CSA 2372: Security Design and Information Assurance

Department of Natural and Behavioral Sciences, Computer Science Program
Computer Science-INTL
Fall 2026 (16-week term)

Meeting Days / Time: Monday and Wednesday, 2:00 PM - 3:15 PM Location: Amy St. Building, Rio Grande College, Room 0A116 Section: 001 CRN: 12130 Modality: Face-to-face

Faculty Information

Dr. Mainuddin Shaik

Email: mainuddin.shaik@sulross.edu

Office Hours: Email to schedule an appointment (in person or via Teams)

Response time: I reply to email within one business day. Please use your Sul Ross email and put “CSA 2372” in the subject line.

Course Description

This course introduces the principles and practices used to design, govern, and assure secure information systems. Students identify assets and security objectives, analyze threats and vulnerabilities, rate and treat risk, select and justify administrative, technical, and physical controls, evaluate conceptual security architectures, and examine policy, privacy, legal, ethical, continuity, and incident-governance questions. A single fictional organization, introduced in the first week and detailed in scenario packets, runs the length of the semester, and students build one cumulative body of work about it, ending in a briefing they deliver and defend. By the end of the semester, students will:

- Analyze an organization’s assets, boundaries, data flows, dependencies, and risks.
- Select and justify proportionate security controls under real budget and staffing constraints.
- Draft governance and policy language that assigns responsibility and can actually be implemented.
- Build and defend an evidence-based security assurance argument to a non-technical audience.

Prerequisite: CSA 1309 Computer Science I.

CSA 2372 requires CSA 1309 for systems literacy, not for programming skill. Students who have written and debugged programs understand what a file, a process, a function boundary, and a network call actually are, and every discussion of system boundaries, trust boundaries, and data flows in this course assumes that understanding. The two claims are separate: the prerequisite is about what you already know, not about what you will be asked to do here.

Programming and tools: None required. CSA 2372 has no programming assignments, no virtual machines, no command-line work, no system configuration, and no hands-on security tooling.

Scope of the Course

This course is deliberately lab-free. It does not use packet capture, virtual machines, vulnerability scanners, SIEM platforms, or penetration-testing tools. That is a design choice, not a limitation of resources. The attention this

course has is spent on reasoning, governance, architecture, risk, policy, and assurance, because those are the things a security decision actually turns on and the things a lab exercise cannot teach.

What this course does not do: prepare you for Security+ or any certification exam; teach quantitative risk analysis; teach control-by-control assessment procedures; teach penetration testing; or claim to make you job-ready as a security operator.

What this course does do: build judgment under constraint, and the ability to explain and defend a security decision to someone who does not work in security.

Course Materials

Textbook: None required, and none recommended. This course runs on freely available public material and on scenario packets I write.

Required readings:

- NIST Cybersecurity Framework 2.0 and the NIST CSF 2.0 Quick Start Guides (free, https://www.nist.gov/cyberframework).
- CIS Controls v8, linked to the official CIS source (https://www.cisecurity.org/controls/v8). Access is free but requires registration with CIS.
- Selected CISA guidance, including the Cybersecurity Performance Goals (https://www.cisa.gov/cybersecurity-performance-goals).
- Instructor-authored scenario packets, posted on Blackboard. These are required.

A note on paywalled standards: ISO/IEC 27001:2022 is not free and cannot be posted. It appears in this course only through material I write about it. Nothing you are graded on requires you to read the standard itself. The same applies to any other paid standard that comes up.

Software and tools:

- Blackboard Ultra for announcements, materials, submissions, discussions, and portfolio feedback.
- A browser, a word processor, and some way to produce a readable diagram or a structured table. Google Drawings, Google Slides, diagrams.net, PowerPoint, and Word shapes are all fine. So is a labeled text outline, which is a fully acceptable substitute for a picture in every assignment in this course.
- Nothing needs to be installed. There are no administrator rights required, no paid subscriptions, and no specialized hardware.

