SMITH COLLEGE INFORMATION SECURITY PROGRAM

November, 2013

1. *Purpose and Scope :*

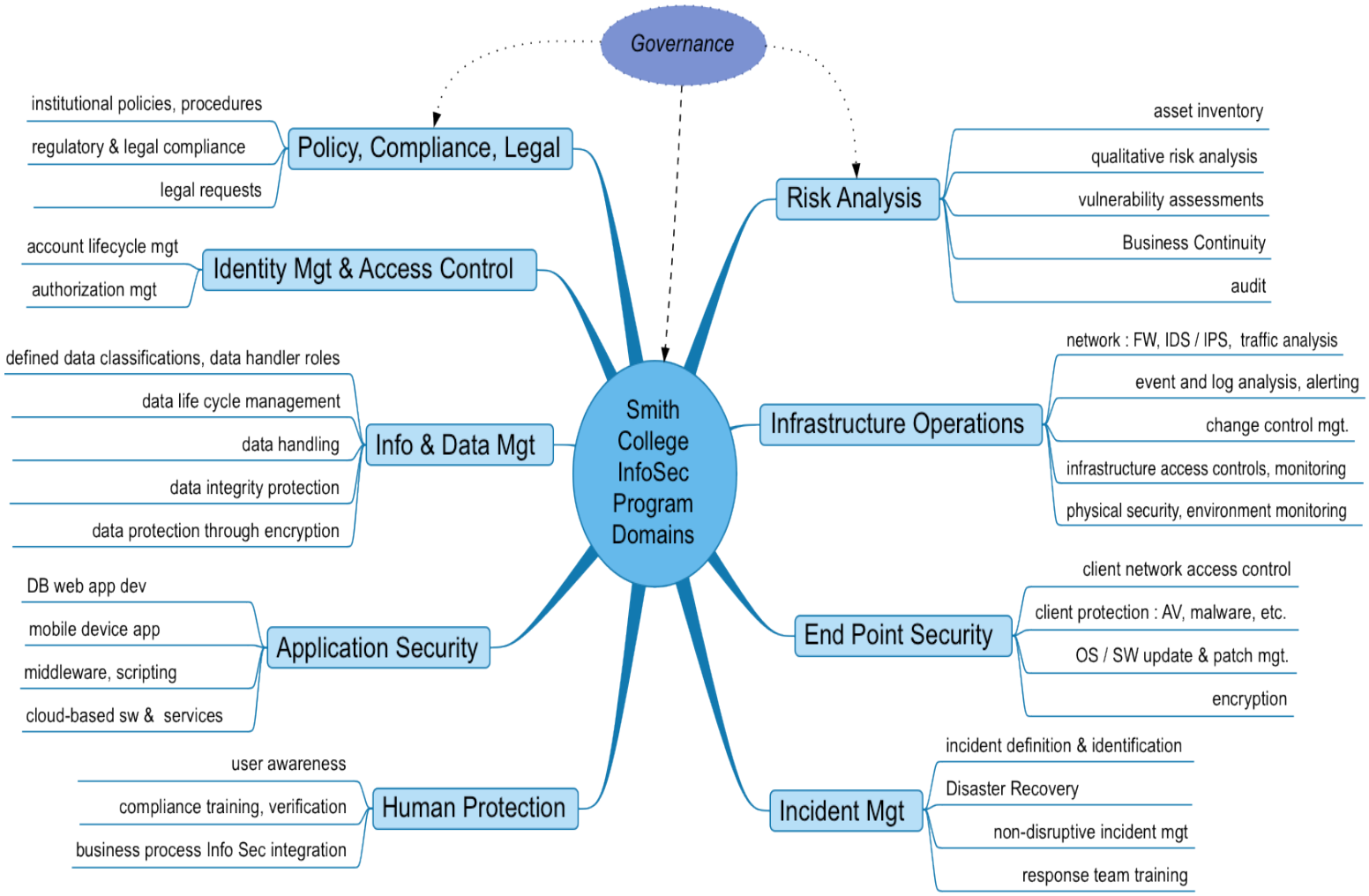
Smith College's information security program serves to promote the assurance of the confidentiality, integrity and availability of the college's information resources. This program provides a framework designed to afford the institution with comprehensive, risk-based information security assurance coverage.

