Albany State University
Strategic Information Security Plan

I. Information Security Governance Process

1. Assess current ASU ITS security governance model – define what type of relationship between USGBOR ITS and ASU (ISO and CISO)
2. Identify Security Steering Committee membership and develop understanding of the specific roles and responsibilities – ASU Academic and Business owners and ITS Technical owners / stewards (hereto all security operational requirements will be submitted through this committee)
    a. Identify who should be the Academic and Business owners - VPs, Directors, etc.
        i. Clearly identify business goals and objectives
        ii. Level and scope of influence
        iii. Role and responsibility
    b. Identify who should be the Technical owner(s) / steward(s) CIO, CISO, CDO, or ITS Directors
        i. Level and scope of influence
        ii. Role and responsibility
    c. Identify the relationship between functional academic and business objectives, technical capabilities, and information and information system security
    d. Identify the role and responsibility of the security owner(s) / steward(s) in relationship with academic and business owners and information and information system stewards, e.g., ISO and CISO
    e. Identify high level ASU security objectives in accordance with USGBOR
3. Develop a Security Charter for key shareholders (Security Steering Committee) that identifies scope of security operations (high Level). Gain approval and commitment.
    a. Risk Assessments, Incident Response, Remediation, etc.
    b. Policies, Standards, and Procedures to secure information assets
        i. Policies – general and high level, clear concise verbiage, easy to understand, and result from and capture intent of the security strategy
        ii. Standards – owed by the CISO / ISO, provide meaningful boundaries of security application (without unnecessary restrictions), and reflect the intent of the security policies. Exception processes must be identified to assist managing the gap between the current USGBOR, State, Federal, etc., and ASU expected end results
        iii. Application of policies and standards to be identified and implemented by academic and business owner, trustees, and information and information system owner(s) / steward(s). Procedures are to be created and implemented at the lowest department level possible, typically a director
    c. Security Management Structure (roles, responsibilities, authorization, and authority)
    d. Information and information system security identified as a critical aspect of all business or technical operations (define "Open" educational environment for ASU)
4. Established clearly defined communications procedures for both internal and external security coordination and reporting
5. Develop Risk Profile and Security Governance Metrics
    a. Key Goal Indicators (KGIs)?
        i. Clear objectives with consensus
        ii. Regulatory compliance
        iii. Address Risk

1) Strategic
2) Financial
3) Reputational
4) Operational
5) Compliance

b. Critical Success Factors (CSFs)?
   i. Identify, categorize, and define controls
   ii. Define appropriate test to determine effectiveness
   iii. Commit resources to facilitate testing requirements

c. Key Performance Indicators (KPIs)?
   i. Key or critical performance factors to achieve security objectives
   ii. Progress in applying control effectiveness
   iii. Defined Testing Plan and periodic review
   iv. Results of testing control effectiveness

d. Implementation of Metrics
   i. Strategic Alignment – security effectiveness supports educational environment and includes legal / regulatory compliance requirements
   ii. Risk Management – efficient and effective controls, that meets expectations and defined objectives for mitigating risk
   iii. Value Delivery - functional alignment of security strategy and business objectives to secure information and information systems
   iv. Resource Management – effectively plan, procure, allocate and control resources (people, processes, and technology
   v. Performance Measurement – Measure, monitor, and report on the effectiveness of security program, e.g., Common Maturity Model of Internal Controls (CMMI)
      1) Variants of the CMMI: CMM & ISO 15504
      2) Identifies <u>WHERE</u> you are at and <u>HOW</u> to get to the next level
         a) Levels of Application
            Level 0: <u>No Recognizable Process</u>, though one is needed
            Level 1: Process is <u>Ad-hoc</u> and performed by key individuals
            Level 2: Process is <u>Repeatable</u>, but not controlled
            Level 3: Process is <u>Defined</u> & <u>Documented</u> and periodically <u>Evaluated</u>
            Level 4: <u>Managed & Measurable</u>; effective Internal Controls with Risk Management
            Level 5: <u>Optimized</u> Enterprise wide risk and control program
         b) Process is progressive and continual
   vi. Assurance and Convergence – create a clearly defined security operational template for old and new applications and processes to be certified as secure per the current information security standards

6. Assess current Information security strategy of USGBOR with ASU ITS – will need separate the two, and hereto will be one in the same)
7. Identify USGBOR and ASU ITS security objectives
8. Determine current state of security at ASU through Fit-Gap analysis
9. Develop an Information Security Strategy – long term and short term objectives

