# Information Security Risk Management
# K-12 Primer

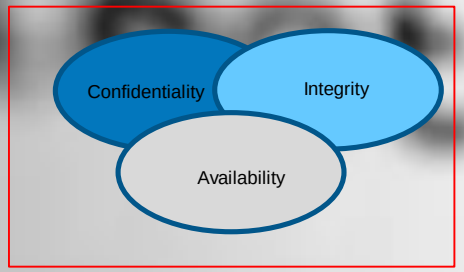
Scott Stansbury- *Director, Technology Infrastructure, Round Rock ISD*

Clarence Campbell- *Information Security Officer, Round Rock ISD*

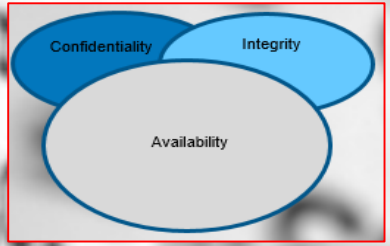
**February 18, 2021**

# Information Security Risk Management

- Information Security can be viewed as the “umbrella” that all of an Organization’s data in any form falls under, e.g. written or electronic.
- Cybersecurity is securing an Organization’s electronic data in cyberspace which belongs to the Information Security umbrella.
- It is almost impossible to completely protect all data, whether written or electronic from the risk of compromise and maintain efficient availability of data and Information Systems
- Therefore, Information Security Risk Management is an absolute must for organizations and business areas to identify and manage the risks of their data being compromised.
- Risk Management can be viewed as the cornerstone of an Information Security Program







# Information Security Risk Management

- **What is Risk Management and how do we apply Risk Management to our InfoSec program ?**
- **Texas Administrative Code 202- Risk Management Defined**
  - The process of aligning information resources risk exposure with the organization's risk tolerance by either accepting, transferring, or mitigating risk exposures.
    - What does this mean and how do we apply this ?
- **Risk Management begins with identification of risk, ranking severity of risk, then planning to address the identified risks.**
  - How do we do this ?
- **Methods of identifying risk**
  - Security Controls Assessment - more compliance based
  - Texas Cybersecurity Framework- more compliance and InfoSec Program maturity based
  - Risk Assessment- more risk and quantification of risk focused *(determination of risk severity)*
  - Continuous Monitoring- Risk is part of InfoSec, new risks will be discovered, determine severity and add them to the Risk Management Tracking solution

# Compliance Requirements

## ❑ Texas Association of School Boards (TASB)

- **TECHNOLOGY RESOURCES CQB CYBERSECURITY (LEGAL), DATE ISSUED: 9/17/2019 UPDATE 114 CQB(LEGAL)-P, CYBERSECURITY POLICY**

  Each district shall **adopt** a cybersecurity policy to:
  1. Secure district cyberinfrastructure against cyber attacks and other cybersecurity incidents; and
  2. Determine cybersecurity risk and implement mitigation planning.

  A district's cybersecurity policy may not conflict with the information security standards for institutions of higher education adopted by the Department of Information Resources (DIR) under Government Code Chapters 2054 and 2059.

## ❑ Texas Department of Information Resources (DIR) Security Standards for Institutions of Higher Education

- **Texas Administrative Code (TAC) 202 Control Standards**

  Establishes a baseline of security standards for Texas state agencies and institutions of higher education, TAC 202 Subchapter C addresses institutions of higher education.

  TAC 202, Subchapter C, 202.76, Security Controls Standards Catalog

  (a) Mandatory Requirements. Mandatory security controls shall be defined by the department in a Control Standards document published on the department's website.

# TX DIR Security Controls Catalog

- **TX DIR Security Controls Catalog, RA-3 Risk Assessment**

  - CONTROL DESCRIPTION The organization:

    - a. Conducts an assessment of risk, **including the likelihood and magnitude of harm**, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;

    - b. Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]];

