

**SECURITY THREAT AND RISK ASSESSMENT (STRA)**

Title of assessment/target assessed.

Date

**Table of Contents**

[1.0 Introduction 2](#_Toc172033334)

[2.0 Target Definition 3](#_Toc172033335)

[2.1 System Business Purpose 4](#_Toc172033336)

[2.2 Concept of Operation 4](#_Toc172033337)

[2.3 Interdependency and Information Sharing 4](#_Toc172033338)

[2.4 System & Data Parameters 5](#_Toc172033339)

[3.0 Information Sensitivity & Criticality 7](#_Toc172033340)

[3.1 Confidentiality 7](#_Toc172033341)

[3.2 Privacy 8](#_Toc172033342)

[3.3 Integrity 9](#_Toc172033343)

[3.4 Availability 10](#_Toc172033344)

[4.0 Threats and Risks Assessment 13](#_Toc172033345)

[4.1 Assessment Stage 13](#_Toc172033346)

[4.2 Identification of Known Vulnerabilities 13](#_Toc172033347)

[5.0 Statement of Acceptable Risk 18](#_Toc172033348)

[5.1 Proposed Treatment Plan/s 18](#_Toc172033349)

[5.2 Risk Treatment Plans 21](#_Toc172033350)

[Information Custodian Signature 21](#_Toc172033351)

[6.0 Reviews and Approvals 22](#_Toc172033352)

[Information Controller Signature 22](#_Toc172033353)

[[Cybersecurity authorized personnel] Signature 22](#_Toc172033354)

[Appendix A: Risk Assessment Considerations 23](#_Toc172033355)

[Glossary of Terms 27](#_Toc172033356)

1.0 Introduction

The Security Threats and Risks Assessment (STRA) is used to identify security threats and assess risks relating to online systems (target of the assessment), develop treatment plans for identified risks, and ensure that identified risks become part of the organization’s Risk Register, ensuring that risks are managed while the related system is used in production.

The STRA can also be used to assist in deciding whether a service or solution should be implemented based on assessed risks and potential treatment of the risks.

|  |  |
| --- | --- |
| **Reference**  | \*For [insert the name of unit responsible for risk in your organization] use only  |
|  |  |
| STRA ID#:  |   |
| Previous risk assessment completed?  | ​​☐​ Yes   ​☐​ No   \*If ‘Yes’ provide previous ID#  |
| Does the application currently exist in an application repository? | ​​☐​ Yes   ​☐​ No   ​☐​ N/A   \*If ‘No’ submit a request through organization-defined process. |
| Application name as in Application repository:  |   |
| Application acronym as in application repository:  |   |
| Application ID as in application repository: |   |

Note: If an application repository does not exist the corresponding questions may be skipped as it does not affect the assessment on the whole.

2.0 Target Definition

|  |  |
| --- | --- |
| System Name: |  |
| Business Unit: |  |
| Business Unit Contact: |  |
| Information Controller:  |  |
| Information Custodian:  |  |
| Cybersecurity Contact: |  |

2.1 System Business Purpose

Please provide a description of the business purpose of the system:

[Please enter your response in here]

2.2 Concept of Operation

A conceptual model can serve as a representation of the proposed system. Insert a diagram, model or a description here of how the system will function:

To promote completeness, please refer to Appendix A for additional information as necessary.

[Please enter your response in here]

2.3 Interdependency and Information Sharing

Due to interdependencies, the loss or degradation of one service and its associated assets may affect other services or assets. It is important to identify these relationships and involvement of third-party stakeholders such as companies in the private sector or other governmental groups.

Please describe any interdependencies for this application. Use a diagram if necessary.

[Please enter your response in here]

To promote completeness, please refer to Appendix A for additional information as necessary.