Important Dates (Fall 2026)

- Mon Aug 24: First day of classes
- Mon Sep 7: Labor Day, no classes
- Wed Sep 9: Twelfth class day (census); last day to drop without an academic record
- Fri Nov 6: Last day to withdraw with a grade of W (4:00 PM, Registrar’s Office)
- Mon Nov 23: Tabletop exercise, in class
- Wed Nov 25 to Fri Nov 27: Thanksgiving holiday, no classes
- Mon Nov 30: Final assurance briefings begin, in class
- Wed Dec 2: Last class day; final briefings continue

- Thu Dec 3: Dead day
- Fri Dec 4, Mon Dec 7 to Wed Dec 9: Final examination period; remaining oral defenses; final portfolio due; grades finalized

Portfolio artifact due dates go up on Blackboard in Week 1. Oral-defense slots are assigned and announced later in the semester.

Program Student Learning Outcomes

Upon completion, students will be able to:

- Define and explain fundamental concepts of computer science, including algorithms, data, abstraction, and systems.
- Identify and evaluate strategies for solving problems computationally.
- Analyze the security, privacy, and reliability implications of computing systems and the data they hold.
- Reason about the ethical, legal, and professional responsibilities that attach to computing work.
- Apply critical thinking to computational problems, systems, and case studies under real-world constraints.
- Communicate technical reasoning, and its limitations, to both technical and non-technical audiences.

Course Student Learning Outcomes

Upon successful completion of this course, students will be able to:

1. Define and distinguish asset, security objective, threat, vulnerability, exploit, control, likelihood, impact, risk, risk treatment, and residual risk in an organizational context.
2. Analyze a system boundary, trust boundary, data flow, stakeholder set, and dependency chain to identify security-relevant conditions.
3. Construct and justify a qualitative risk register that states likelihood, impact, risk treatment, control rationale, risk owner, and residual risk.
4. Apply security design principles to select proportionate administrative, technical, and physical controls under stated operational and budget constraints.
5. Evaluate a conceptual security architecture involving identity, access control, segmentation, remote access, cloud services, vendors, and supply-chain dependencies.
6. Draft and revise an implementable policy or procedure that assigns responsibility and addresses governance, privacy, ethical, legal, and regulatory considerations.
7. Use NIST Cybersecurity Framework 2.0 and CIS Controls v8 to communicate cybersecurity priorities, control choices, and assurance evidence.
8. Compare NIST SP 800-53 Rev. 5, ISO/IEC 27001:2022, FAIR, NIST CSF 2.0, and CIS Controls v8 at an introductory level, explaining what each is for, who uses it, and why an organization would choose it.
9. Participate in a tabletop exercise and defend security decisions, escalation choices, and residual-risk acceptance using evidence from your own portfolio.
10. Deliver a concise assurance briefing and answer questions about your own risk register, control choices, policy decisions, evidence, and residual risk.

Marketable Skills

Students will develop:

- **Risk Analysis and Judgment:** identifying what matters, rating uncertainty, and choosing proportionate responses under constraint.
- **Governance and Policy Literacy:** writing implementable policy, assigning accountability, and handling exceptions.
- **Framework Fluency:** using NIST CSF 2.0 and CIS Controls v8 as working vocabulary rather than as trivia.
- **Evidence and Documentation:** producing traceable records that support a decision after the fact.
- **Stakeholder Communication:** explaining a technical decision, and its limits, to people who do not work in security.

Controlled Vocabulary

These terms have fixed meanings in this course, and your written work should use them consistently. Precision here is not pedantry: most bad security arguments are bad because someone slid between two of these words without noticing.