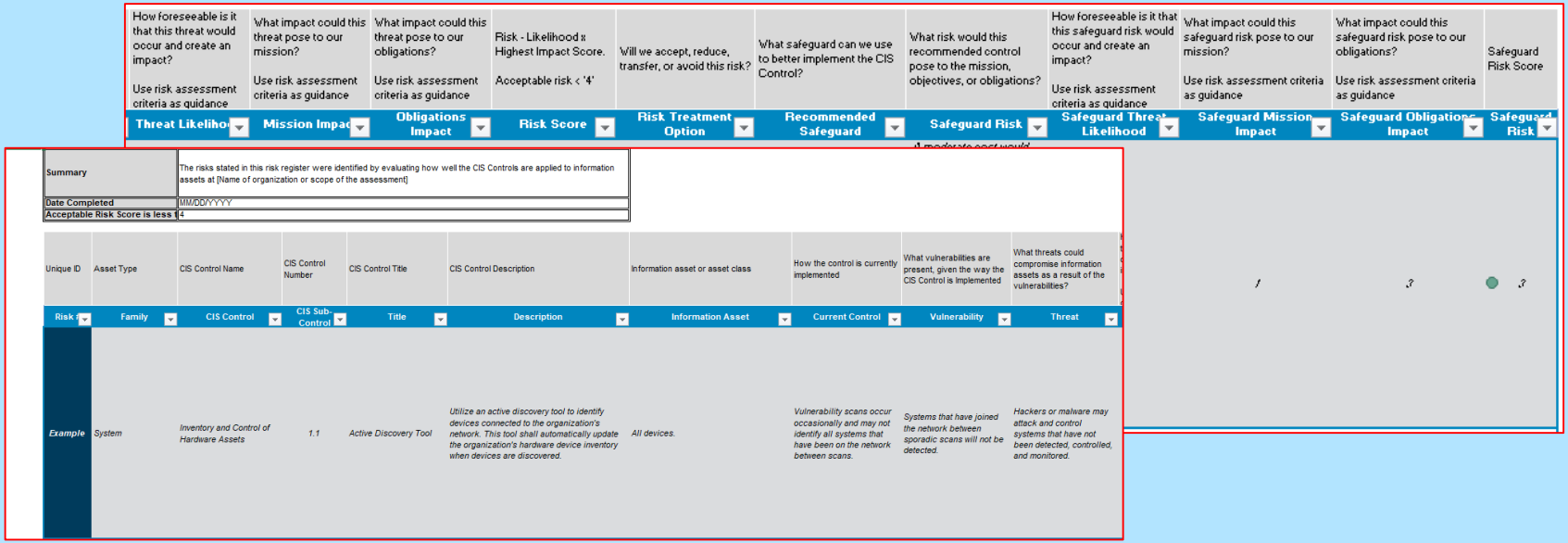
    - c. Reviews risk assessment results [Assignment: organization-defined frequency];

    - d. Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and

    - e. Updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

# Risk Assessment Plan

- **Risk Assessment Plan**
- **Leadership Buy-in**
- **Center for Internet Security Risk Assessment Method- Workbook**
  - The workbook can be tailored- e.g. compare to TX DIR Controls catalog and TX CSF- Add TX Dir and TX CSF Controls
  - Create a Hybrid workbook with the NIST CSF-CISRAM Mapped xlsx Document, may want to include mapping to DIR Security Controls and TX CSF
  - Remember- identifying and determining risk severity is the objective



| How foreseeable is it that this threat would occur and create an impact?<br><br>Use risk assessment criteria as guidance | What impact could this threat pose to our mission?<br><br>Use risk assessment criteria as guidance | What impact could this threat pose to our obligations?<br><br>Use risk assessment criteria as guidance | Risk - Likelihood x Highest Impact Score.<br><br>Acceptable risk < '4' | Will we accept, reduce, transfer, or avoid this risk? | What safeguard can we use to better implement the CIS Control? | What risk would this recommended control pose to the mission, objectives, or obligations? | How foreseeable is it that this safeguard risk would occur and create an impact?<br><br>Use risk assessment criteria as guidance | What impact could this safeguard risk pose to our mission?<br><br>Use risk assessment criteria as guidance | What impact could this safeguard risk pose to our obligations?<br><br>Use risk assessment criteria as guidance | Safeguard Risk Score |
|---|---|---|---|---|---|---|---|---|---|---|
| Threat Likelihoo | Mission Impac | Obligations Impact | Risk Score | Risk Treatment Option | Recommended Safeguard | Safeguard Risk | Safeguard Threat Likelihood | Safeguard Mission Impact | Safeguard Obligations Impact | Safeguard Risk |

| | |
|---|---|
| Summary | The risks stated in this risk register were identified by evaluating how well the CIS Controls are applied to information assets at [Name of organization or scope of the assessment] |
| Date Completed | MM/DD/YYYY |
| Acceptable Risk Score is less t | 4 |