The implementation goal is to minimize risk to information with minimal impact on its productive use. The program addresses the institution's information and data assets regardless of form or media.

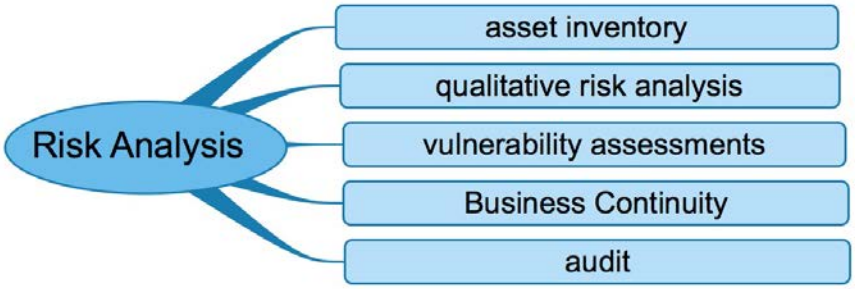
2. *The Information Security Control Domains Framework :*

The information security program defines broad control domains to most effectively manage existing information security controls, and to help prioritize security initiatives. A **framework** of security control domains is used to ensure that an institution's information security program covers all major areas where risks are present.

The following diagram defines the major domains of the framework, and the general sub-domain control groups within each domain.


Governance
Smith College InfoSec Program Domains
Policy, Compliance, Legal
institutional policies, procedures
regulatory & legal compliance
legal requests
Identity Mgt & Access Control
account lifecycle mgt
authorization mgt
Info & Data Mgt
defined data classifications, data handler roles
data life cycle management
data handling
data integrity protection
data protection through encryption
Application Security
DB web app dev
mobile device app
middleware, scripting
cloud-based sw & services
Human Protection
user awareness
compliance training, verification
business process Info Sec integration
Risk Analysis
asset inventory
qualitative risk analysis
vulnerability assessments
Business Continuity
audit
Infrastructure Operations
network : FW, IDS / IPS, traffic analysis
event and log analysis, alerting
change control mgt.
infrastructure access controls, monitoring
physical security, environment monitoring
End Point Security
client network access control
client protection : AV, malware, etc.
OS / SW update & patch mgt.
encryption
Incident Mgt
incident definition & identification
Disaster Recovery
non-disruptive incident mgt
response team training

3. *Information Security Controls Overview :*



The **Risk Analysis** domain *provides a general assessment of the information security environment for governance review*.

A strategic review of the critical **information systems assets** of the College is required to effectively evaluate what is to be protected, where the exposure to threat is highest, and to set risk mitigation priorities for areas that may be ineffectively covered. Areas with mission critical assets include :

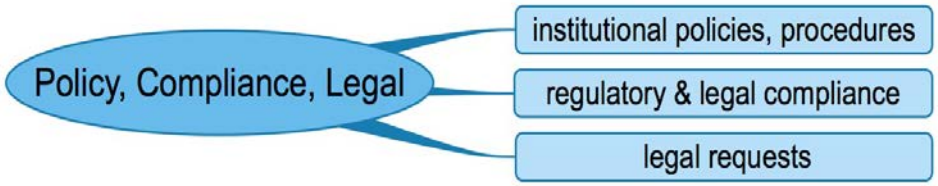
- administrative ERP systems & service platforms, storage and support infrastructure that provide key administrative services (payroll and financial business processes);
- academic LMS and supporting services, and other critical services supporting the academic mission of the College;
- protected academic research information and systems, storage and devices.

A **qualitative risk analysis** on core administrative assets, identifying areas with relative risk exposure, was performed several years ago. An updated and expanded inventory risk analysis is needed to identify areas requiring mitigation efforts, as well as areas that are acceptably covered by current controls.

Similarly, a strategic Business Continuity Plan was created several years ago. An updated **Business Continuity Plan** that articulates goals for maximum allowable critical systems downtime, and current strategic controls that are in place to achieve those objectives, should be created for governance review. The institution can then accept the current plan, or choose to allocate resources to provide increased assurance of service availability.