Term	Meaning in this course
Asset	Information, system, service, person, capability, or resource that has value to an organization
Security objective	A protection goal for an asset: confidentiality, integrity, availability, authenticity, accountability, or resilience
System boundary	The defined scope of what is included in an analysis, including components, users, interfaces, services, and dependencies
Trust boundary	A point where data, authority, identity, or control crosses between parties with different trust assumptions
Data flow	The movement of data between actors, systems, services, storage locations, or trust boundaries
Threat	A potential cause of an unwanted event that could harm an asset or security objective
Vulnerability	A weakness or condition that a threat can exploit
Exploit	A method that uses a vulnerability to cause an unwanted event
Control	An administrative, technical, or physical safeguard that reduces likelihood, impact, or exposure
Risk	The potential effect of uncertainty on objectives, evaluated in this course through likelihood and impact
Risk register	The cumulative record of identified risks, ratings, treatment decisions, control

Term	Meaning in this course
	rationale, ownership, and residual risk
Risk treatment	The decision to avoid, mitigate, transfer, or accept a risk
Residual risk	The risk that remains after selected controls and treatment are applied
Security design principle	A general principle used to make a design more secure
Access-control model	A representation of who or what may access a resource, under what conditions, and with what authority
Security architecture	A conceptual arrangement of systems, services, trust boundaries, controls, and dependencies supporting security objectives
Security governance	The structures, responsibilities, decisions, policies, evidence, and oversight through which an organization directs cybersecurity risk
Policy hierarchy	The relationship among policy, standard, procedure, guideline, and exception documents
Assurance argument	A structured claim that a design is justified by risks, controls, responsibilities, evidence, limitations, and residual risk
Control effectiveness	The extent to which a control is implemented and achieves its intended risk reduction
Evidence	Information that supports a claim about a security decision, control, condition, or outcome
Tabletop exercise	A structured scenario activity in which participants document decisions, communications, escalation, and recovery priorities without operating any systems

NICE Framework Alignment

This course provides introductory exposure and early practice, not job-ready mastery, in the following NICE Framework work roles. The identifiers are useful language for résumés and job postings.

NICE work role	Identifier	What this course develops
Cybersecurity Policy and Planning	OG-WRL-004	Policy reasoning, policy hierarchy, exception analysis, accountability assignment
Security Control Assessment	OG-WRL-012	Introductory reasoning about control selection, effectiveness, evidence, and gaps
Systems Security Management	OG-WRL-014	Introductory reasoning about organizational risk, responsibility, governance, and residual-risk acceptance

NICE work role	Identifier	What this course develops
Systems Security Architecture	DD-WRL-006	Conceptual architecture analysis: trust boundaries, segmentation, identity, dependencies, controls
Systems Security Analysis	DD-WRL-007	System-boundary analysis, data-flow analysis, threat modeling, risk analysis, security requirements
Incident Response	PD-WRL-003	Incident-governance and tabletop decision-making practice

Course Assignments and Grading

Assignment Type	% of Final Grade	Description
Knowledge Checks and Scenario Annotations	10%	Short Blackboard checks on vocabulary and framework concepts, plus brief annotations applying course terms to supplied scenario facts.
Security Design Portfolio	35%	The spine of the course. Six cumulative artifacts built across the semester: asset inventory, boundary and data-flow analysis, threat model, risk register, revised risk register, and framework and assurance crosswalk. Individual.
Control and Architecture Review	15%	An access-control model, a conceptual security architecture, and a control-selection rationale, each applied to your own risk register. Individual.
Security Governance Policy Exercise	15%	A policy or procedure excerpt, its placement in the policy hierarchy, a traceability table, a structured self-audit of the draft against your own Week 7 risk register and Week 11 revised risk register, and a revision memo stating what the self-audit surfaced and what changed. Individual.
Tabletop Exercise and After-Action Review	10%	An in-class inject sequence with an individual decision log, followed by an individual after-action review.
Final Assurance Briefing and Oral Defense	15%	A four-minute briefing on your own portfolio and six minutes of questions about it. Individual.
Total	**100%**	

Grading Scale:

A: 90 to 100 B: 80 to 89 C: 70 to 79 D: 60 to 69 F: below 60

Late Assignment Statement:

Portfolio artifacts and written assignments are due by 11:59 PM on the posted due date. Late submissions are accepted up to 48 hours past the deadline with a 10% deduction per day. Work submitted more than 48 hours late will not be accepted unless prior arrangements have been made.

