OCTAVE Allegro Risk Assessment

System: Securing a University’s Online Learning Platform

|  |  |  |  |
| --- | --- | --- | --- |
| **Allegro Worksheet 1** | **Risk Measurement Criteria – Reputation and Customer Confidence** | | |
| **Impact Area** | **Low** | **Moderate** | **High** |
| *Reputation* | Reputation is minimally affected; little or no effort or expense is required to recover. | Reputation is damaged, and some effort and expense is required to recover. | Reputation is irrevocably destroyed or damaged. |
| *Customer Loss* | Less than 5% reduction in customers due to loss of confidence | 5% to 15% reduction in customers due to loss of confidence | More than 15% reduction in customers due to loss of confidence |
| *Academic Trust:* | Negative social media attention, temporary complaints | News coverage or external audit | Regulatory involvement or university ranking impact |

|  |  |  |  |
| --- | --- | --- | --- |
| **Allegro Worksheet 2** | **Risk Measurement Criteria – Financial** | | |
| **Impact Area** | **Low** | **Moderate** | **High** |
| *Operating Costs* | Increase of less than 5% in yearly operating costs | Yearly operating costs increase by 5% to 15%. | Yearly operating costs increase by more than 15%. |
| *Revenue Loss* | Less than 2% yearly revenue loss | 2% to 10% yearly revenue loss | Greater than 10% yearly revenue loss |
| *One-Time Financial Loss* | One-time financial cost of less than $5,000 | One-time financial cost of $5,000 to $50,000 | One-time financial cost greater than $50,000 |
| *Incident Response* | Minor system restoration | Need to reimplement major services | Major infrastructure overhaul |

|  |  |  |  |
| --- | --- | --- | --- |
| **Allegro Worksheet 3** | **Risk Measurement Criteria – Productivity** | | |
| **Impact Area** | **Low** | **Moderate** | **High** |
| *Staff Hours* | Staff work hours are increased by less than 10% for 1 to 3 day(s). | Staff work hours are increased between 10% and 20% for 4 to 6 day(s). | Staff work hours are increased by greater than 30% for 7 to 14 day(s). |
| *Learning Disruption* | Minor assignment delays | Missed exams or coursework | Full academic calendar disruption |

|  |  |  |  |
| --- | --- | --- | --- |
| **Allegro Worksheet 4** | **Risk Measurement Criteria – Safety and Health** | | |
| **Impact Area** | **Low** | **Moderate** | **High** |
| *Life* | No loss or significant threat to customers’ or staff members’ lives | Customers’ or staff members’ lives are threatened, but they will recover after receiving medical treatment. | Loss of customers’ or staff members’ lives |
| *Health* | Minimal, immediately treatable degradation in customers’ or staff members’ health with recovery within four days | Temporary or recoverable impairment of customers’ or staff members’ health | Permanent impairment of significant aspects of customers’ or staff members’ health |
| *Safety* | Safety questioned | Safety affected | Safety violated |

|  |  |  |  |
| --- | --- | --- | --- |
| **Allegro Worksheet 5** | **Risk Measurement Criteria – Fines and Legal Penalties** | | |
| **Impact Area** | **Low** | **Moderate** | **High** |
| *Fines* | Fines less than $10,000 are levied. | Fines between $10,000 and $100,000 are levied. | Fines greater than $100,000 are levied. |
| *Lawsuits* | Non-frivolous lawsuit or lawsuits less than $5,000 are filed against the organization, or frivolous lawsuit(s) are filed against the organization. | Non-frivolous lawsuit or lawsuits between $5,000 and $50,000 are filed against the organization. | Non-frivolous lawsuit or lawsuits greater than $50,000 are filed against the organization. |
| *Investigations* | No queries from government or other investigative organizations | Government or other investigative organization requests information or records (low profile). | Government or other investigative organization initiates a high-profile, in-depth investigation into organizational practices. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Allegro Worksheet 6** | **Risk Measurement Criteria – User Defined** | | |
| **Impact Area** | **Low** | **Moderate** | **High** |
| *Academic Integrity* | Minor data exposure | Tampering with assignments or grades | Widespread grade manipulation or leaks |
| *Student Satisfaction* | Minor dissatisfaction; few complaints. | Noticeable complaints affecting course evaluations. | Widespread dissatisfaction causing student retention problems. |

|  |  |  |
| --- | --- | --- |
| **Allegro Worksheet 7** | | **Impact Area Prioritization Worksheet** |
| **Priority** | **Impact Areas** | |
| 1 | **Reputation and Customer Confidence** | |
| 3 | **Financial** | |
| 2 | **Productivity** | |
| 4 | **Safety and Health** | |
| 6 | **Fines and Legal Penalties** | |
| 5 | **User Defined** | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Allegro Worksheet 8** | **Critical Information Asset Profile** | | | | |
| **(1) Critical Asset**  *What is the critical information asset?* | **(2) Rationale for Selection**  *Why is this information asset important to the organization?* | | | **(3) Description**  *What is the agreed-upon description of this information asset?* | |
| University’s Online Learning Platform | It is vital for delivering education, conducting assessments, maintaining academic records, and communication. | | | An online platform that supports course delivery, assignments, discussions, grading, and examinations for students and faculty. | |
| **(4) Owner(s)**  *Who owns this information asset?* | | | | | |
| IT Department and Academic Affairs Office. | | | | | |
| **(5) Security Requirements**  *What are the security requirements for this information asset?* | | | | | |
| * **Confidentiality** | Only authorized personnel can view this information asset, as follows: | | ** Students may access only their own courses, grades, and personal data.**  ** Faculty and instructors can access student submissions, course materials, and grading information.** | | |
| * **Integrity** | Only authorized personnel can modify this information asset, as follows: | | **Instructors and professors can modify course content, grades, and assessment results.** | | |
| * **Availability** | This asset must be available for these personnel to do their jobs, as follows: | |  Students must have continuous access to course materials, assignment submissions, discussion forums, and exams at all times during academic terms.   Faculty **and Instructors** must have uninterrupted access to create, manage, and grade course content to meet academic deadlines.   | | |
| This asset must be available for 24 hours,7 days/week, 50 weeks/year. | |  Administrative **Staff** must be able to access the system for enrollment management, academic record keeping, and reporting functions.   **IT Support Staff** must have administrative access for maintenance, troubleshooting, and incident response 24/7. | | |
| * **Other** | This asset has special regulatory compliance protection requirements, as follows: | | **** Must adhere to **GDPR**  ** Must comply with FERPA** | | |
| **(6) Most Important Security Requirement**  *What is the most important security requirement for this information asset?* | | | | | |
| * Confidentiality | * Integrity | * Availability | | | * Other |

