**Girls Global Academy**

**FY: 2023**

**Prior Year (FY22) Audit Concerns and Recommendations**

| **FY2022 PY Concerns** | **FY2022 PY Recommendations** | **FY2023 Current Year Status and Validation** |
| --- | --- | --- |
| **Logical Access Control**  There is no formal documented process for granting access, changing access, removing system access and entitlement reviews is not in place. Processes currently in place are informal.  There is no process in place to account for and monitor the use of accounts with escalated permissions.  Exposure to unauthorized transactions is increased. Accounts compromised with escalated permissions can lead to disruption of operations.  **Medium Risk** | Girls Global Academy School is recommended to put a formal process in place for granting access, changing access, removing system access and entitlement reviews are performed.  A process be put in place to account for and monitor the use of accounts with escalated permissions. | **Implemented**  Based on the current year follow up with the Management of Girls Global Academy, the School now has a formal process in place for granting access, changing access, removing access and to ensure entitlement review is performed. Therefore, the prior year concern has been addressed.  Based on the current year’s follow up, Girls Global Academy now has a process in place to account for and monitor the use of accounts with escalated permissions. Therefore, the Prior year concern has been addressed. |
| **Network Security and communication**  The following concerns were identified:  Vulnerability scanning is not performed.  Penetration and vulnerability tests are not performed on a periodic basis.  There are no defined timeframes for the remediation of high and medium risk vulnerabilities.  Lack of appropriate vulnerability scanning increases the risk that unidentified vulnerabilities may be exploited which may result in cyberattack, theft of data, or disruption to operations.  **(Medium Risk)** | Girls Global Academy School is recommended to do the following:  Adopt a formal process to perform vulnerability scanning.  Evaluate the cost and benefits of performing annual penetration testing.  Define a formal timeframe for the remediation of critical, high, and medium risk vulnerabilities. | **Implemented/Closed**  Discussion with the Management of Girls Global Academy revealed that management has already discussed additional scanning with DNS, their IT MSP. DNS has added additional functionality to the scanning they were already doing to provide additional security. Additionally, the students use Chromebooks, and the administration uses MAC books which are automatically maintained by Google/Apple. The few laptops in use are patched on a weekly basis.  In addition, management has researched the cost/benefit and has elected to not currently perform any penetration testing. Since their IT environment is 100% cloud based, the risk is somewhat mitigated. |
| **Cloud Service Provider:** The following concerns were identified:  A formal process is not in place to review the SOC reports.  The SOC report is not evaluated and shared with management in identifying exceptions and determining the impact on the risk environment.  **(Low Risk)** | * SBC recommended Girls Global Academy continue the effort of coordinating with Cloud Service Provider to receive and review updated audit (annually) reports (e.g., SOC/SSAE18) and ensure proper I.T. controls are in place. | **Partially Implemented** Discussion with management revealed that SOC reports are obtained from third party service providers and are reviewed. However, exceptions identified on the SOC reports and the risk they pose to the school are not shared with management. Additionally, the complementary user controls contained in the SOC report are not reviewed and implemented, where necessary.  **CY recommendation:**   * Continue efforts to share the results of the SOC report reviews, including the risk to the school posed by those exceptions. Additionally, review and implement, where applicable, the complementary user entity controls. |
| **Information Technology Support Processes/Cybersecurity Preparedness**  A risk assessment has not been performed to determine the critical risk threats to Girls Global Academy and to determine if the risk has been properly mitigated.  The following policies are not in place:  Cybersecurity Policy  Incident Response Plan  Lack of an Information Security/Cybersecurity Policy increases the risk that inappropriate security practices will be performed leading to the risk of a potential cybersecurity attack.  Failure to perform an annual risk assessment may expose GGA’s security environment to risks and vulnerabilities.  **Risk Level: Low** | Girls Global Academy should expand the current Information Technology policy to include additional Information Security areas like Data breach response plan and Remote access plan. It is also recommended to perform a risk assessment periodically. | **Partially Implemented**  Discussions with Girls’ Global Management revealed that a information/cybersecurity policy has been developed. However, a risk assessment has not been performed in the past 12 months.  **CY Recommendation:**  Girls’ Global PCS is recommended to put processes in place to perform an enterprise-wide risk assessment**.** |