Late work carries an additional cost in this course that it does not carry elsewhere, and it is worth understanding why. Each artifact is the input to the next one. An asset inventory submitted three weeks late arrives after the threat model that was supposed to be built on it. The deduction is the smaller problem. Talk to me before a deadline rather than after it.

The tabletop exercise and the oral defense run in fixed windows and cannot be made up without prior arrangement.

Attendance and Participation:

Security judgment is built by arguing about cases, so much of the work of this course happens in the room. Please attend, and let me know in advance if you must miss a session. The tabletop exercise on Monday, November 23 and the oral defense are the two sessions where absence is hardest to recover from.

I also know that many of you work, commute, and carry responsibilities outside this classroom. Every major assessment in this course has an alternative path that does not require you to be physically present at a particular hour, and those paths are listed below. They cost you nothing in the grade and require no documentation.

Grading Rubrics

Security Design Portfolio (35% of grade):

Criterion	Share	Standard
Cumulative traceability	35%	Your asset inventory, threat model, risk register, revised risk register, controls, evidence, and assurance argument stay consistent with your own earlier submissions. Every material change is explained in a change memo.
Accurate security and risk analysis	25%	Correct use of the controlled vocabulary, relevant security objectives identified, plausible qualitative risk reasoning.
Proportionate decision-making	20%	Controls and risk treatment fit the organization's stated constraints, priorities, and risks. A perfect control nobody can afford is a wrong answer.
Evidence and framework use	10%	Appropriate evidence, accurate application of NIST CSF 2.0 and CIS Controls v8.
Revision quality and communication	10%	Clear writing, readable artifacts, responsiveness to feedback, documented changes.

Traceability carries the largest share deliberately. This course grades the chain of reasoning, not vocabulary density or framework name-matching.

Control and Architecture Review, Policy Exercise, and Assurance Briefing (45% combined):

Criterion	Share
Correctness of analysis (accurate reasoning about boundaries, controls, governance, and risk)	40%
Justification (tradeoffs named, rejected options explained, constraints acknowledged)	30%
Traceability to your own prior work	20%
Clarity and professional communication	10%

Oral defense protocol. You receive the question categories and the rubric in advance. There are no surprise questions. I ask three prepared questions about a risk rating, a rejected control, and one residual-risk decision, then introduce one scenario change ("the identity provider is down for eight hours," "the vendor will not provide audit evidence," "the budget drops 20%"), and you explain what changes and what does not. The authenticity comes from your own evolving portfolio, not from ambush.

Course Schedule

Scenario packets are posted on Blackboard the week before they are needed. The schedule may be adjusted; changes will be announced in class and on Blackboard.