|  |  |  |
| --- | --- | --- |
| **Allegro Worksheet 9a** | **Information Asset Risk Environment Map (Technical)** | |
| **Internal** | | |
| **Container Description** | | **Owner(s)** |
| 1. University Learning Management System (LMS) servers | | University IT Department |
| 1. Database Servers | | Database Administrator Team |
| 1. Backup and recovery systems | | IT Operations |
| 1. Authentication servers | | IT Security Team |
| **External** | | |
| **Container Description** | | **Owner(s)** |
| 1. Cloud hosting provider | | Amazon AWS |
| 1. Third-party plagiarism detection systems | | Vendor (IT department oversees) |
| 1. Online proctoring software | | Vendor (managed by Academic Affairs) |

|  |  |  |
| --- | --- | --- |
| **Allegro Worksheet 9b** | **Information Asset Risk Environment Map (Physical)** | |
| **Internal** | | |
| **Container Description** | | **Owner(s)** |
| 1. data server rooms | | University Facilities |
| 1. Campus networking closets and cabling infrastructure | | IT Network Team |
| 1. Computer labs used by students | | |  | | --- | |  |  |  | | --- | | **Lab Technicians** | |
| **IT Support** |
| **External** | | |
| **Container Description** | | **Owner(s)** |
| * **Cloud vendor's data centers** | | Amazon AWS |
| * **Off-site backup facilities** | | Disaster Recovery Provider |

|  |  |  |
| --- | --- | --- |
| **Allegro Worksheet 9c** | **Information Asset Risk Environment Map (People)** | |
| **Internal Personnel** | | |
| **Name or Role/Responsibility** | | **Department or Unit** |
| 1. Students | | Students Affairs |
| 1. **Faculty and Instructors** | | Academic Affairs |
| 1. IT Administrators | | IT Department |
| **External Personnel** | | |
| **Contractor, Vendor, Etc.** | | **Organization** |
| 1. Cloud service account managers | | Amazon AWS |
| 1. External cybersecurity consultants | | PWC |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Allegro - Worksheet 10** | | | **Information Asset Risk Worksheet** | | | | | |
| **Information Asset Risk** | **Threat** | Information Asset | University Online Learning Platform (LMS) | | | | | |
| Area of Concern | *Platform security vulnerabilities* | | | | | |
| (1) Actor  *Who would exploit the area of concern or threat?* | | hacker | | | | |
| (2) Means  *How would the actor do it? What would they do?* | | * Brute force attack on weak passwords * exploiting known vulnerabilities in LMS software * phishing faculty credentials | | | | |
| (3) Motive  *What is the actor’s reason for doing it?* | | * To change grades in favor of themselves or others * sabotage academic integrity | | | | |
| (4) Outcome  *What would be the resulting effect on the information asset?* | | * **Disclosure** * **Modification** | | * **Destruction** * **Interruption** | | |
| (5) Security Requirements  *How would the information asset’s security requirements be breached?* | | Breach of **Integrity** (modifying academic records without authorization) | | | | |
| (6) Probability  *What is the likelihood that this threat scenario could occur?* | | * **High** | * **Medium** | | * **Low** | |
| (7) Consequences  *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?* | | | | (8) Severity  *How severe are these consequences to the organization or asset owner by impact area?* | | | |
| **Impact Area** | | **Value** | **Score** |
| Loss of academic integrity | | | | Reputation & Customer  Confidence | | High | 3 |
| Financial | | Moderate | 2 |
| Student and faculty distrust the platform | | | | Productivity | | Moderate | 2 |
| Safety & Health | | low | 1 |
| Possible lawsuits from affected students | | | | Fines & Legal Penalties | | Moderate | 2 |
| User Defined Impact Area | | High | 3 |
| **Relative Risk Score** | | | | | | | | **13** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **(9) Risk Mitigation**  *Based on the total score for this risk, what action will you take?* | | | | |
| * **Accept** | | * **Defer** | * **Mitigate** | * **Transfer** |
| **For the risks that you decide to mitigate, perform the following:** | | | | |
| *On what container would you apply controls?* | *What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?* | | | |
| LMS Servers and Databases | unknown vulnerabilities (zero-day attacks) | | | |
| Authentication Systems | Residual risk remains from social engineering attacks (phishing attacks) | | | |
| Backup and Recovery Systems | backup corruption or delayed restoration | | | |
| Cloud Hosted Environment | cloud provider service outages or misconfigurations | | | |