Is information shared with the following? (*Check all that apply*)

|  |
| --- |
| [ ]  Other internal business areas[ ]  Other departments within the organization |
| [ ]  Other public agencies |
| [ ]  Government of Canada[ ]  Other Canadian governmental organizations[ ]  Other non-Canadian governmental organizations[ ]  Non-governmental organizations/Private sector companies[ ]  None |
| [ ]  Other: |  |

At a high level, describe the sharing arrangement, if any exist, or legislation/legal that applies to any sharing arrangement. This includes identifying the information classification used to classify the information as well as handling procedures for that information. Use a diagram if necessary.

[Please enter your response in here]

To promote completeness, please refer to Appendix A for additional information as necessary.

2.4 System & Data Parameters

What is the type of system? *(Check all that apply)*

|  |
| --- |
| [ ]  Cloud-based Procured Service (XaaS)[ ]  Cloud Hosted Custom (internally developed) |
| [ ]  On Premise Hosted Procured System (off the shelf) |
| [ ]  On Premise Hosted Custom System (internally developed)  |
| [ ]  Other |  |

Technologies and Platforms making up the solution (*Check all that apply*)

|  |
| --- |
| [ ]  Windows [ ]  Web Application [ ]  Mobile [ ]  Cloud[ ]  Linux/Unix [ ]  Local Client/Server [ ]  Desktop Application |
| [ ]  Other: |  |

What is the target audience or user community? (*Check all that apply*)

|  |  |
| --- | --- |
| [ ]  Internal | Example: A system that only internal users can access. |
| [ ]  External Business Client: | Example: A site-to-site VPN between the organization and an agency. |
| [ ]  Public: | Example: A system accessible by anyone on the internet. |
| [ ]  Other: |  |

Number of End-Users:

Identify the estimated total of all users (internal and external) of the system.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| [ ]  <25 | [ ]  25 – 100 | [ ]  100 – 500 | [ ]  500 – 1000 | [ ]  > 1000 |

3.0 Information Sensitivity & Criticality

The following section captures the *Confidentiality, Integrity* and *Availability (CIA)* properties of the information within the system and will assist in identifying its risk sensitivity.

3.1 Confidentiality

|  |  |
| --- | --- |
| Confidentiality: | System and data confidentiality refers to the protection of information from unauthorized, unanticipated, or unintentional disclosure. Disclosure could result in loss of public confidence, embarrassment, legal action, or injury to the organization or customers. |

**Please describe the types of information that will be contained, collected, or processed by the system:**

[Please enter your response in here]

There are usually four levels or categories of security classifications that organizations may apply to their data and information. Organizations may have guidelines that are available to help classify data and information. To ensure application information remains consistent, please obtain the data for this section from the Application Repository. If this is a new system, information is missing or is not what you expected, please contact relevant teams.

**Note:** Information that has been received from another department/organization MUST maintain the classification level assigned by the originating organization; and be handled according to the rules and procedures established by that organization.

|  |
| --- |
| **Assessed Overall System Classification:** (Check only the highest classification identified)[ ]  Public [ ]  Protected A [ ]  Protected B [ ]  Protected C |

**Note:** Tailor the classifications to be organization specific.

**Impact of loss of confidentiality:**

The ***overall*** impact to the business should information contained within the application or service be **used inappropriately** (e.g., unauthorized access). *Please choose from the red drop-down menu:* Choose the impact.

**Please choose all *business* impacts below that apply:**

[ ]  Financial

[ ]  Legal/Regulatory

[ ]  Life and Safety

[ ]  Environmental

[ ]  Operational

[ ]  Reputational

Please enter any additional details here.

To promote completeness, please refer to Appendix A for additional information as necessary.

3.2 Privacy

If the system collects, processes, stores or transmits personal information as it pertains to the Freedom of Information and Protection of Privacy (FOIP) Act, and a Privacy Impact Assessment (PIA) or other privacy review mechanism has not been completed, please consult relevant Privacy management team.

Organizations maybe responsible for completing PIAs concerning the collection, use, and/or disclosure of health information, and submitting them to the Alberta Office of the Information and Privacy Commissioner (OIPC) ahead of implementation.

Alberta Health can be contacted via AHprivacy@gov.ab.ca  for roles and expectations regarding the management and protection of health information.