| Unique ID | Asset Type | CIS Control Name | CIS Control Number | CIS Control Title | CIS Control Description | Information asset or asset class | How the control is currently implemented | What vulnerabilities are present, given the way the CIS Control is implemented | What threats could compromise information assets as a result of the vulnerabilities? |
|---|---|---|---|---|---|---|---|---|---|
| Risk # | Family | CIS Control | CIS Sub-Control | Title | Description | Information Asset | Current Control | Vulnerability | Threat |
| *Example* | *System* | *Inventory and Control of Hardware Assets* | *1.1* | *Active Discovery Tool* | *Utilize an active discovery tool to identify devices connected to the organization's network. This tool shall automatically update the organization's hardware device inventory when devices are discovered.* | *All devices.* | *Vulnerability scans occur occasionally and may not identify all systems that have been on the network between scans.* | *Systems that have joined the network between sporadic scans will not be detected.* | *Hackers or malware may attack and control systems that have not been detected, controlled, and monitored.* |

# Risk Severity
# Determining Likelihood and Magnitude of Harm

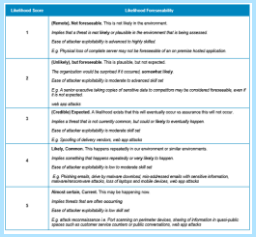
- **CENTER FOR INTERNET SECURITY RISK ASSESSMENT METHOD (CISRAM)**

| Likelihood Score | Likelihood Foreseeability |
|---|---|
| 1 | **(Remote), Not foreseeable.** This is not likely in the environment.<br>*Implies that a threat is **not likely** or plausible in the environment that is being assessed.*<br>*Ease of attacker exploitability is advanced to highly skilled.*<br>*E.g. Physical loss of complete server may not be foreseeable of an on premise hosted application.* |
| 2 | **(Unlikely), but foreseeable.** This is plausible, but not expected.<br>*The organization would be surprised if it occurred, **somewhat likely**.*<br>*Ease of attacker exploitability is moderate to advanced skill set*<br>*E.g. A senior executive taking copies of sensitive data to competitors may be considered foreseeable, even if it is not expected.*<br>*web app attacks* |
| 3 | **(Credible) Expected.** A likelihood exists that this will eventually occur vs assurance this will not occur.<br>*Implies a threat that is not currently common, but could or **likely** to eventually happen.*<br>*Ease of attacker exploitability is moderate skill set*<br>*E.g. Spoofing of delivery vendors, web app attacks* |
| 4 | **Likely, Common.** This happens repeatedly in our environment or similar environments.<br>*Implies something that happens repeatedly or **very likely** to happen.*<br>*Ease of attacker exploitability is low to moderate skill set*<br>*E.g. Phishing emails, drive by malware download, mis-addressed emails with sensitive information, malware/ransomware attacks, loss of laptops and mobile devices, web app attacks* |
| 5 | **Almost certain, Current.** This may be happening now.<br>*Implies threats that are often occurring*<br>*Ease of attacker exploitability is low skill set*<br>*E.g. attack reconnaissance i.e. Port scanning on perimeter devices, sharing of information in quasi-public spaces such as customer service counters or public conversations, web app attacks* |