Week	Dates	Topic	Notes: content, framework, AI connection, deliverables
1	Aug 24 - 30	Information Assurance Foundations	What information assurance is. Systems, stakeholders, assets. Confidentiality, integrity, availability, plus authenticity, accountability, and resilience. NIST CSF 2.0 introduced as a communication framework. Syllabus, scenario introduction, and the course AI policy in plain terms. AI connection: how this course will use AI output as material to check rather than as a source to trust. In class: scenario briefing and a low-stakes annotation identifying assets and security objectives. Nothing is submitted.
2	Aug 31 - Sep 6	Security Objectives and Core Vocabulary	Data classification. Threat, vulnerability, exploit, control, likelihood, impact, residual risk. NIST CSF 2.0 six Functions, with emphasis on GOVERN, which establishes direction, oversight, prioritization, and accountability. AI connection: an AI-written asset description that confuses asset with system, for you to correct. **Portfolio Artifact 1: Asset Inventory and Data Classification Rationale.**
3	Sep 7 - 13	Threat Context	Threat actors, attack paths, social engineering, ransomware, insider risk, physical and environmental threats. Distinguishing threat context from a control decision. AI connection: a fluent AI threat assessment containing one plausible but wrong attribution claim. Deliverable: scenario annotation and knowledge check. Note: Labor Day, Mon Sep 7, no classes. Wed Sep 9 is the census date.
4	Sep 14 - 20	Threat Modeling I	System boundary, trust boundary, data flow, attack surface. NIST CSF 2.0 supports communicating assets and outcomes; it is not itself a threat-modeling method. AI connection: an AI-generated data-flow description that omits a trust boundary. **Portfolio Artifact 2A: Boundary and Data-Flow Analysis.**
5	Sep 21 - 27	Threat Modeling II	Assumptions, security requirements, refinement, applied to one high-value service. AI connection: comparing an AI threat list against your own boundary analysis and identifying what it could not have known. **Portfolio Artifact 2B: Threat Model**, plus a change memo revising the asset inventory if the threat model exposed a gap.
6	Sep 28 - Oct 4	Qualitative Risk I	Likelihood, impact, rating methods, risk appetite. NIST CSF 2.0 GOVERN and IDENTIFY. AI connection: an AI risk rating delivered with false precision, for you to challenge. In class: qualitative risk analysis exercise. Nothing is submitted.
7	Oct 5 - 11	Qualitative Risk II	Risk treatment: avoid, mitigate, transfer, accept. Residual risk. Building the register. NIST CSF 2.0 GOVERN supports treatment decisions, ownership, and residual-risk acceptance. AI connection: an AI treatment recommendation that ignores a stated budget constraint. **Portfolio Artifact 3: Qualitative Risk Register and Risk-Treatment Memo.**
8	Oct 12 - 18	Security Design Principles	Least privilege, defense in depth, separation of duties, fail-safe defaults, secure defaults, zero trust as a design posture. CIS Controls v8 introduced as the control-selection layer. AI connection: an AI control recommendation that is technically sound and financially impossible for the organization. Deliverable: control-selection rationale and knowledge check.
9	Oct 19 - 25	Identity and Access	Authentication, authorization, MFA, role-based and attribute-based access control, privileged access, lifecycle management. Least privilege applied. CIS Controls v8 and CSF PROTECT. AI connection: an AI-generated role matrix that quietly grants excess privilege. **Control and Architecture Review, Part A: Access-Control Model and Change Memo.**
10	Oct 26 - Nov 1	Network and Architecture Patterns	Segmentation, DMZs, proxies, remote access, cloud and SaaS trust boundaries, dependencies. Defense in depth applied. CIS Controls v8 and CSF PROTECT and DETECT. AI connection: an AI architecture description that treats a SaaS boundary as internal. **Control and Architecture Review, Part B: Security Architecture and Control Rationale.**
11	Nov 2 - 8	Governance, Vendor Risk, and Third-Party Risk	Accountability, roles, policy hierarchy, exceptions, awareness, metrics, evidence. Vendor due diligence, supply-chain dependency. CSF GOVERN; final week of CIS Controls v8 as an active layer. AI connection: an AI vendor-risk summary that accepts a vendor's claim as evidence. **Portfolio Revision 2: Revised Risk Register and Change Memo**, plus a vendor-risk decision memo. Note: last day to withdraw with a W, Fri Nov 6.