To promote completeness, please refer to Appendix A for additional information as necessary.

|  |  |
| --- | --- |
| Has a previous Privacy Impact Assessment (PIA) or privacy scan been performed on the system?[ ]  Yes [ ]  No [ ]  Unknown  |  |
|  |
| If “Yes”, provide the date completed and a link to the previous PIA or privacy scan document. |

3.3 Integrity

|  |  |
| --- | --- |
| Integrity: | System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. |

**Impact of loss of integrity:**

The ***overall*** impact to the business should there be a **loss of information integrity** (e.g., data is inadvertently modified) within the application or service**.** *Please choose from the red drop-down menu:* Choose the impact.

**Please choose all *business* impacts below that apply:**

[ ]  Financial

[ ]  Legal/Regulatory

[ ]  Life and Safety

[ ]  Environmental

[ ]  Operational

[ ]  Reputational

Please enter any additional details here.

To promote completeness, please refer to Appendix A for additional information as necessary.

3.4 Availability

|  |  |
| --- | --- |
| Availability: | If a key IT system is unavailable to its end users, the organization’s mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time or reputation; thus, impeding the end users’ performance of their functions in supporting the organization’s mission. |

**Impact of loss of availability:**

The ***overall*** impact to the business should this application or service become **unavailable** for an extended period. *Please choose from the red drop-down menu:*

 Choose the impact.

**Please choose all *business* impacts below that apply:**

[ ]  Financial

[ ]  Legal/Regulatory

[ ]  Life and Safety

[ ]  Environmental

[ ]  Operational

[ ]  Reputational

Please enter any additional details here.

Is the system/service identified as a ‘Critical Business Service’ for Business Continuity purposes?

[ ]  Yes [ ]  No

If “Yes”, identify the Critical Service(s) that the system supports:

Please enter your response here.

If “Yes”, identify the alternate means of delivering the Critical Service(s):

Please enter your response here.

|  |  |
| --- | --- |
| IT Disaster Recovery: | IT disaster recovery is the technical aspect of business continuity that ensures IT systems and applications can be recovered to a known working state (recovery time and recovery point) following an unplanned IT outage or disaster event.  |

For consistency, the following disaster recovery values could be tailored to organization.

**Recovery Time Objective (RTO - business)**: The maximum estimated time that an application or system can be down to avoid unacceptable consequence to the business following a disaster.

|  |  |
| --- | --- |
| [ ]  **RTO 0** | * No Downtime
 |
| [ ]  **0 to 24 hours** | * Must be restored within 24 hours
 |
| [ ]  **24 to 72 hours** | * Must be restored within 72 hours
 |
| [ ]  **72 hours to 2 weeks** | * Must be restored within 2 weeks
 |
| [ ]  **More than 2 weeks** | * Must be restored within more than 2 weeks
 |

**Recovery Point Objective (RPO) - business):** The maximum data loss the business can tolerate before significant impact to business operations, measured from the point of the disaster event.

|  |  |
| --- | --- |
| [ ]  **No Data Loss** | * Little to no interruption or data loss
 |
| [ ]  **Up to 1 hour** | * Minimal data loss
 |
| [ ]  **1 to 4 hours** | * Some data loss
 |
| [ ]  **4 to 24 hours** | * Moderate data loss
 |
| [ ]  **More than 24 hrs** | * Significant data loss
 |

**Note:** In instances where specific information technology pieces support more than one classification of essential services, they should be restored using the priority of the highest classification level.

4.0 Threats and Risks Assessment

4.1 Assessment Stage

Applications and other digital solutions go through a lifecycle that normally includes:

 *Concept -> Design -> Development -> Implementation -> Production -> Maintenance -> Decommission*

The particular stage when the assessment is performed can usually indicate the level of confidence that should be given to the assessment. A system assessed at the idea or conceptual stage for instance may change as the lifecycle progresses, but one already in production would truly reflect the threats that come with the system.