The general information security threat landscape changes rapidly. To stay current with these changes, a **vulnerability assessment** should be performed periodically to identify potential exposure to the threat landscape. A vulnerability assessment solution that can perform select assessments, both on demand and as automated assessments on critical infrastructure components, should be identified and implemented. An external vulnerability assessment and security audit is recommended.

Lastly, an **audit** of the effectiveness of security program controls and the institution's general information security profile should be considered. This might include internal efforts to identify security controls performance metrics, perform a security controls assessment, or a compliance conformation analysis. An external analysis of the institution's security profile might also be considered.



The **Policy, Compliance, Legal** Domain *establishes strategic directive controls mandated by internal governance and external regulatory entities*.

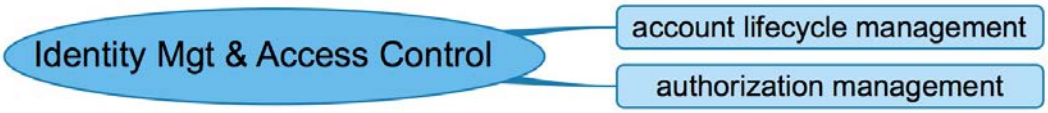
The Smith College community maintains a comprehensive portfolio of information security related **policies** and similar administrative directive security controls, developed with governance approval by departments, committees and data owners. Largely, these policies are posted for access and review on Smith's main Web site or departmental sites, with select policies also printed for dissemination to Smith community members. Policy awareness efforts are performed by HR, Student Affairs, and ITS among others. An effort to create a unified policy content structure by the College's compliance committee is underway, which will enhance policy intent, promote more consistent enforcement, and provide for more timely updates to or decommissioning of policies.

Mandated information security requirements exist :

- in state, federal and international law;
- in requirements from regulatory agencies;
- as components of grant and research agreements;
- in institutional and departmental policies.

The identification of applicable information security **compliance** requirements is currently the responsibility of the data owner, with general oversight by the College's Compliance Committee. Verification of adherence to compliance controls is an important component of directive controls effectiveness, but is generally uneven and difficult to perform. A review and update of existing policies should be performed as part of any ongoing security review process, and should include awareness efforts to promote compliance.

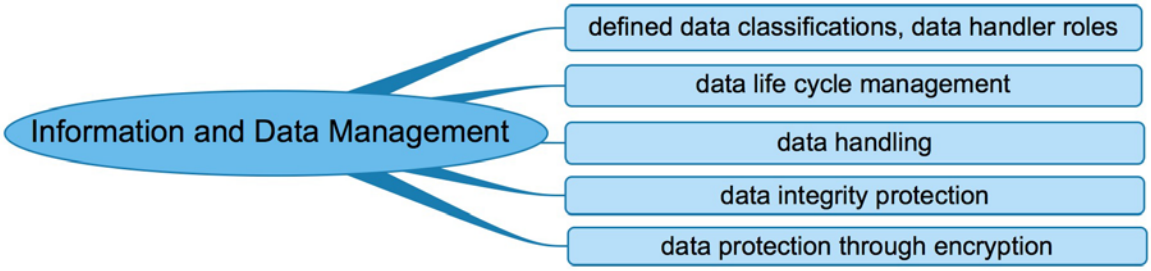
Procedures for the handling of **legal** requests such as DMCA violations or litigation hold notices, and for authorization override requests such as access to an individual account's content by a supervisor, or by public safety for life/safety issues, are generally well understood and appropriate controls in place to provide information as required without violating confidentiality or privacy policies and goals.



The **Identity Management and Access Control** Domain *sets the electronic identity and functional roles for individual users*.

Management of the electronic identity of an individual that is both timely and efficient has grown with exponential importance as increasing numbers of services use "single sign on" and federated access for identity authentication, privileged authorization, and access control. Smith has an established set of policies, business processes, and administrative controls that provide adequate control over account life cycle and user authorization management. Smith also has an established technical infrastructure supporting account directory services to adequately meet current authentication and authorization needs.

However, both the administrative processes and the technical infrastructure show signs of inadequacy in their ability to perform core identity management functions with requisite alacrity, such as : provision accounts, add attributes, change authorized access settings, de-provision accounts, and audit activity; or to easily integrate with new services requiring access to institutional identity, authorization and user attribute information services. Retaining the current environment affects the availability of services for both new users and for existing users with new roles, increases risk of identity management errors, potentially limits future expansion of services requiring IAM support, and increases risks to identity information integrity.