Week	Dates	Topic	Notes: content, framework, AI connection, deliverables
12	Nov 9 - 15	Privacy, Ethics, Law, and Regulation	Data minimization, retention, disclosure, professional judgment. CSF GOVERN. AI connection: an AI-drafted policy excerpt that is fluent, well-formatted, and assigns responsibility to nobody. **Security Governance Policy Exercise:** policy excerpt, hierarchy placement, traceability table, self-audit against your own Week 7 and Week 11 risk registers, revision memo stating what the self-audit surfaced and what changed.
13	Nov 16 - 22	Framework Landscape, Assurance, and Incident Governance	Monday: the only comparative framework session. NIST SP 800-53 Rev. 5, ISO/IEC 27001:2022, and FAIR set against NIST CSF 2.0 and CIS Controls v8. What each is for, who uses it, why an organization picks it. Then assurance: evidence, control effectiveness, gaps, exceptions, monitoring, crosswalks. Wednesday: continuity and incident governance. Escalation, communication, recovery priorities, lessons learned. CSF GOVERN, RESPOND, and RECOVER. Tabletop roles and rules distributed. AI connection: an AI framework comparison containing one confident category error. **Portfolio Artifact 5: Framework and Assurance Crosswalk.**
14	Nov 23 - 24	Tabletop Exercise	The full Monday session is the tabletop, run as a timed inject sequence: ransomware, a third-party service disruption, and AI-enabled phishing. You apply your own assurance argument under time pressure and record decisions, escalation choices, and communications as you make them. CSF GOVERN, RESPOND, and RECOVER. AI connection: the phishing inject is itself AI-generated, which is the point. **Individual decision log due at the end of the session; After-Action Review due Sun Nov 29.** Note: Thanksgiving holiday Wed Nov 25 through Fri Nov 27, no classes.
15	Nov 30 - Dec 2	Final Assurance Briefings	Finalize the portfolio as one connected argument: assets, threats, risks, controls, architecture, governance, evidence, residual risk. AI connection: an AI-generated assurance briefing that is fluent and well-structured and claims the design is secure and compliant, while stating no limitations, no evidence gaps, and no residual risk. **Briefings and oral defenses run in both class sessions.** Wed Dec 2 is the last class day. Dead day Thu Dec 3.
Finals	Dec 4, 7 - 9	Remaining Briefings and Defenses	Remaining oral defenses by appointment. **Final portfolio due,** plus any post-defense correction or clarification. Grades finalized.

The AI Connection

Every week of this course includes an AI-generated artifact that is fluent, confident, correctly formatted, uses the right vocabulary, and is wrong in one specific way. Your job is to find the error.

This is not a trick and it is not an argument against using these tools. It is the argument for the entire course. A security recommendation that sounds authoritative is the normal case, not the exception, and it arrives from vendors, consultants, forum posts, colleagues, chatbots, and instructors alike. **If you cannot evaluate a security decision yourself, you cannot tell whether the one you were handed is any good.** Everything you learn this semester is a way of checking.

The errors are placed where students most often go wrong, which means that by the time you catch one, you will usually have just made the same mistake yourself. That is the design.

ADA Statement

SRSU Accessibility Services. Sul Ross State University (SRSU) is committed to equal access in compliance with the Americans with Disabilities Act of 1973. It is SRSU policy to provide reasonable accommodations to students with documented disabilities. It is the student's responsibility to initiate a request each semester for each class. Students seeking accessibility/accommodations services must contact Mrs. Mary Schwartze Grisham, LPC, SRSU's Accessibility Services Director, or Ronnie Harris, LPC, Counselor, at 432-837-8203 or email mschwartze@sulross.edu or ronnie.harris@sulross.edu. RGC students can also contact Alejandra Valdez at 830-758-5006 or email alejandra.valdez@sulross.edu. Our office is located on the first floor of Ferguson Hall, room 112, and our mailing address is P.O. Box C122, Sul Ross State University, Alpine, Texas, 79832.

Alternative Paths in This Course

Separately from formal accommodations, every major assessment has an alternative path that requires no documentation and no request:

Assessment	Alternative path
Knowledge checks and annotations	Asynchronous Blackboard window, accessible text and table formats
Portfolio artifacts	Structured text or accessible table in place of any visual-only diagram
Control and architecture review	Diagram, slides, structured text, or accessible table identifying components, boundaries, flows, and controls
Policy exercise	Standard word-processed document with heading styles
Tabletop exercise	Timed asynchronous inject sequence in Blackboard with a timestamped individual decision log, for students who cannot be present on Nov 23
Oral defense	Four-minute captioned recorded briefing, six written questions through Blackboard, one written follow-up

Choosing an alternative path costs you nothing in the grade and requires no explanation.

Student Responsibilities Statement

All full-time and part-time students are responsible for familiarizing themselves with the Student Handbook and the Undergraduate & Graduate Catalog and for abiding by the University rules and regulations. Additionally,

students are responsible for checking their Sul Ross email as an official form of communication from the university. Every student is expected to obey all federal, state, and local laws and is expected to become familiar with the requirements of such laws.