Please indicate below at which stage this assessment was performed (pick from above):

Choose a Stage

4.2 Identification of Known Vulnerabilities

Vulnerabilities are the known potential weaknesses or shortcomings of a solution that are known and could be exploited by an attack.

Threats are the potential exploits of vulnerabilities that could be executed during an attack, and the potential negative impacts resulting from these exploits.

The Risk is the organizational exposure generated by the probability and potential impact of a threat materializing itself. It is assessed by multiplying the probability (P) factor with the impact (I) factor to obtain the overall exposure (E=PxI) factor, which is used to prioritize identified threats.

Recommended Treatment refers to the expected response to identified risks based on probability, impact, and overall exposure. Should the Information Controller Accept the risk and do nothing to mitigate them? Should they Reduce the risk by implementing controls to reduce the probability and/or the impact of the risk? Should they Avoid the risk by discontinuing activities that are generating the risk? Should they Transfer the risk by outsourcing work relating to potential impacts or passing the risk to partners?

Please enter your response here.

To promote completeness, please refer to Appendix A for additional information as necessary.

| **ID** | **Risk Description**Bold the **risk statement/negative event**, then explain the causes and potential consequence/s in lowercase.Please use short descriptions but also clear. They must refer to the exact threat and business impacts posed by the risks that have been identified.The completed risk description should look something like:[Negative Event] caused by [cause/s] resulting in [consequence/s]. | **P** | **I** | **Exposure**E=PxI | **Treatment**Accept/ Avoid/ Transfer/ Reduce | **Risk Owner**By default, this is the information controller, unless already assigned |
| --- | --- | --- | --- | --- | --- | --- |
| R1 | <e.g., ***Unauthorized access to Protected Information through brute force attacks*** *caused by weak passwords resulting in financial losses, identify theft and reputational losses*.> | ? | ? | <PxI> |  | Name of risk owner |
| R2 | <e.g., ***Accidental breach of Protected Information*** *caused by an untrained user not following information disclosure policies by sharing a file through an email attachment, thereby losing access controls to the file and resulting in Reputational Losses, potential Legal/Regulatory violations*> | ? | ? | <PxI> |  | Name of risk owner |

LEGEND FOR PROBABILITY (P):

|  |  |  |
| --- | --- | --- |
| **5** | **Critical** | Almost certain for the organization. Vulnerability verified, exploits confirmed in the industry, and reported attempted attacks confirmed. |
| **4** | **High** | Confirmed occurrence in industry. Vulnerability has been verified, and there are some confirmed exploits in the industry. |
| **3** | **Medium** | Confirmed chance it might happen. Vulnerability has been verified, but no reported exploit in the industry. |
| **2** | **Low** | Unconfirmed chance it could happen. Newly identified vulnerability that would be hard to exploit, and no actual exploits reported. |
| **1** | **Very Low** | Negligible, unlikely to happen. Vulnerability unconfirmed, no exploits reported. |

LEGEND FOR IMPACT (I):

|  |  |  |
| --- | --- | --- |
| **5** | **Critical** | Catastrophic: Multiple impacts, nearly impossible to recover. |
| **4** | **High** | Major: Large impacts, difficult to recover. |
| **3** | **Medium** | Moderate: Large impacts, plans in place to recover. |
| **2** | **Low** | Minor: Minimal impacts, plans in place to recover quickly. |
| **1** | **Very Low** | Insignificant: Negligible/minimal disruptions, easy to recover. |

LEGEND FOR EXPOSURE (E): Priority indicator

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **5** | **5** | **10** | **15** | **20** | **25** |
| **4** | **4** | **8** | **12** | **16** | **20** |
| **3** | **3** | **6** | **9** | **12** | **15** |
| **2** | **2** | **4** | **6** | **8** | **10** |
| **1** | **1** | **2** | **3** | **4** | **5** |
| **P / I** | **1** | **2** | **3** | **4** | **5** |

5.0 Statement of Acceptable Risk

The Statement of Acceptable Risk is a vehicle for the Information Controller to document existing and proposed mitigations for risks identified in section 4.