| Impact Score | Impact to Our Mission | Impact to Objectives | Impact to Obligations |
|---|---|---|---|
| | *Ability to sustain <org name > business and education operations that depend on IS and IS components* | *Interruption of Business and Education services* | *Maintain confidentiality and or integrity of personal, confidential, or <org name > sensitive information* |
| 1. Negligible<br>*No impact, Insignificant* | *<org name > staff and students continue to have full access to IS and services* | *No interruption of IS or services availability* | *No breach or compromise of staff /student/ <org name > data* |
| 2. Acceptable<br>*Minor Impact* | *The majority (over 90%) of <org name > staff and students continue to have access to IS and services* | *The majority (over 90%) of <ORG NAME > staff and students continue to have access to IS and services*<br>*Or*<br>*Does not include an entire campus*<br>*Does not include an entire department*<br>*Or*<br>*Minimal effect: the organization can still provide all priority or critical business impact services but has lost some efficiency.* | *No breach or compromise of staff /student/ <ORG NAME > data* |
| 3. Unacceptable<br>*Moderate Impact* | *Only 75-89% of <ORG NA staff and students continu access to IS and services* | *50- 69% of <ORG NAME > staff and students continue to have access to IS and services*<br>*Or*<br>*The organization has lost the ability to provide a Major Business Impact service to a department(s) or campus(s).* | |
| 4. High<br>*Major Impact* | *50- 69% of <ORG NAME > staff and students continue to have access to IS and services* | *Or*<br>*The organization has lost the ability to provide a service to a Major Business Impact Information System or subset of system users for that system.* | *Breach or compromise of staff /student confidential data, <ORG NAME > sensitive data*<br>*Exceeds x number of records* |
| 5. Catastrophic<br>*Critical Impact* | *Less than 50% of <ORG NAME > staff and students continue to have access to IS and services* | *Information System(s) that protects human life or safety*<br>*Or*<br>*Less than 50% of <ORG NAME > staff and students continue to have access to Information Systems and services*<br>*Or*<br>*The organization is no longer able to provide Critical Business Impact services to department(s) or campus(s).* | *Breach or compromise of staff /student confidential data, <ORG NAME > sensitive data*<br>*Exceeds x number of records* |

# Risk Severity
# Determining Likelihood and Magnitude (Impact) of Harm

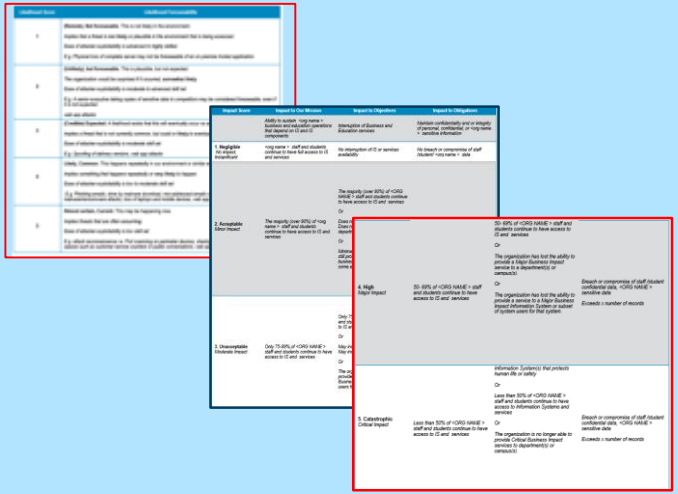
- **CENTER FOR INTERNET SECURITY RISK ASSESSMENT METHOD (CISRAM)**



| Impact Score | Impact to Our Mission | Impact to Objectives | Impact to Obligations |
|---|---|---|---|
| | *Ability to sustain <org name > business and education operations that depend on IS and IS components* | *Interruption of Business and Education services* | *Maintain confidentiality and or integrity of personal, confi > sensitive infor* |
| **1. Negligible** *No impact, Insignificant* | *<org name > staff and students continue to have full access to IS and services* | *No interruption of IS or services availability* | *No breach or cor /student/ <org na* |
| **2. Acceptable** *Minor Impact* | *The majority (over 90%) of <org name > staff and students continue to have access to IS and services* | *The majority (over 90%) of <ORG NAME > staff and students continue to have access to IS and services*<br>*Or*<br>*Does not include an entire campus Does not include an entire department*<br>*Or*<br>*Minimal effect; the organization can still provide all priority or critical business impact services but has lost some efficiency.* | *No breach or cor /student/ <ORG* |
| **3. Unacceptable** *Moderate Impact* | *Only 75-89%,of <ORG NAME > staff and students continue to have access to IS and services* | *Only 75-89% of <ORG NAME > staff and students continue to have access to IS and services*<br>*Or*<br>*May include an entire department May include an entire campus*<br>*Or*<br>*The organization has lost the ability to provide a service to a Moderate Business Impact system or subset of users for that Information System.* | *Breach or compr personal data, <* *sensitive data*<br>*~Limited to x rec* |
| **4. High** *Major Impact* | *50- 69% of <ORG NAME > staff and students continue to have access to IS and services* | *50- 69% of <ORG NAME > staff and students continue to have access to IS and services*<br>*Or*<br>*The organization has lost the ability to provide a Major Business Impact service to a department(s) or campus(s).*<br>*Or*<br>*The organization has lost the ability to provide a service to a Major Business Impact Information System or subset of system users for that system.* | *Breach or compromise of staff /student confidential data, <ORG NAME > sensitive data*<br>*Exceeds x number of records* |
| **5. Catastrophic** *Critical Impact* | *Less than 50% of <ORG NAME > staff and students continue to have access to IS and services* | *Information System(s) that protects human life or safety*<br>*Or*<br>*Less than 50% of <ORG NAME > staff and students continue to have access to Information Systems and services*<br>*Or*<br>*The organization is no longer able to provide Critical Business Impact services to department(s) or campus(s).* | *Breach or compromise of staff /student confidential data, <ORG NAME > sensitive data*<br>*Exceeds x number of records* |