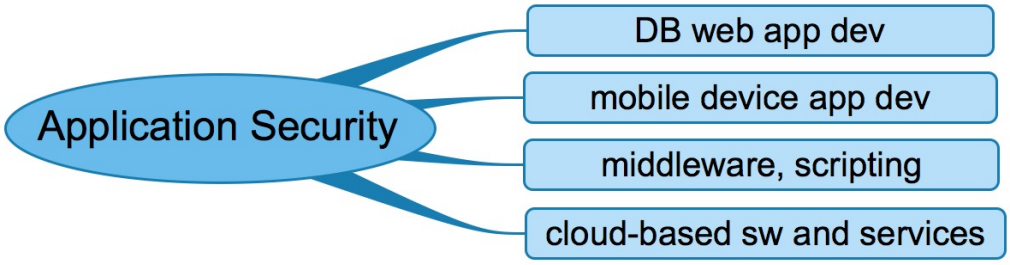
The **Information & Data Management** domain *sets security controls on all aspects of institutional data and records, including data classification, confidentiality, integrity, and data life cycle management.*

Information and Data Management security controls apply to all aspects of institutional data and records. These controls include :

- data classification,
- controls for data confidentiality and integrity,
- processes for data life cycle management, and
- administrative controls for legal and regulatory compliance mandates.

Institutional data is classified as specified in section 5.5 of this program, and made available to authorized users for only as long as a legitimate business or academic need requires.

Smith has developed institution level policies for data handling and data life cycle management, and has provided some staff training for compliance and data handling. Technical controls are in place to protect data accuracy and integrity, including separation of production and development services of administrative systems, and data backup processes for recovery of lost or corrupt information. Encryption of data at rest in data center storage, and in transit within the Smith local area network is selectively but not widely implemented.



The **Applications, Services and Software** Domain *incorporates confidentiality and integrity considerations in the development or incorporation of application software, middleware implementation, back end script development and implementations, and in the adoption of public cloud based applications or services.*

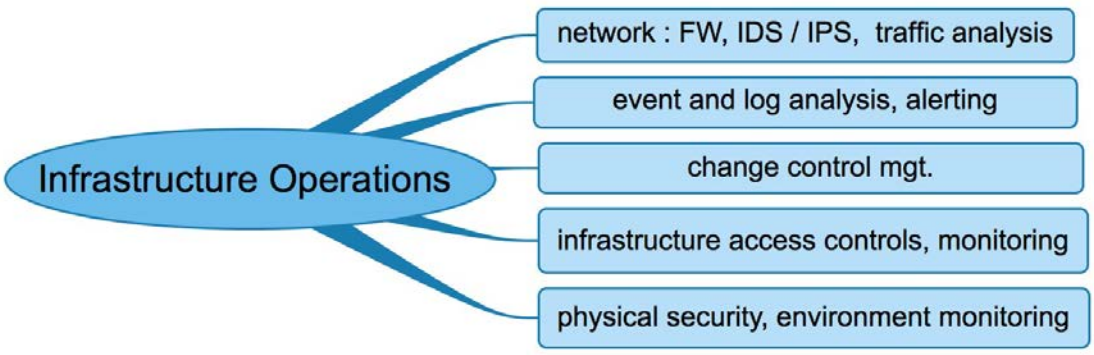
The rapid growth of software development and service deployment generally has elevated the need for security integration and security controls to a top tier domain. The domain infuses confidentiality and integrity considerations into the development or incorporation of web front end, application software, middleware implementations, back end script development and implementations, and the adoption of public cloud based applications or services.

Security checks and controls should be incorporated into :

- database-driven web program development and web application implementation,
- mobile device application development for apps that access institutional information,
- enterprise middleware development or 3rd party middleware adoption, and
- script development for the automation of back end or repeated processes,

to ensure enforcement of access and data modification authorization, and to protect production data integrity. Methods for vulnerability testing and checks for embedded security verification should be identified and incorporated as an integral part of the general software development and service implementation process.