5.1 Proposed Treatment Plan/s

Provide any recommended treatment plans for each risk identified in section 4, hopefully reducing either likelihood and/or impacts of the risks. Explain what needs to happen and when. Provide justification for the proposed plan.

| **ID** | **Proposed Treatment Plan**Documented outline of the treatment plan for each risk, explain what needs to happen and when.  | **Target Date**If a date is not known at this time, please indicate an estimated Target Date. | **Individual assigned to carry out Treatment Plan (e.g., Information Custodian)** |
| --- | --- | --- | --- |
|
| R1 | <**e.g**., *It was identified that there were 10 user accounts that were using weak and noncompliant passwords in the software.**A treatment plan has been created, the Administrator for the software will work with the Individuals assigned to carry out the treatment plan to ensure that the passwords are compliant to the organization’s standards for each user account.* *The Administrator will send a Password reset request with instructions to ensure each user to ensure they will be able to reset their passwords to* ***password standard (if it exists)*** *and understand the importance of using secure complex passwords.* *The estimated time to complete this will be 2 – 3 weeks.**After the time to completion has expired an audit will be conducted to ensure that passwords have been changed to organization compliant passwords. If not, the Administrator will send another password rest request to the noncompliant accounts*. > | <*Year, Month* >  | <*Name* >  |
| R2 | <**e.g**., *Users of the system have not been trained in Information Management protocols and disclosure of information for the system in use in the department.**The Individual assigned to carry out the treatment plan will ensure users of the system have taken the Information Management training modules.**In addition, each user of the system will be trained on the disclosure of the information in use with the system as well as the acceptable use policies for information in use with the system and its users. This will take approximately 1-2 months to complete*.> | <*Year, Month* > | <*Name* >  |

| **ID** | **Residual Risk Assessment**Provide a summary risk assessment after treatment for each risk, including the likelihood and potential impacts of the risk and an explanation thereof. Use business terms to ensure the information controller understands residual risks. Use numbers, but ensure that when describing risks or exposure, you also use the words: 1-2=Very Low, 4-6=Low, 8-12=Medium, 15-16=High, 20-25=Critical | **P** | **I** | **Residual Exposure**E=PxI |
| --- | --- | --- | --- | --- |
| R1 | <**e.g.,** *Once the passwords for all 10 Accounts have been reset to Compliant complex passwords. The likelihood of a breach due to brute force attacks to guess the password will drop. probability. The impact will not change. This will result to a LOW risk*.> | <e.g, 1> | <e.g., 4> | <e.g., 4> |
| R2 | <**e.g**., *Once all users of the system have taken the Noverant Information Management modules and have been trained in Information disclosure and acceptable use policies for the system it is estimated that the probability will drop. This will result to a LOW risk*.> | ? | ? | <e.g., 4> |

5.2 Risk Treatment Plans

*<****Information custodians****. Information custodians are responsible for implementing the maintenance, risk management, and security of systems and applications to align with the business requirements as identified by the information controllers.>*

Information Custodian Signature

As Information Custodian, I acknowledge the treatment plan(s) identified and my or my team’s responsibility for implementation of these technical mitigations. .

Digital Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

6.0 Reviews and Approvals

Process: Upon final review of the document:

1. Creator of STRA must forward the completed STRA to their organization’s Cybersecurity Governance, Risk, and Compliance through the organization set procedure/process, requesting a review of the document.
2. Cybersecurity Governance, Risk, and Compliance will review and provide feedback to the creator of the STRA.
3. The creator of the STRA could convert the final document to a PDF and add electronic signature boxes below (add more approval lines if required).
4. The creator of STRA will then proceed with obtaining electronic approval from the Information Controller or designated risk owner.
5. Once the form is signed and returned by the Information Controller, the STRA creator may forward the signed PDF to Cybersecurity Governance, Risk, and Compliance requesting closure and the official recording of risks, if any.
6. Cybersecurity Governance, Risk, and Compliance would proceed with a final review of the form, signing the form to confirm compliance to processes, storing the STRA in the organization’s risk register, and recording pertinent risks into the register.

