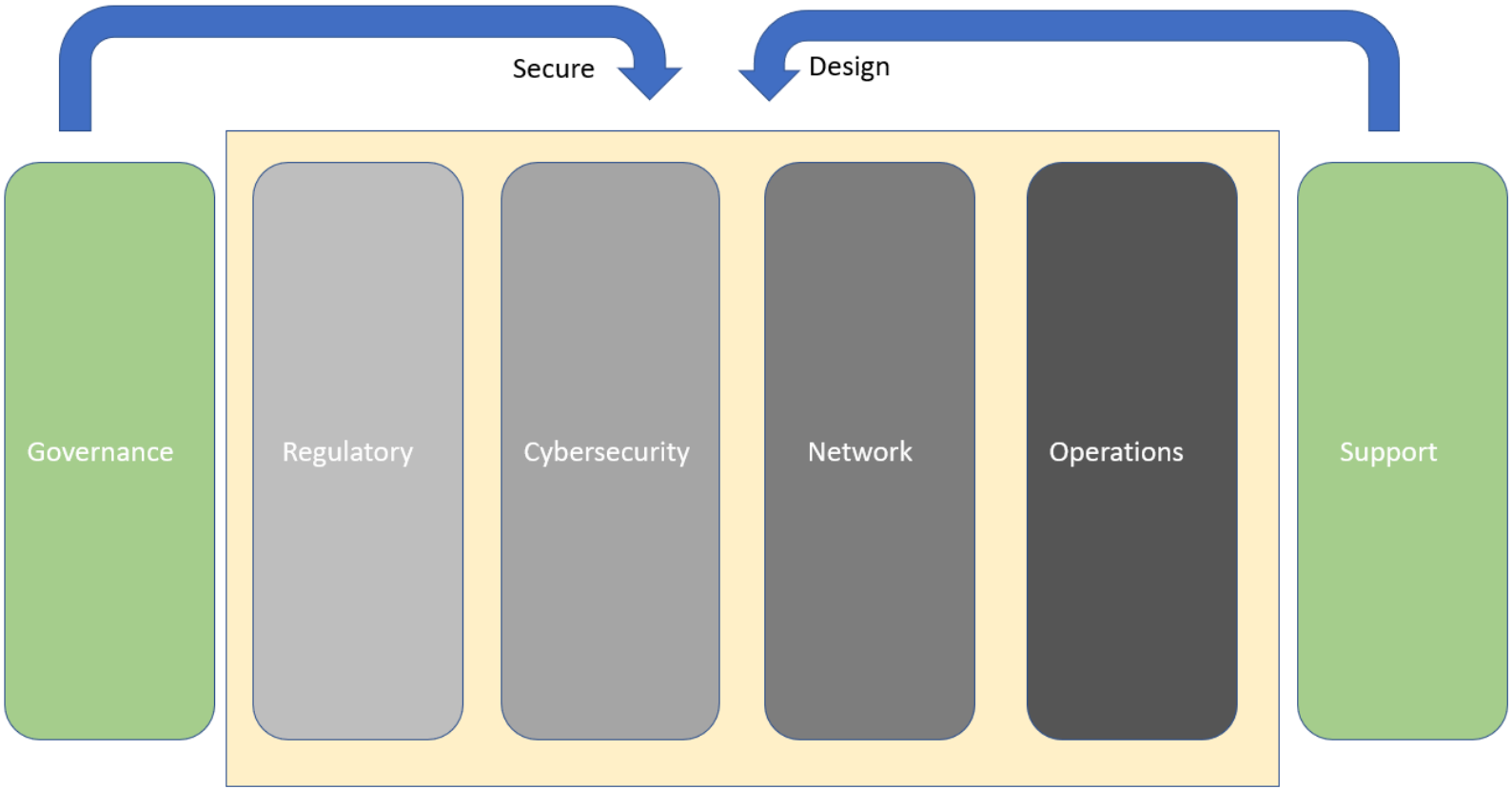
Basic Domains of an Controlled IT Program



