RISK ASSESSMENT REPORT (RAR) TEMPLATE

Happy Land School  
*Learning Management System (LMS)*September 20, 2024

**Record of Changes:**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Sections Modified | Description of Changes |
| 0.1 | 05 10 2024 | Initial RAR | Initial report setup |

**System Description**

The **Learning Management System (LMS)** is designed to support Happy Land School in facilitating online course management, communication between teachers, students, and parents, and grade recording. The system processes **Confidential-Low** level data, and its risk categorization is assessed as **Moderate-Low-Low**.

**IS# LMS-001** is located in the school's IT infrastructure (if applicable), housed in a secured server room or in a secured room. The LMS has no external connections (wired or wireless) beyond the internal school network. This system is utilized for course delivery, student record management.

**Information Owner:** [TBA]  
**ISSM:** [TBA]  
**ISSO:** [TBA]

**Scope**

The scope of this risk assessment focuses on the LMS’s utilization of resources and control measures to mitigate vulnerabilities exploited by internal and external threat agents. The assessment was conducted following the **NIST SP 800-53** framework, ensuring compliance across all critical controls.

* **Range of threats:** Adversarial, structural, and environmental risks.
* **Compliance tools:** Automated system scans, vulnerability assessments, and manual checks against **NIST SP 800-53** controls.
* **Operating and physical security conditions:** The system is housed in a physically secure, climate-controlled environment with backup power. All access to the system is controlled and monitored.
* **Timeframe:** This initial assessment will guide the LMS implementation phase and be updated post-certification testing.

**Purpose**

*The purpose of this risk assessment is to document and evaluate residual risks following the selection and implementation of security controls for the LMS. The assessment is conducted to provide a risk profile and inform key stakeholders of potential areas of vulnerability.*

**Risk Assessment Approach**

This assessment follows the **NIST SP 800-30** guidelines and employs a **qualitative** approach to determine risk based on identified threat events, likelihood of occurrence, system vulnerabilities, and potential impact on the school’s mission.

**Table 1: Sample Threat Sources**

**Table 1: Sample Threat Sources (see NIST SP 800-30 for complete list)**

| TYPE OF THREAT SOURCE | DESCRIPTION |
| --- | --- |
| ADVERSARIAL | Insiders, privileged users, or external groups seeking to exploit vulnerabilities in the LMS. |
| STRUCTURAL | Failures in IT equipment, software bugs, and environmental control malfunctions. |
| ENVIRONMENTAL | Natural disasters (floods, fires) and infrastructure failures (e.g., power outages, network loss). |

The following tables from the NIST SP 800-30 were used to assign values to likelihood, impact, and risk:

**Table 2: Assessment Scale – Likelihood of Threat Event Initiation (Adversarial)**

| Qualitative Values | Semi-Quantitative Values | | Description |
| --- | --- | --- | --- |
| Very High | 96-100 | 10 | Adversary is **almost certain** to initiate the threat event. |
| High | 80-95 | 8 | Adversary is **highly likely** to initiate the threat event. |
| Moderate | 21-79 | 5 | Adversary is **somewhat likely** to initiate the threat event. |
| Low | 5-20 | 2 | Adversary is **unlikely** to initiate the threat event. |
| Very Low | 0-4 | 0 | Adversary is **highly unlikely** to initiate the threat event |

**Table 3: Assessment Scale – Likelihood of Threat Event Occurrence (Non-adversarial)**

| Qualitative Values | Semi-Quantitative Values | | Description |
| --- | --- | --- | --- |
| Very High | 96-100 | 10 | Error, accident, or act of nature is **almost certain** to occur; or occurs **more than 100 times per year**. |
| High | 80-95 | 8 | Error, accident, or act of nature is **highly likely** to occur; or occurs **between 10-100 times per year**. |
| Moderate | 21-79 | 5 | Error, accident, or act of nature is **somewhat likely** to occur; or occurs **between 1-10 times per year**. |
| Low | 5-20 | 2 | Error, accident, or act of nature is **unlikely** to occur; or occurs **less than once a year,** but **more than once every 10 years**. |
| Very Low | 0-4 | 0 | Error, accident, or act of nature is **highly unlikely** to occur; or occurs **less than once every 10 years**. |

**Table 4: Assessment Scale – Impact of Threat Events**

| Qualitative Values | Semi-Quantitative Values | | Description |
| --- | --- | --- | --- |
| Very High | 96-100 | 10 | The threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation. |
| High | 80-95 | 8 | The threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries. |
| Moderate | 21-79 | 5 | The threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries. |
| Low | 5-20 | 2 | The threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals. |
| Very Low | 0-4 | 0 | The threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. |

**Table 5: Assessment Scale – Level of Risk**

| Qualitative Values | Semi-Quantitative Values | | Description |
| --- | --- | --- | --- |
| Very High | 96-100 | 10 | Threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation. |
| High | 80-95 | 8 | Threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. |
| Moderate | 21-79 | 5 | Threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. |
| Low | 5-20 | 2 | Threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. |
| Very Low | 0-4 | 0 | Threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. |

**Table 6: Assessment Scale – Level of Risk (Combination of Likelihood and Impact)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Likelihood (That Occurrence Results in Adverse Impact)** | **Level of Impact** | | | | |
| Very Low | Low | Moderate | High | Very High |
| Very High | Very Low | Low | Moderate | High | Very High |
| High | Very Low | Low | Moderate | High | Very High |
| Moderate | Very Low | Low | Moderate | Moderate | High |
| Low | Very Low | Low | Low | Low | Moderate |
| Very Low | Very Low | Very Low | Very Low | Low | Low |

Risk Assessment Approach

**Risk Assessment Results**

| Threat Event | Vulnerabilities / Predisposing Characteristics | Mitigating Factors | Likelihood (Tbl 2 or 3) | Impact (Table 4) | Risk  (Tbls 5 & 6) |
| --- | --- | --- | --- | --- | --- |
| *Cyber Attack* | *Weak authentication mechanisms* | *Multi-factor authentication* | *Low* | *High* | *Moderate* |
| Power Outage | Dependence on electrical grid | Backup generators | *Moderate* | *Low* | *Low* |
| Data Breach | Insufficient encryption of student records | Data encryption standards | *Low* | *High* | *Moderate* |
| Flood | Server room located in low-lying area | Physical flood barriers | *Low* | *High* | *Moderate* |
| Human Error | Inexperienced LMS administrators/teachers | Regular training | *Moderate* | *Moderate* | *Moderate* |

\* Likelihood / Impact / Risk = Very High, High, Moderate, Low, or Very Low