Similarly, the risks and security implications of public cloud based software, applications, or services that require access controls or hold classified data, should be reviewed, and possible security controls adopted. An institutional policy should be considered that addresses cloud service security, and any legal or compliance accountability transfer, before cloud-based service agreements are made.

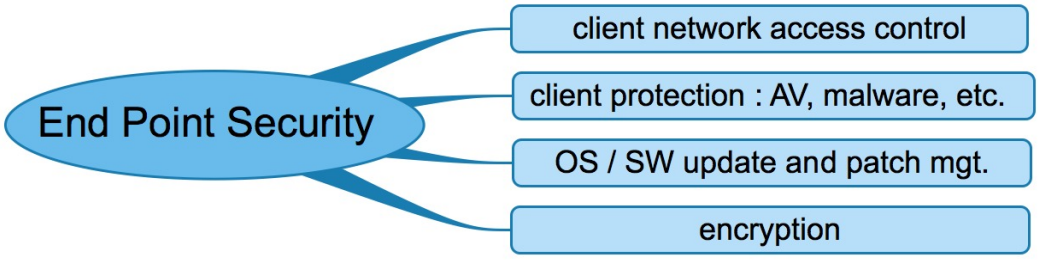


The **Infrastructure Operations** Domain *protects the College's central systems, services and infrastructure through a variety of technical and physical controls.*

Perhaps the most traditional and well understood control domain, security protections for the College's central systems, services and infrastructure are accomplished through a variety of technical and physical controls. Controls implemented by Smith include :

- network traffic controls such as firewalls, intrusion detection, intrusion prevention, and network traffic anomaly detection and alerting;
- network device, system and service log aggregation, analysis, and alerting;
- change control management, including system patch and security updates, for core network, systems, and services;
- infrastructure administrative access controls and monitoring;
- physical security controls, including : restricted physical access to data center and network devices, physical access monitoring and logging, and alerting options and response procedures;
- data center environment monitoring, alerting, and response procedures for power, temperature, humidity, smoke & fire, and other parameters that present a threat to normal data center operations

Recent major upgrades to data center and network infrastructure have provided the opportunity to increase resiliency and incorporate new control points, including firewall and IPS controls, log management, network and service monitoring, and environment monitoring. The implementation and tuning of these controls is ongoing. Other controls, in particular change control management, should be reviewed for improvement.



The **End Point Security** Domain *addresses all aspects of network edge device security.*

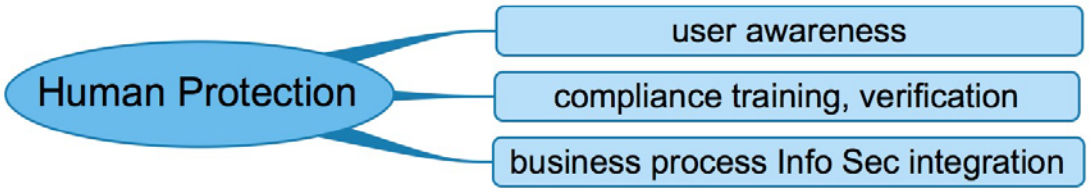
With the mushrooming variety of devices connecting to network based resources, the device and operating system manufacturers have taken significant steps to build both device and information security into these systems and the applications they run. Unfortunately, black hats have also taken a dark shine to finding and exploiting vulnerabilities in these very widely deployed new devices. Consequently, use of mobile devices for processing of classified data is restricted, and in some cases prohibited.

In addition, the incorporation of infrastructure and institutional services on data networks has also increased substantially. These include : Security devices and security monitoring, HVAC and SCADA equipment, building control systems, OneCard and other

access control services, medical equipment, research lab equipment monitoring and data gathering, and more. These may require special IS controls particular to the specific service or devices.