Note: This may be tailored to the organization’s review and approval process in place.

Information Controller Signature

The Information Controller or delegate (Service/Risk Owner) has reviewed this assessment and signs below to confirm that they understand the documented risks with their chosen treatment options. In addition, as Information Controller, I accept the proposed treatment plan/s and residual risks as documented in section 5, statement of acceptable risk.

Digital Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[Cybersecurity authorized personnel] Signature

[Cybersecurity] has reviewed this assessment and confirms that due diligence was used in its completion. Please note that [Cybersecurity] does not sign off risks.

Digital Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\*\*Note rename [Cybersecurity] to name of unit responsible for risk in your organization

Appendix A: Risk Assessment Considerations

| **#** | **Control Questions** | **Yes/No** | **Notes** |
| --- | --- | --- | --- |
| **1** | Is there a technical design document for this application? | [ ]  Yes [ ]  No  |  |
| **2** | Is the information contained in the defuncted Statement of Sensitivity or previous Security Threat Risk Assessment, accurate, current and signed off by the information controller? | [ ]  Yes [ ]  No  |  |
| **3** | Is this application subject to any ongoing audit, review or vulnerability assessment? | [ ]  Yes [ ]  No  |  |
| **4** | Are users made aware of acceptable use policies for this application? | [ ]  Yes [ ]  No  |  |
| **5** | Are controls in place to detect and/or prevent inappropriate use of this application? (e.g., Read Access Logging) | [ ]  Yes [ ]  No  |  |
| **6** | Is the environment where the application is hosted subject to ongoing security updates, monitoring and maintenance? | [ ]  Yes [ ]  No  |  |
| **7** | Is the application subject to ongoing security updates and maintenance and vendor support for maintenance? (e.g., is the application version current, is the vendor actively issuing any updates, if there are third party notices of vulnerabilities are these corrected by the vendor?) | [ ]  Yes [ ]  No  |  |
| **8** | Was the default (out of the box) configuration for this application reviewed and updated? | [ ]  Yes [ ]  No  |  |
| **9** | Is the organization made aware of planned changes or enhancements to this application and has a process in place to assess the impact? | [ ]  Yes [ ]  No  |  |
| **10** | Are there controls in place to preserve the integrity of financial transactions (e.g., to detect or prevent fraudulent financial transactions, theft or duplicate payments)? | [ ]  Yes [ ]  No  |  |
| **11** | Is access to this application exclusively using organization’s approved authentication services (e.g., Active Directory accounts)? | [ ]  Yes [ ]  No  |  |
| **12** | Is multi-factor authentication enabled for all access to this application? | [ ]  Yes [ ]  No  |  |
| **13** | Is there a process to approve access to this application, review access and terminate access to users that are no longer authorized for access? | [ ]  Yes [ ]  No  |  |
| **14** | Is access to this application segregated by security roles? | [ ]  Yes [ ]  No  |  |
| **15** | Is access to reports or queries restricted to authorized users? | [ ]  Yes [ ]  No  |  |
| **16** | Are there processes in place to manage and safeguard data exported from this application (e.g., results of queries)? | [ ]  Yes [ ]  No  |  |
| **17** | Are controls in place to preserve integrity and security of integrations between this application and other organization Applications or devices? | [ ]  Yes [ ]  No  |  |
| **18** | Are controls in place to preserve integrity and security of integrations between this application and third-party applications or Internet-of-Things devices? | [ ]  Yes [ ]  No  |  |
| **19** | Are controls in place to validate the integrity of data added through a mass upload? | [ ]  Yes [ ]  No  |  |
| **20** | Are controls in place to manage any dependencies on any organization Applications? | [ ]  Yes [ ]  No  |  |
| **21** | Are controls in place to manage any dependencies on third-party applications (e.g., current version of Google Chrome) | [ ]  Yes [ ]  No  |  |
| **22** | Are controls in place to manage any dependencies on any third-party services (e.g., Google Maps or Natural Language Processing)? | [ ]  Yes [ ]  No  |  |
| **23** | Are controls in place to manage how/whether third party applications request access to this application's data? (e.g., through federated user access, mobile applications, advertising services) | [ ]  Yes [ ]  No  |  |
| **24** | Are controls in place to manage how/whether this application can access to data on a user's device (e.g., location information, contacts)? | [ ]  Yes [ ]  No  |  |
| **25** | Are there controls in place to detect or prevent unauthorized or accidental destruction of data? | [ ]  Yes [ ]  No  |  |
| **26** | Is data used to test this application protected with appropriate security controls (e.g., non-sensitive data is used for testing, data is scrambled, security controls in test are identical to production) | [ ]  Yes [ ]  No  |  |
| **27** | Is data encrypted in transit and at rest using current industry standard encryption methods? | [ ]  Yes [ ]  No  |  |
| **28** | Does the organization have control over all keys used to encrypt data in this application? | [ ]  Yes [ ]  No  |  |
| **29** | Does this application enable users to store or copy data outside of the organization’s environment? | [ ]  Yes [ ]  No  |  |
| **30** | Have there been any security or privacy incidents involving loss of confidentiality, integrity or availability in this application during the past year? | [ ]  Yes [ ]  No  |  |