SRSU Distance Education Statement

Students enrolled in distance education courses have equal access to the university's academic support services, such as library resources, online databases, and instructional technology support. For more information about accessing these resources, visit the SRSU website.

Students should correspond using Sul Ross email accounts and submit online assignments through Blackboard, which requires a secure login. Students enrolled in distance education courses at Sul Ross are expected to adhere to all policies pertaining to academic honesty and appropriate student conduct, as described in the student handbook. Students in web-based courses must maintain appropriate equipment and software, according to the needs and requirements of the course, as outlined on the SRSU website. Directions for filing a student complaint are located in the student handbook.

Counseling

Sul Ross has partnered with TimelyCare, where all SR students have access to nine free counseling sessions. You can learn more about this 24/7/365 support by visiting TimelyCare/SRSU. The SR Counseling and Accessibility Services office will continue to offer in-person counseling in Ferguson Hall room 112 (Alpine campus), and telehealth Zoom sessions for remote students and RGC students.

Libraries

The Bryan Wildenthal Memorial Library and Archives of the Big Bend in Alpine offer FREE resources and services to the entire SRSU community. Access and borrow books, articles, and more by visiting the library's website, library.sulross.edu. Off-campus access requires logging in with your LoboID and password. Librarians are a tremendous resource for your coursework and can be reached in person, by email (srsulibrary@sulross.edu), or by phone (432-837-8123).

No matter where you are based, public libraries and many academic and special libraries welcome the general public into their spaces for study. SRSU TexShare Cardholders can access additional services and resources at various libraries across Texas. Learn more about the TexShare program by visiting library.sulross.edu/find-and-borrow/texshare/ or ask a librarian by emailing srsulibrary@sulross.edu.

Mike Fernandez, SRSU Librarian, is based in Eagle Pass (Building D-129) to offer specialized library services to students, faculty, and staff. Utilize free services such as InterLibrary Loan (ILL), ScanIt, and Direct Mail to get materials delivered to you at home or via email.

Academic Integrity

Students in this class are expected to demonstrate scholarly behavior and academic honesty in the use of intellectual property. Students should submit work that is their own and avoid the temptation to engage in behaviors that violate academic integrity, such as turning in work as original that was used in whole or part for another course and/or professor; turning in another person's work as one's own; copying from professional works or internet sites without citation; or collaborating on a course assignment, examination, or quiz when collaboration is forbidden. Use of generative AI tools is governed by the course AI policy below. Violations of

academic integrity can result in failing assignments, failing a class, and/or more serious university consequences. These behaviors also erode the value of college degrees and higher education overall.

One rule specific to this course. All coursework uses the fictional organization supplied in the scenario packets. Do not analyze, characterize, or submit findings about real Sul Ross systems, real Sul Ross vendors, real Sul Ross vulnerabilities, your employer's systems, or any real institution's security posture. Public sources are fine for general context when cited. Real organizations are not targets for coursework, and treating them as such in this class is an integrity violation regardless of intent.

Classroom Climate of Respect

Importantly, this class will foster free expression, critical investigation, and the open discussion of ideas. This means that all of us must help create and sustain an atmosphere of tolerance, civility, and respect for the viewpoints of others. Similarly, we must all learn how to probe, oppose, and disagree without resorting to tactics of intimidation, harassment, or personal attack. No one is entitled to harass, belittle, or discriminate against another on the basis of race, religion, ethnicity, age, gender, national origin, or sexual preference. Still, we will not be silenced by the difficulty of fruitfully discussing politically sensitive issues.

Supportive Statement

I aim to create a learning environment for my students that supports various perspectives and experiences. I understand that economic disparity, health concerns, or unexpected life events may impact the conditions necessary for you to succeed. My commitment is to be there for you and help you meet the learning objectives of this course. I do this to demonstrate my commitment to you and to the mission of Sul Ross State University to create a supportive environment and care for the whole student as part of the Sul Ross Familia. If you feel like your performance in the class is being impacted by your experiences outside of class, please don't hesitate to come and talk with me. I want to be a resource for you.