A variety of security controls to protect client devices are in place. These include authorization for access to Smith's network and services, resources for client protection from viruses and malware infestation, and information for users about client management best practices, including :

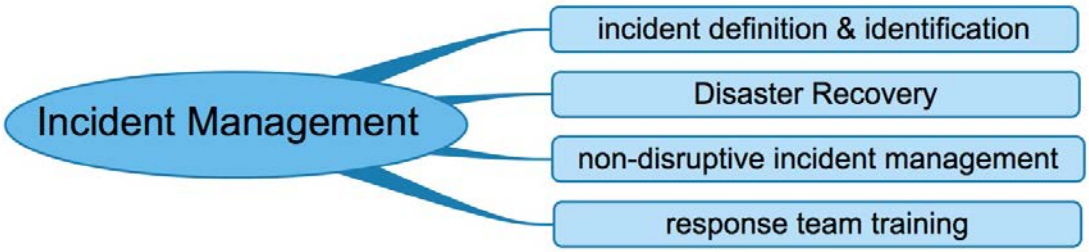
- regular operating system and software update checks,
- personal backups of important information and files,
- setting password protections to prevent unauthorized client access,
- use of encryption to protect important personal or institutional information if the device becomes lost or stolen,
- physical security of the device itself, and
- recognition of client compromise and response options.



The **Human Protection** Domain *promotes keeping users safe, the safe use of information resources, and proselytizing Info Security awareness.*

The weakest link in any institution's information security profile is widely recognized to be its people. Initiatives in this domain include promoting user awareness of current threats and best practices; providing users with policy and compliance training, and promoting information security integration into business processes and the user's work environment.

This domain also includes helping community members protect themselves online : recognizing and promoting personal security and privacy. Users at every level should feel prepared to deal with issues involving personal privacy, account and password security, on-line harassment, personal Denial of Service, personal account compromise, identity theft, credit card account compromise, and other online personal security issues.



The **Incident Management and Response** Domain *defines the breadth of incidents, and sets procedures for minimizing the impact of incidents.*

A "security incident," as defined in section 5.7, could be a successful hacker intrusion into a server, a data center fire, or a software glitch that crashes a widely used service. It is important for any member of the community to recognize that an anomaly or unexpected quirk encountered in their normal information business work may indicate a potential security incident, and when in doubt, bring such information forward to the ITS user support center for further evaluation.

A **Disaster Recovery** (DR) plan addresses any service interruption or data loss event, or potential data exposure such as an intrusion event; it articulates incident handling and response procedures, including :

- data recovery capability (fka data backups), recovery procedures, and an expected mean or maximum restoration time frame,
- service recovery capability (fka server backups), recovery procedures, and expected mean or maximum restoration time frame,
- recommended processes for complete incident handling :
    - incident triage,
    - communications with both decision makers and community members,
    - escalation procedures,
    - containment, eradication, and restoration processes,
    - post-incident reporting, and lessons learned.

Smith's Disaster Recovery plan was originally developed several years ago; while aspects of that plan remain applicable, a substantive revision and update is needed.

Incident handling and response procedures for ***non-disruptive*** **incidents**, such as a legal or policy violation or a health-safety related incident, are also needed. The legal and compliance requirements that should be included in incident response and forensic analysis plans should be discerned and included in any incident response plans.

Finally, incident response teams should be identified and called together for DR plan and incident response testing such as a hypothetical incident tabletop discussion exercise. Any response or forensic tools or other resources should be identified and tested. Incident response logging, especially for a potential MA PII data breach event, should be included during response testing; log format and content entries should be discussed.

4. *The Information Security Program Process :*

The security controls framework requires a general process for its elements to be evaluated and implemented, and its ongoing value assessed, as best fit the needs of the college. The COBIT 5 standard framework notes two framework and process architecture goals that are directly relevant this program :

Simplicity : The enterprise architecture should be designed and maintained to be as simple as possible while still meeting enterprise requirements.

Agility : The enterprise architecture should incorporate agility to meet changing business needs in an effective and efficient manner.

This Program implements the general process design described by COBIT (5.0) :

Plan & organize:
Acquire and Implement :
Deliver and Support :
Monitor and Evaluate :

Plan & Organize :

- Perform general risk domain assessment :
  - itemize essential assets, identify & evaluate probable threats, assess applicable vulnerabilities
  - identify / confirm current controls
- Identify current compliance requirements :
  - update applicable policies, procedures, standards
- Evaluate current security controls :
  - consort with stakeholders, identify resources
  - identify high risk gaps (gap analysis)
  - perform risk mitigation options analysis, identify security initiatives & projects

Acquire & Implement :

based on planning assessment, identify appropriate technologies, tools and resources
set and implement security initiative projects