Duties within the Domains

Security and Compliance

Duties	Description
Risk Management	Oversees, evaluates, and supports the documentation, validation, assessment, and authorization processes necessary to assure that existing and new information technology systems meet the organization's cybersecurity and risk requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.
Cybersecurity Management	Oversees the cybersecurity program of an information system or network, including managing information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, requirements, policy enforcement, emergency planning, security awareness, and other resources.
Strategic Planning and Policy	Develops policies and plans and/or advocates for changes in policy that support organizational cyberspace initiatives or required changes/enhancements.
Cyber Defense Analysis	Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network to protect information, information systems, and networks from threats.
Incident Response	Responds to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.
Vulnerability Assessment and Management	Conducts assessments of threats and vulnerabilities; determines deviations from acceptable configurations, enterprise or local policy; assesses the level of risk; and develops and/or recommends appropriate mitigation countermeasures in operational and nonoperational situations. Analyzes collected information to identify vulnerabilities and potential for exploitation.
Digital Forensics	Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.

Threat Analysis	Analyzes threat information from multiple sources, disciplines, and agencies across the Intelligence Community. Synthesizes and places intelligence information in context; draws insights about the possible implications. Identifies and assesses the capabilities and activities of cybersecurity criminals or foreign intelligence entities against High Value Assets here at [institution].
Cyber Operations (OPS)	Performs activities to gather evidence to mitigate possible or real-time threats, protect against outside or inside threats.

Operations

Duties	Description
Software Development (devops)	Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.
Systems Architecture/ Systems Analysis	Develops system concepts and works on the capabilities phases of the systems development life cycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes. Technology R&D (TRD) Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility. Studies an organization's current computer systems and procedures, and designs information systems solutions to help the organization operate more securely, efficiently, and effectively. Brings business and information technology (IT) together by understanding the needs and limitations of both.
Systems Administration	Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and

	availability. Manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration.
Infrastructure Support	Tests, implements, deploys, maintains, reviews, and administers the infrastructure hardware and software that are required to effectively manage the computer network defense service provider network and resources. Monitors network to actively remediate unauthorized activities.
Endpoint Administration	Installs, configures, troubleshoots, and maintains desktops and laptops configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration.

Support, Planning and Communication

Duties	Description
Knowledge Management	Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content in order to provide useful information to customers.
Support	Addresses problems; installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g. tiered-level customer support). Typically provides initial incident information to the Incident Response specialty.
Systems Requirements Planning	Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs. Test and Evaluation (TST) Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating IT.

Network

Duties	Description
Network Services	Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (e.g., hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.

Regulatory

Duties	Description
Legal Advice and Advocacy/ Contract Management	Provides legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain. Advocates legal and policy changes and makes a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings.
Regulatory Analysis	Develops, plans, coordinates, delivers and/or evaluates training courses, methods, and techniques as appropriate. Training, Education, and Awareness (TEA) Conducts training of personnel within pertinent subject domain.

Governance

Duties	Description
Executive Cyber Leadership	Supervises, manages, and/or leads work and workers performing cyber and cyber-related and/or cyber operations work. Governing hardware, software, and information system acquisition programs and other program management policies. Provides direct approvals for acquisitions.

Collection Operations (CLO)	Executes collection using appropriate strategies and within the priorities established through the collection management process.
Program/Project Management (PMA)	Applies knowledge of data, information, processes, organizational interactions, skills, and analytical expertise. Categories Specialty Areas Specialty Area Descriptions exchange capabilities to manage acquisition programs. Provides direct support for acquisitions applying IT-related laws and policies and provides IT-related guidance throughout the total acquisition life cycle.

Source: NIST SP 800-181 NICE FRAMEWORK, adjusted to fit current duties spread to various roles at [institution]. These duties reflect a modern IT program.

