Glossary of Key Terms and Concepts in ISAAC

Administrative Controls/Countermeasures: Non-technical security measures such as developing and publishing of policies, standards, procedures, and guidelines; personnel screening and background checks; security-awareness training; and change control procedures.

Asset Value – Virtually all existing security standards and best practices require adopters to take inventory of their systems and assign value to all digital resources, but they are equally inconsistent with regard to methodology. For our purposes, we determined the relative value of the information to be High, Medium, or Low, determined as a function of the Confidentiality (C), Integrity (I), and Availability (A) ratings used elsewhere in the assessment to define System Importance.

At the start of each assessment, the subject information asset is rated according to its need for Confidentiality (C), Integrity (I), and Availability (A). The need for each is rated as High (3), Medium (2), or Low (1). The asset value is then determined as follows:

- High Value = any asset with Availability = High (3) or System Importance (C*I*A) > 17
- Moderate Value = any asset with a System Importance (C*I*A) between 6 and 17
- Low Value = any asset with a System Importance (C*I*A) less than 6

Availability: The assurance of reliable and timely access to information and resources when that access is required and requested.

- Low Need: Information is generally available from alternate, perhaps even non-university sources, or is not time sensitive. The disruption of access can be managed to prevent any significant damage to the University, department, or individuals.
- Moderate Need: People or services are hindered or inconvenienced by the unavailability. The department or University may incur significant damage and cost, but they would retain the ability to teach, perform research, and perform critical administrative functions, although perhaps in a diminished capacity.
- High Need: Unavailability of information resources would shut down operations and services. The University, department, or an individual would incur significant damage or cost resulting in financial loss, adverse legal action, loss of public confidence, or the inability to perform research, education, or critical administrative functions.

Confidentiality: The guarantee that information is disclosed only to those who are authorized to have it. The unauthorized or unintended release of confidential information can result in negative publicity for an institution, financial loss, adverse legal action, or personal embarrassment or fraud.

- Low Need: The unauthorized disclosure would not adversely affect the University or an individual. Loss can be managed to prevent any damage to the University or individuals. A low need of confidentiality usually applies to Public (Level 1) information (see definition under Confidential Information).
**Moderate Need:** The unauthorized disclosure would have an adverse affect on the University or an individual. The department or University may incur significant damage and cost, but would retain the ability to teach, perform research, and perform critical administrative functions, although perhaps in a diminished capacity. A moderate need of confidentiality might apply to Sensitive (Level 2) or Restricted/Confidential (Level 3) information (see definition under Confidential Information).

**High Need:** The unauthorized disclosure would have a severe adverse affect on the University operations, University assets or individuals. The University, department, or an individual would incur significant damage or cost resulting in financial loss, adverse legal action, loss of public confidence, or the inability to perform research, education, or critical administrative functions. PII, PHI, and PCI are all considered to be highly confidential and the presence of any one is sufficient to establish the need as high. A high need of confidentiality applies to Restricted/Confidential (Level 3) information and might apply to Sensitive (Level 2) information (see definition under Confidential Information).

**Confidential Information:**
Higher education and industry best practices suggest the need for three classes, or levels, with respect to data confidentiality. In order from least to most confidential, these are:

a. **Public (Level 1) Information**
   Public information is information that by its very nature is designed to be shared broadly, without restriction, or at the complete discretion of the owner. It may or may not have been explicitly designated as public. There is no such thing as unauthorized disclosure of this information and it may be freely disseminated without potential harm to the University, individuals, or affiliates. From the perspective of confidentiality, public information may be disclosed or published by any person at any time.
   
   Examples: advertising, degree program descriptions, course offerings and schedules, campus maps, published research (within copyright restrictions), job postings, press releases, general information about university products and services, certain types of unrestricted directory information as specified by FERPA and HIPAA, etc.

b. **Sensitive (Level 2) Information**
   Sensitive information is the most difficult to describe as it often presents attributes of both Public and Restricted/Confidential information. Sensitive information is often considered “public” in the sense that it is releasable under provisions of the Texas Public Information Act, while also requiring assurances that its release is both controlled and lawful. Sensitive information is often intended for use within a specific workgroup, department, or group of individuals with a legitimate need-to-know. Likewise, access to Sensitive information is often controlled by identity authentication and authorization.
measures (e.g., NetID and password). Unauthorized disclosure of Sensitive information could adversely impact the University, individuals, or affiliates.

