Andrew Plum

Mr. Alves-Foss

Cyb 110

10/13/21

Ch. 6 Homework

Nist Exercise:

1) AU-1 Audit and Accountability Policy and Procedures
2) AU-2 Audit Events
3) AU-2(1) AUDIT EVENTS | COMPILATION OF AUDIT RECORDS FROM MULTIPLE SOURCES
4) AU-12. AU-2(2) AUDIT EVENTS | SELECTION OF AUDIT EVENTS BY COMPONENT
5) AU-12. AU-2(3) AUDIT EVENTS | REVIEWS AND UPDATES
6) AU-2(4) AUDIT EVENTS | PRIVILEGED FUNCTIONS
7) AU-3 Content of Audit Records
8) AU-3(1) CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION
9) AU-3(2) CONTENT OF AUDIT RECORDS | CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT
10) AU-4 Audit Storage Capacity
11) AU-4(1) AUDIT STORAGE CAPACITY | TRANSFER TO ALTERNATE STORAGE
12) AU-5 Response to Audit Processing Failures
13) AU-5(1) RESPONSE TO AUDIT PROCESSING FAILURES | AUDIT STORAGE CAPACITY
14) AU-5(2) RESPONSE TO AUDIT PROCESSING FAILURES | REAL-TIME ALERTS
15) AU-5(3) RESPONSE TO AUDIT PROCESSING FAILURES | CONFIGURABLE TRAFFIC VOLUME THRESHOLDS
16) AU-5(4) RESPONSE TO AUDIT PROCESSING FAILURES | SHUTDOWN ON FAILURE
17) AU-6 Audit Review, Analysis, and Reporting
18) AU-6(1) AUDIT REVIEW, ANALYSIS, AND REPORTING | PROCESS INTEGRATION
19) AU-6(2) AUDIT REVIEW, ANALYSIS, AND REPORTING | AUTOMATED SECURITY ALERTS
20) AU-6(3) AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT REPOSITORIES
21) AU-6(4) AUDIT REVIEW, ANALYSIS, AND REPORTING | CENTRAL REVIEW AND ANALYSIS
22) AU-6(5) AUDIT REVIEW, ANALYSIS, AND REPORTING | INTEGRATION / SCANNING AND MONITORING CAPABILITIES
23) AU-6(6) AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH PHYSICAL MONITORING
24) AU-6(7) AUDIT REVIEW, ANALYSIS, AND REPORTING | PERMITTED ACTIONS
25) AU-6(8) AUDIT REVIEW, ANALYSIS, AND REPORTING | FULL TEXT ANALYSIS OF PRIVILEGED COMMANDS
26) AU-6(9) AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH INFORMATION FROM NONTECHNICAL SOURCES
27) AU-6(10) AUDIT REVIEW, ANALYSIS, AND REPORTING | AUDIT LEVEL ADJUSTMENT
28) AU-7 Audit Reduction and Report Generation
29) AU-7(1) AUDIT REDUCTION AND REPORT GENERATION | AUTOMATIC PROCESSING
30) AU-7(2) AUDIT REDUCTION AND REPORT GENERATION | AUTOMATIC SORT AND SEARCH

31) AU-8 Time Stamps
32) AU-8(1) TIME STAMPS | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE
33) AU-8(2) TIME STAMPS | SECONDARY AUTHORITATIVE TIME SOURCE

Ch. 6 Questions:

1) The Family Educational Rights and Privacy Act (FERPA) of 1974 is a federal government regulation which is in place to protect student's records. The regulation applies to all students at all levels. When students turn 18, the rights to these records shift from the parents to the students. FERPA outlines how institutions must handle student records in order to protect them and how people can view and share them. FERPA is one of the US laws applicable to computing because schools now commonly hold student records in digital form which entails data management and security.

2) A compliance audit might be a positive occur because it holds people accountable and makes sure there is good practice at play in order to meet security standards. Holding people accountable helps to ensure these people aren't negligent and aids in deterring malicious behavior. An audit can also help an institution evaluate its practices and make improvements so that it can better protect its data. Meeting compliance in an audit can help an institution in a court of law so that if there is a breach in security and sensitive data was leaked, there is proof from the audit that the institution followed good practice.

7) Industry regulations can enable or disable an institution's ability to conducts business. For example, PCI DSS regulations are regulations that govern processing credit card transactions and protecting associated data. Credit card companies want businesses using their credit card services to use good practices because consumers would not want to use these credit card services if good practices weren't in place to protect their credit card information. If a company doesn't meet industry compliance, they may face fines or have their status reduced which will in turn hinder their ability to conduct business in the industry.

10) The two indicators of the type of compliance standards your company might fall under are government and industry compliance regulations. Government compliance standards are regulations put in place by the government, whether its domestic or foreign, that must be followed, or the company could face lawsuits, fines, jail time for certain bad actors, and even be shut down if practices are bad enough. Industry compliance standards are put in place by businesses in the industry to help them in conducting business and protect their reputation as a business. Consequences for not meeting industry compliance could entail fines and or a reduced status which would disable the company's ability to conduct business.