**Information Security Risk Assessment Template**

**1. Risk Identification**

* **Information Security Risk ID:**
* **Risk Observation:**
* **Risk Statement:**

**2. Threat Analysis**

* **Threat Actor Source:**
* **Threat Target:**
* **Threat Motive:**

**3. Impact Assessment**

* **Impact on Confidentiality (Score 0-5):** [Assess the potential impact on the confidentiality of the targeted asset]
* **Impact on Integrity (Score 0-5):** [Assess the potential impact on the integrity of the targeted asset]
* **Impact on Availability (Score 0-5):** [Assess the potential impact on the availability of the targeted asset]
* **Impact Score:** [Sum of the impact scores]

**4. Threat Capability Assessment**

* **Threat Means (Score 0-5):** [Assess the capability of the threat actor to carry out the threat]
* **Threat Motive (Score 0-5):** [Score the strength of the threat actor's motivation]
* **Threat Opportunity (Score 0-5):** [Assess the opportunity the threat actor has to exploit the vulnerability]
* **Threat Score:** [Sum of the threat capability scores]

**5. Risk Scoring**

* **Inherent Risk Score:** [Impact Score \* Threat Score]
* **Likelihood of Occurrence (Score 0-5):** [Assess the likelihood that the risk event will occur]

**6. Risk Evaluation**

* **Overall Risk Score:** [Inherent Risk Score \* Likelihood]

**7. Control Effectiveness**

* **Strength of Control (Score 0-5):** [Evaluate the effectiveness of existing controls in mitigating the risk]

**8. Residual Risk**

* **Residual Risk Score:** [Overall Risk Score \* (1 - Strength of Control/5)]

**9. Risk Treatment Plan**

* **Mitigation Strategy:** [Describe the approach to mitigate, transfer, accept, or avoid the risk]
* **Responsible Party:** [Identify who is responsible for implementing the mitigation strategy]
* **Timeline:** [Specify the timeline for implementing the mitigation]