# Risk Severity
## Determining Likelihood and Magnitude (Impact) of Harm

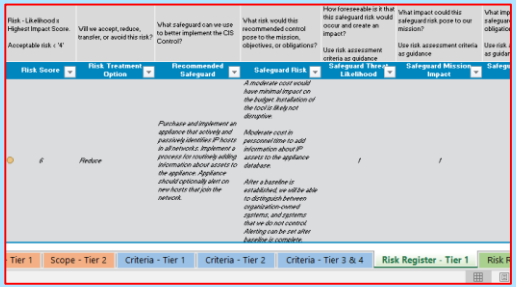
- **CENTER FOR INTERNET SECURITY RISK ASSESSMENT METHOD (CISRAM)**



| Risk Scoring | Risk Severity |
|---|---|
| Likelihood x Impact = | 9 or less = Low |
| Likelihood x Impact = | 10-14 = Mod |
| Likelihood x Impact = | 15-20 = High |
| Likelihood x Impact = | 21 and higher = Very High |

# Tracking, Prioritizing & Managing Risk

- **Governance, Risk, Compliance (GRC) Application**
- **Risk Register- CISRAM Workbook Tab**




- **Prioritize risk remediation/mitigation efforts based on severity rating and current threat landscape, e.g. Top Twelve**
- **Review risks to determine**
  - **Risk Remediation**
  - **Risk Mitigation**
  - **Risk Transference (Cannot transfer responsibility)**
  - **Risk Acceptance**
  - **Risk Avoidance**
    - **Reference TAC 202 For Higher Education**

(4) Approval of the security risk acceptance, transference, or mitigation decisions shall be the responsibility of:

(A) the information security officer or his or her designee(s), in coordination with the information owner, for systems identified with Low or Moderate residual risk.

(B) The state institution of higher education head for all systems identified with a residual High Risk.

# Information Technology and InfoSec Partnership to Address Risk

- **Risk based approach for remediation/mitigation of risk findings**
  - **Project Prioritization**
  - **Budget Allocation**
  - **Resource Allocation**
- **Collaboration is key**
  - **Discovery**
  - **Planning**
  - **Implementation**
  - **Monitoring**
- **Documenting processes, establishing technology policy**
  - **Establish central repository for all documentation**
  - **Include Information Security with proposed changes and technology**

# References

- **TX DIR**
  **TX DIR TAC 202 Control Standards and Security Controls Catalog**
  **https://dir.texas.gov/View-About-DIR/Information-Security/Pages/Content.aspx?id=2**

- **TEA TX Secure Gateway**
  **https://www.texasgateway.org/resource/cybersecurity-tips-and-tools**

- **TX TEA Cybersecurity Coordinator Forum**
  **https://attendee.gotowebinar.com/register/8234183618339320587**

- **Texas Association of School Boards (TASB)**
  **https://www.tasb.org/services/legal-services/tasb-school-law-esource/business/documents/school-cybersecurity-texas-requirements.pdf**

- **TX ISAO**
  **https://dir.texas.gov/View-About-DIR/Information-Security/request-list-access.html**

- **MS-ISAC**
  **https://www.cisecurity.org/ms-isac/**

- **CENTER FOR INTERNET SECURITY (CIS) and CISRAM**
  **https://www.cisecurity.org/cybersecurity-tools/**

- **CIS Mapping to NIST CSF (TX CSF is based on NIST CSF, NIST CSF Maps to TX DIR Controls Catalog, NIST Based)**
  **https://www.cisecurity.org/white-papers/cis-controls-v7-1-mapping-to-nist-csf/**

Questions

Feedback

# Cybersecurity in Layers - Not a Single Solution