10. Identify needed strategic operational resources, logistical requirements, and any associated constraints or barriers
    a. ASU shareholder levels of investment and feedback
        i. Each academic and business objective identified with outcomes and the technology in place to support it effectively
        ii. Security required to afford business success and mitigate risk
    b. Physical / Technical Resources and the level of investment needed from various entities and the commodities they manage
    c. Critical Objectives, Milestone, and Time lines
    d. Legal Obligations
    e. Interrelationships between the aforementioned and possible barriers
11. Develop a Plan of Action for Security Strategy implementation
12. Align Security Strategy with Governance – modify scope accordingly and finalize POA
13. Sell the plan and gain approval from key shareholders for implementation
14. Communicate, train, and support all security team players

II. Information Risk Management Process

1. Risk Management Strategy
    a. Identify information asset ownership and classification
        i. Business / Technical unit identify applications and use
        ii. Classify criticality or sensitivity
        iii. Identify interdependencies among ASU agencies (aggregated or cascading risk)
        iv. Perform a Business Dependency / Business Impact Analysis (BIA), e.g., what if we lose the use of …?
    b. Identify associated threats, vulnerabilities, exposures, and likelihood
    c. Assess and identify Risk Management options
        i. Terminate activity
        ii. Transfer risk
        iii. Tolerate / accept the risk
        iv. Mitigate the risk
    d. Develop a Risk Management Framework
    e. Acknowledgment and determination of reporting requirements
    f. Alignment with security governance committee's guidance and objectives, Legal liabilities, and regulatory compliance
2. Risk Assessments
    a. High impact and high probability focus on critical / sensitive information and information systems
    b. Focus on the results of the Business Dependency / Business Impact Analysis (BIA)
    c. Fit-Gap analysis and Baseline modeling
    d. Conducted periodically and systematically with clearly defined principles and practices
    e. Internal and external audits
3. Analysis Methodologies
    a. Knowledge and skill sets required
    b. Structured framework with operational processes that are measurable, repeatable, and documented
    c. Provide guidance to Business and Technical owners on how to implement controls

        i. Preventive: controls to stop the problem from occurring
        ii. Detective: controls to find the problem
        iii. Corrective: controls to repair the problem after detection
        iv. Administrative: policies, standards, guidelines, & procedures
        v. Technical: controls using hardware or software for processing & analysis
        vi. Physical: controls to implement barriers or deterrents
    d. Based upon industry certification standards & requirements
    e. Critical Implementations
        i. Academic and Business owners, Users (trustees), and Technical owner security guide
        ii. Exceptions and variances to policy or standards
        iii. Identity and Access Control Management
        iv. Perimeter and Network Access Control and Management
        v. Patch Management
        vi. Configuration and Change Management
        vii. Project Implementation Management
        viii. Incident and Response, Disaster Recovery, and Business Continuity (BCCP) Management
        ix. Third Party and Contract Management
    f. Determine if residual risk exist and cost versus benefit analysis
4. Implementing Control and Countermeasures
    a. Utilize cost-benefit analysis
    b. Industry standards
        i. FISMA / NIST, ISO, etc.
        ii. Various other recognized tools, e.g., ITIL
    c. Integrate controls and countermeasure in project management, development, procurement, and employment life cycles
5. Information Resource Valuation – as it relates to risk management
    a. Cost of Hardware / software
    b. Cost of Information
    c. Cost of personnel
    d. Other cost factors
6. Recovery Time Objectives
    a. Amount of acceptable time to recover from an incident and reestablish normal operations
    b. Reconciliation of the BIA and Business Continuity and Contingency Plan in practical terms
    c. Third Party influence or dependencies
7. Integration with all SDLC processes – where is the security consideration step or influence into the process?
    a. Initiation
    b. Development and acquisition
    c. Implementation
    d. Operations and Maintenance
    e. Disposal
8. Security Control Baselines
    a. Acknowledge and establish understanding of current state of security
    b. Maintain or build controls and resources to meet security requirements
    c. Test for consistency and continuity

9. Risk Monitoring and Communications
    a. Processes involved for monitoring security readiness state
    b. Documentation Plan
        i. Processes for documenting security readiness
        ii. Reporting process for deviation or violation of security standards
10. Methodology for enforcement and realignment with security policies and standards
11. Periodic training and awareness of security requirements