Examples: Some employee records (such as performance appraisals, dates of birth, and email addresses), departmental policies and procedures that might reveal otherwise restricted information, the contents of e-mail, voicemail, instant messages, and memos, unpublished research, information covered by non-disclosure agreements, donor information, etc.

c. Restricted/Confidential (Level 3) Information
According to Chapter 202 of the Texas Administrative Code (TAC 202), Restricted/Confidential information is “information that is excepted from disclosure requirements under the provisions of applicable state or federal law” such as the Texas Public Information Act (TPIA) and the Family Education Rights and Privacy Act (FERPA). Restricted/Confidential information presents the most serious risk of harm if improperly disclosed. Restricted/Confidential information is generally intended for a very specific purpose and should not be disclosed to anyone without a demonstrated need-to-know, even within a workgroup or department. Disclosure of Restricted/Confidential information is generally regulated by specific legal statutes (e.g., TPIA, FERPA, HIPAA), published opinions by the Office of the Attorney General of Texas, Texas State University System rules, or contractual agreements. Unauthorized disclosure of this information could have a serious adverse impact on the University, individuals, or affiliates.

Examples: Student records protected under FERPA, credit card information, bank account numbers, social security numbers, driver license numbers, personally identifiable medical records, passport information, crime victim information, library transactions (e.g., circulation records), court sealed records, access control credentials (e.g., PINs and passwords), etc.

Control/Countermeasure: A device, method, technique, or procedure employed to prevent a threat agent from exploiting a vulnerability. A countermeasure is put into place to mitigate risk. See also safeguard.

Custodian: A person (or unit) responsible for management of an information resource, and for implementing owner-defined controls that regulate physical and logical access to the information resource. Example: System Administrator

DIR (The Texas Department of Information Resources): The Texas state agency vested by the Texas Information Resources Management Act of 1993 with oversight authority over the use of information resources in Texas state agencies and universities. DIR promulgates and enforces standards and rules in the Texas Administrative Code.
Effectiveness of Information Systems Protection: Normally Moderate to High for most systems. If not at least Moderate, the Information Systems are considered inadequately protected.

**Very Low:** Daily problems are encountered with Information Systems availability and/or there is little, if any, assurance of maintaining data integrity and/or data confidentiality.

**Low:** Problems with Information Systems availability are not uncommon and/or there is limited assurance of maintaining data integrity and/or confidentiality.

**Moderate:** Information Systems are normally available to support operations; and data integrity and/or confidentiality are well protected.

**High:** Information Systems are rarely unavailable and data integrity and confidentiality are well protected.

**Very High:** Information Systems availability and data integrity and confidentiality are assured. This level is normally achieved only in fully redundant, highly standardized, and heavily secured technical infrastructures.

Electronic Protected Health Information (E PHI): refers to any protected health information (PHI) that is created, received, maintained, or transmitted in electronic format.

FERPA: The common acronym for the Family Educational Rights and Privacy Act of 1974, a federal law that protects the privacy of the student education records and guarantees students’ access to their own records.

Information System Owner: The person accountable for the function supported by the information system and responsible for determining the access and processing controls necessary to protect the confidentiality, integrity, and availability of the information system. The person who holds this role is typically a department or unit head and is generally responsible for assigning a value to the information system and defining the commensurate controls necessary to protect the information system.

Integrity: Assurance that information is accurate, reliable, and protected against unauthorized, unanticipated, or unintentional modification or destruction.

**Low Need:** Unauthorized modification or destruction of data would have minimal adverse effect on the University, department, or individuals. Modifications or destruction can be managed to prevent any significant damage to the University, department, or individuals.

