | Hybrid. Technical and Administrative. | High | Configuration overview to ensure access to all assets is within specified acceptable tolerances. | System access and controls itself. | Probing (system backdoor, router backdoor) | Testing of all system hardware and software to ensure compliance with security requirements before implementation and integration into the system. |
| Security update(s): Inhouse and vendor patches for system software assets. | Maintenance (MA-1, 2, 3)  System and Information Integrity (SI-1, 4, 7) | Hybrid. Technical and Administrative. | High | Update any software that is not at its current version. | System hardware. | Take asset offline for testing of patch. Run patch checking for an anomalies or system issues. Apply patch to rest of assets if acceptable. | Ensure policies are put in place requiring all external software is brought up to its current instanciation. Establish policies to replace legacy software when patches are no long available. |

**References**

Gonzalez, K. (June 8, 2018) A Step-By-Step Guide to Vulnerability Assessment

Retrieved from <https://securityintelligence.com/a-step-by-step-guide-to-vulnerability-assessment/>

Rogers, B. E., Dunkerley, D. (2015). CRISC Certified in Risk and Information Systems Control All-in-One Exam Guide.

[[VitalSource Bookshelf version]]. Retrieved from vbk://1260118088

Scarfone, K., Souppaya, M., Cody, A., Orebaugh, A. (September 2008) National Institute of Standards and Technology Special Publication

(NIST) 800-115: Technical Guide to Information Security Testing and Assessment

Retrieved from <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf>

Walkowski, D. (August 22, 2019) What Are Security Controls?

Retrieved from <https://www.f5.com/labs/articles/education/what-are-security-controls>

Walsh, P. (January 28, 2014) 11 Key Components of Your Vulnerability Assessment Plan

Retrieved from <https://www.businesssecurityinformation.com/2014/01/11-components-vulnerability-assessment-plan/>