Use of Generative Artificial Intelligence (AI)

University Statement (required):

The University does not recommend or endorse any specific AI tools or resources. Students should be aware that many generative AI tools (e.g., ChatGPT, Google Gemini, Microsoft Copilot) store user input and may use this data to train future models. For this reason, students should never upload or share personal, confidential, or identifiable information, such as names, ID numbers, health data, or assignment submissions containing such details, into any generative AI platform. When using AI tools, students should verify whether the tool complies with student privacy standards as indicated by the University. Faculty may recommend specific tools that better align with institutional data privacy policies, but ultimate responsibility for data protection rests with users. Students are encouraged to use faculty-recommended platforms when engaging in coursework involving generative AI. The University is not liable for any adverse experience or impact when students interact with these tools.

Course Policy: Generative AI is permitted with disclosure.

Generative AI may be used on any assignment in this course when you disclose the use and remain responsible for the accuracy, relevance, confidentiality, citations, and reasoning in what you submit. Each major artifact includes a brief AI-use statement identifying (a) whether AI was used, (b) which tool, (c) for what purpose, (d) what substantive output you accepted, modified, or rejected, and (e) how you verified factual claims and made the final decision. "No AI was used" is a complete and acceptable statement.

Never enter into an AI tool: nonpublic institutional information, real systems, real vendor details, real vulnerabilities, personal information, or protected information. This applies to your coursework as a matter of habit and to everything else as a matter of policy.

The disclosure statement is not graded and is not a detection mechanism. I am not going to pretend otherwise. It exists to normalize transparent practice. What actually holds this course together is different: every artifact is built on the one before it, and the oral defense is about your own work. A risk register that does not follow from your own asset inventory will not survive contact with the questions, and a policy that does not trace to your own risk register will not either. The chain is the assessment.

You remain responsible for every claim, source, diagram, risk rating, policy statement, control rationale, and citation submitted under your name, and you must be able to explain and defend any of it. Fabricated evidence, fabricated citations, undisclosed substantive use, or misrepresented authorship falls under the Academic Integrity policy above.

Where This Course Sits

CSA 2372 is the theory-oriented counterpart to CSA 3350 Secure Programming Practices. Four ideas run across all three courses in the sequence, and it is worth knowing where each one is going.

Trust boundary. CSA 1309 introduces the function and module boundary, including scope and the movement of information between parts of a program. CSA 2372 owns the system boundary and the organizational trust boundary: data crossing between systems, services, users, vendors, and cloud dependencies. CSA 3350 elaborates the trust boundary as the place where input validation happens.

Least privilege. CSA 1309 does not name this concept. CSA 2372 owns least privilege as a security design principle and applies it through role-based and attribute-based access control. CSA 3350 elaborates it through file permissions, API scopes, and dependency isolation.

Failure and correctness. CSA 1309 introduces debugging and test cases as ways of reasoning about how programs fail. CSA 2372 owns fail-safe defaults and residual risk as ways of reasoning about how systems and organizations fail. CSA 3350 elaborates it through error handling, fuzzing, and defensive coding.

Evidence. CSA 1309 does not name this concept. CSA 2372 owns evidence through the assurance argument and control effectiveness. CSA 3350 elaborates it through test coverage and static analysis output.

If you have taken CSA 1309, you have already met the first version of two of these. This course generalizes them from programs to organizations. CSA 3350 will take them back down to code.

Reference Links

- NIST Cybersecurity Framework 2.0: https://www.nist.gov/cyberframework
- NIST CSF 2.0 Quick Start Guides: https://www.nist.gov/cyberframework/quick-start-guides
- CIS Controls v8: https://www.cisecurity.org/controls/v8
- CISA Cybersecurity Performance Goals: https://www.cisa.gov/cybersecurity-performance-goals
- NIST SP 800-53 Rev. 5: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
- NICE Framework: https://niccs.cisa.gov/workforce-development/nice-framework