**Moderate Need:** Unauthorized modification or destruction of data would have a significant adverse effect on the University, department, or individuals. The department or University may incur significant damage and cost, but would retain the ability to teach, perform research, and perform critical administrative functions, although perhaps in a diminished capacity.

**High Need:** Unauthorized modification or destruction of data could result in fraud, or errors in financial or student records and processing. The University, department, or an individual would incur significant damage or cost resulting in financial loss, adverse legal
action, loss of public confidence, or the inability to perform research, education, or critical administrative functions.

**Mission Critical:** An information system or asset that is defined by the University or information resource owner as essential for proper and continuous operation of the University or owner’s business function. Loss of access would result in more than an inconvenience. An event causing the unavailability of mission critical information would result in consequences such as significant financial loss, public embarrassment for the institution, failure to comply with regulations or legal obligations, or closure of the university or department. Data is considered Mission Critical if its loss may have significant negative impact on the owner’s ability to teach, conduct research, or provide essential service; or if its loss results in significant risk to the lives, health, or financial well being of students, faculty, staff, or the community. Data is not Mission Critical if its loss only presents an inconvenience to any or all of those parties.

- If a department’s ability to teach, conduct research, or provide essential services would be lost if access to the information were lost, then the department probably owns and maintains mission critical data.
- If a department’s loss of access to the information could be adequately addressed by alternate or manual processes (e.g. paper and phone), then the department probably does not "own and maintain" mission critical data.

**Owner:** The person responsible for a university function and accountable for the information resources used by that function. Owners are responsible for defining the controls that regulate physical and logical access to the information resource. Examples: Dean, Director, Dept Chair

**PCI - Payment Cardholder Information:** An individual’s first name or initial and last name, in combination with a financial account number, credit card number, or debit card number, and any security code, access code, PIN, password, or similarly confidential credential that would permit access to the individual’s account.

**PHI - Protected Health Information:** Any information created or received by a health care provider, health plan, public health authority, employer, insurer, school or university, or health care clearinghouse that relates to the past, present, or future physical or mental health or condition of an identifiable individual; to the provision of health care to an identifiable individual; or to the payment for the provision of health care to an identifiable individual.

**PII - Personal Identifying Information:** An individual’s first name or initial and last name, in combination with any one or more of the following items:

- Social Security Number
- Taxpayer ID Number
- Driver License Number

**Physical Controls/Countermeasures:** Measures designed to protect personnel, hardware, programs, networks, and data from physical circumstances and events that could cause serious
losses or damage. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism. Examples include: data center ingress and egress restrictions, magnetic media (e.g., tape, disk, removable devices) distribution and storage controls, fire prevention and detection systems, and environmental monitoring systems.

**Risk:** The probability and impact of a vulnerability being exploited. To provide for comparative risk analysis, risk is often depicted as the probability of exploitation times the impact of an occurrence \( R = P \times I \).

**Safeguard:** A software configuration, hardware configuration, data configuration, or procedure that eliminates vulnerability or reduces the risk that a threat agent might exploit a vulnerability. See also control/countermeasure.

**SAO (The Texas State Auditor’s Office):** The Texas state agency charged with assessing governmental compliance with state laws, standards, and rules, including the Texas Administrative Code.

**Technical Controls/Countermeasures:** Using technical means to assure that access to information resources is restricted to persons with appropriate authorization. Examples include: Usernames with Passwords/PINs, access control lists, network intrusion prevention appliances, firewalls, and network architectures.

**Threat:** A potential that a vulnerability will be exploited by a threat agent.

**Threat agent:** A person or a thing, which acts, or has the power to execute, cause, carry, transmit, or support a threat.

**Vulnerability:** Any weakness that offers a potential avenue of attack against an information resource, including things like viruses, incorrectly-configured systems, passwords stored in plain text (unencrypted), etc.

**Vulnerability Scan:** The use of an industry-recognized methodology and toolset to identify known, unpatched, and exploitable vulnerabilities in an information system.