Process Outline

Governance, Risk, and Compliance, Security Awareness Alignment

Step 1: Policy and Governance (Project Leadership)	Step 2: Review current Business Processes (SPS IRB EXC\IAO As Needed)	Step 3: Create Security Controls (Service Owners)	Step 4: Creating Training Program (Regulator Offices)

• Define the scope for your program (Mission)
  ○ Create or adopt a change management process
• Defined Roles
  ○ Assign Primary Roles
  ○ Assign Secondary/Oversight Roles
• Perform Policy Reviews
• Create a Unified Glossary
• Create Unified Templates
	• Create Workflows
	• Verify Staffing Levels
	  ○ Roles
	  ○ Groups
	• Additional Requirements
	  ○ Defined per institution
	• Training Requirements
	  ○ Outline of your existing options and any additional requirements.
		• Based on Regulator Requirement, existing institutional controls Example:
		  ○ L1 Fundamental Research
		  ○ L2 Sensitive Research
		  ○ L3 HIPAA and FERPA
		  ○ L4 Controlled US Person+
		  ○ Crosswalk all regulator control sheets (Mapping the Controls for Audits)
		• Create a process to ensure controls are meeting the threat level of existing and newly discovered vulnerabilities.
		  ○ Threat Model for Research per institution
		• Set SOC Monitoring Requirements
			• Modify current training options if required
			• Reviews current trends and immediate risks
			• Review compliance training requirements
			• Determine how training will be offered
			• Create new training materials

Alignment Process, Business Continuity and Disaster Recovery

Step 5: Categorize Information Systems (Service Owners)	Step 6: Select the defined Security Controls (Service Owners Regulator Offices)	Step 7: Implement Security Controls (Service Owners Regulator Offices)	Step 8: Access Security Controls (Service Owners Regulator Offices)

• Categorize Information System
  ○ Type of Data
  ○ Operational Requirements
• Described the Information System
• Start Drafting Security Plans
• Start Risk Assents for new systems
• Review Risk Assessments for existing systems
• Added to asset to inventory
	• Determine Access Level as defined in step 4
	• Tailor controls if required
	• Add to monitoring strategy
	• Complete new Risk Assessments
	• Complete Security Plans
		• Implement Security Controls
		• Amend Security Plan if required
		• Communicate completion date to stakeholders
		• Complete required compliance training
			• Security must test the security controls prior to go live. Create a security report outlining any findings.
			• Adjust any findings or determine its safe to operate.
			• Add the remaining findings to risk assessment or Adjust the Security Plan
			• Test final SOC requirements

Step 9: Authorize Information System (Service Owners Regulator Offices)			
• Document residual risk using a Plan of action and milestones (POAM) template • Collect all reports, documentation and store it in a secure location for future reference. • Complete risk acceptance and sign the system security plan and distribute. Work with Regulator Offices and Contracts, providing the required details to recommend or authorize the use of the service			

Audits/Alerts, Incident Management and Response Security Awareness Communications, and Training

Step 10: Monitor Security Controls (Service Owners Regulator Offices)	Step: 11 Conduct and Access Training (Service Owners Regulator Offices)

● Control System and Environment Changes
  ○ Change Management
  ▪ Create an internal process to review RFCs before they are submitted for accuracy and compliance requirements
  ○ Vulnerability scanning
  ○ Vendor notification
  ○ Log review
● Review Access Controls
  ○ Define a set reviewed annually
  ○ Define a set reviewed by continuous monitoring
● Remediate finds
  ○ Create a remediation guide based on risk
● Update required documentation
  ○ System Security Plan
  ▪ Changes to required controls
  ○ POAM
  ▪ Controls residual risk
● Define Decommission Process
● Document/Review Incident Response
	● Conduct In person trainings for new topics
	  ○ Supplement with online training as topic matures
	● Enable Online training for topics that need to be referenced often. Provide written materials.
	● Conduct communications based on immediate risk
	● Send notification to individuals missing mandatory training
	● Conduct Tabletop Exercise
	  ○ New Monitoring tools
	  ○ Incident Response
	  ○ Disaster Recovery
	● Measure training results