Glossary of Terms

**Information Controller -** have the responsibility and decision-making authority for information throughout its life cycle, including creating, classifying, restricting, regulating and administering its use or disclosure.

Department Heads are responsible for assigning Information Controllers to Information Assets and IT Systems.

Information Controllers are responsible for accepting risks and treatment plans for their systems.

Any residual risks after the risk treatment process must be documented, managed and approved by the Information Controller.

Information Controllers document risks (and residual risks) along with existing and proposed mitigations using the Statement of Acceptable Risk (SoAR).

Information Controllersare responsible for ensuring that security risks to IT systems needed to support programs and services are assessed and understood.

The Information Controllers (or delegates) will, in most cases, engage/consult a security practitioner from the organization’s cybersecurity unit responsible for risk to coordinate and facilitate the IT security risk assessment.

Information Controllers are responsible for most of the risk management phases, such as Risk Context, Risk Assessment and Risk Treatment phases, which includes ensuring that a Security Threats and Risks Assessment (STRA) is performed when required as per the organization’s directive.

The Information Controller should be prepared to “sign-off” the security assessment as acknowledgement of the identified risks.

Information Controllers (or delegates) are responsible for updating risks statuses and mitigation progresses as recorded inside the Risk Register

To assist in monitoring their risks, the information controller is notified with an automated email message listing the risks that the information controller will need to provide a status update.

**Information custodians** are responsible for implementing the maintenance, risk management, and security of systems and/or applications to align with the organization’s information management policy instruments and the business requirements identified by the information controller(s).

**Risk** - the unwanted “effect of uncertainty on objectives” and is constantly present in the environment. A risk, in plain language, is a chance of something bad happening combined with how bad it would be if it did happen.

**Vulnerability** - A weakness in people, process or technology, as well as physical aspects in an environment, which could be exploited by one or more threats.

**Threat** - A threat is anything that is capable, by its action or inaction, of causing harm to an information asset and exploits a vulnerability in the environment.

**Risk Treatment** - An “Action Plan” in which you need to specify which security controls you need to implement, who is responsible for them, what the deadlines will be, and which resources (i.e., Financial and human) are required.

The risk treatment options are Avoid, Reduce, Transfer and Accept. Please contact your organization’s cybersecurity unit responsible for risk for additional assistance and guidance with these options.

**Avoid** - stop performing certain tasks or processes if they incur such risks that are simply too big to mitigate with any other options.

**Reduce** - implementation of safeguards (controls) to decrease the severity of the risk.

**Transfer** - transfer the risk to another party, e.g.) you buy an insurance policy for your building against fire.

**Accept** – to allow the risk to exist or occur without doing anything about it.