III. Information Security Program Development and Management Plan of Attack

1. Organizational roles, responsibilities, and effective communication
    a. Security is everyone's responsibility, but particulars must be disseminated
    b. Communicate and maintain security policies, standards, guidelines, and operational procedures
2. Information Security Management Framework
    a. What security activities will be performed
    b. Promote a security culture that compliment Higher Education
    c. Framework should be simply, intuitive, and systematic
    d. Information and Information System infrastructure and architecture
        i. Security framework on which to build upon
        ii. Provides guidance and direction
        iii. Should be clearly defined and simple allowing layering and modularization
        iv. Business focus beyond the technical limitations or associated domains of influence
        v. Should include both technical and non-technical controls
        vi. SABSA Matrix – What, Why, How, Who, Where, and When
            1) Strategy and concept
            2) Design
            3) Implement
            4) Manage and measure
3. Performance measurement of Information security management
    a. Aligning business objectives and technical capabilities with security program
    b. Establish clearly defined metrics
4. Expected security management challenges and other considerations
    a. Undefined Higher Education "Open" security culture
    b. Resistance due to changes in role or responsibility as a result of security implementations
        i. Internal ITS departments
        ii. Colleges and departments
        iii. ASU and USGBOR institution exchange
        iv. Existing Third party or Contracted agencies
    c. Overreliance on subjective metric
    d. Perception of increased security reducing academic and business functionality
    e. Ineffective project management that delays security initiatives
    f. Procedural compliance without managerial involvement (Academic/Business and Technical owner)
    g. Previously undetected security implementations which violate new security standards
    h. Third Party and contracts
5. Information security management resources

    a. Skills required
    b. Technology required
    c. Alignment of people, process, and technology
    d. Cost / Benefit Analysis
6. Information security management state determination
    a. Security has not had in the past a predetermine emphasis or influence
    b. Fit-Gap analysis will need to thoroughly identify what is the current security state for institution information and information systems
    c. Determination is dependent upon business and technology owners
7. Information security management implementation (continuous life cycle)
    a. Plan
    b. Implement
    c. Monitor and measure
    d. Improve or correct
8. Result of an effective Information and Information Systems Security Program
    a. Vision for information and information system security should establish the ground work for identifiable strategic objectives - key goal indicators (KGIs)
    b. Objectives allow the establishing of critical success factors (CSFs)
    c. CSFs provide targets for key performance indicators (KPIs)
    d. KPIs support business and technical owners information needed to implement controls or change business or technical applications
    e. Produce identifiable observable improvement in information and information systems security and awareness throughout the institution

IV. Incident Management and Response Considerations

1. Scope and Charter of Incident Response Management
    a. Formally establishes roles and responsibilities (business and technical owners)
    b. Delegates appropriate authorization and authority to quickly respond
    c. Describes the mission, scope, organizational structure, information flow, and services provided
2. Incident Management Objectives
    a. Incident detection
    b. Determination of severity level
    c. Assessment and triage
    d. Declaration criterion for escalation of severity level
    e. Scope of incident management
    f. Response capabilities
3. Incident Management Metric and Indicators
4. Incident Response Management resources and training requirements
5. Incident Management Procedures and Documentation
    a. Clearly defined scope and operational procedures
    b. Must integrate BIA and Risk Assessment effectively into IRP / DRP / BCP
    c. Document detection, triage, response
6. Challenges in development of an effective IRP
    a. Lack of management buy-in and organizational consensus

    b. Mismatch or improper orientation to organizational goals or structure
    c. Lack of resources or skill sets to properly respond
    d. IR team member turnover
    e. Lack of effective communication process or procedures
    f. To complex and scope not clearly defined
7. Determine current state of Incident Management capabilities – Fit-Gap analysis of possible interruption window
    a. Recovery Time Objectives (RTOs)
    b. Recovery Performance Objectives (RPOs)
    c. Service Delivery Objectives (SDOs)
    d. Maximum Tolerable Outages (MTOs)
8. Develop Incident Response Plan - IRP
9. Develop Recovery Plans (Disaster Recovery Plan - DRP and Business Continuity Plan - BCP)
10. Testing IRP, DRP, and BCP (determination and escalation criterion)
11. Execution of IRP, DRP, and BCP
12. Post event reviews, analysis, and documentation