Deliver & Support :

once in place, ensure that controls are active and functioning properly
confirm Quality of Service impact, cost, and staff resource needs meet expectations
manage changes and updates to existing controls

Monitor & Evaluate :

acquire and audit performance metrics where available
confirm compliance with regulatory and policy requirements
evaluate controls performance and comprehensive security profile
develop general Security Profile Assessment report for IT & Compliance governance review
include recommendations for prioritized risk mitigation next steps

5. *Important Concepts, Definitions, and Terms :*

5.1) **Information Security** (IS) :

Information Security goals are often distilled into three core concepts : confidentiality, integrity, and availability (CIA). Very simply, **confidentiality** refers to ensuring that only authorized users are allowed access to data or services. **Integrity** refers to the trust that the information and services provided and received are accurate, valid, and come from a known or authorized source. **Availability** seeks to ensure that IT information and services remain available and useful for all who need them.

5.2) Information Security **Risk** :

"**Risk**," generally defined, is the probability that a particular threat will cause harm to a particular target. The target must have some vulnerability to that threat, or there is no potential harm and therefore no risk from that threat. Risk reduction or risk mitigation is therefore the process of identifying and reducing vulnerability to probable threats.

5.3) **Security Controls** :

A "**Security Control**" is any form of safeguard implemented to reduce risk associated with information security. In practice, Information Security is about implementing "security controls" designed to balance risk mitigation with pragmatic utility; and with vigilance, to dynamically alter or replace controls as those risks and utilization needs change (see additional note in section 6.1).

5.4) **Data defined** :

Institutional data : any information or data that has been generated or aggregated for use by the College in any of its academic or business functional needs. Information collected by an individual for their personal use, or by a group working outside the confines of a recognized college function or service, is not Institutional data and is not subject to the Security Program or institutional data governance.

It is important to remember that institutional data should be identified and classified regardless of its medium or form.

5.5) **Data Classification** :

Within the context of Information Security, there are three levels of "**Classified**" information, summarized here (see additional note in section 6 for more detail) :

PII : Personally Identifiable Information, or Personal Information (PI) : "Personal Information" is explicitly defined by MA General Law. Data in this category requires the highest level of security and control.

Protected Information : Protected Information is any data that has explicit legal, regulatory, or compliance restrictions for its protection; or any data whose loss, corruption or unauthorized disclosure may impair the core functions of the College, or result in any business, financial, or legal loss.

Sensitive Information : Sensitive Information is any data not explicitly protected by legal or regulatory compliance, but whose unauthorized disclosure may be damaging to the College or our client community.

Unclassified Information : Any information that is not classified as PII, Protected or Sensitive is considered "unclassified" for Information Security purposes, and has no Information Security Program coverage requirements.

5.6) **Data or Records Handlers** :

The classification of specific information is made by the data "**Owner**," generally the head of the department that creates or compiles that information for institutional use.

Data "**Custodians**" are typically department managers with control of classified data, and are responsible for its authorized use, dissemination, storage and life cycle management.

An "**Authorized User**" is anyone who is authorized by the Data Owner or Custodian to access classified information to perform their job function, academic assignment, or fulfill a contractual obligation.

5.7) **Data Security Incident, Data Breach** :

Generally, a ***disruptive* info security incident** is any unexpected or unauthorized change, disclosure of or interruption to Smith College's information resources that could be damaging to our students, staff, faculty, alumnae, donors, parents, prospective students and/or reputation. It also includes any event that has the potential for unauthorized change or disclosure of classified data, such as a system intrusion where the extent of the intruder's activity may not be initially known.

A ***non-disruptive* info security incident** does not render data or services unusable for general use, but is an event where normal controls have been bypassed for some reason, or some other anomalous event has occurred that crosses the general privacy and security goals of the college, such as a policy or legal violation, or a health / safety event where electronic information or metadata may play a role in the event.

A **Data Breach** is *defined by MA 201 CMR 17.00* as : the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth.

6. *Additional Notes :*

6.1 Frameworks Note 1 : **Control domain framework standards**

have been created for general business, government, and other regulated organizations. In general, these frameworks do not readily adapt to the higher education environment, and also require resources that make them impractical for smaller institutions to implement. Information Security Control Domain Framework standards that were reviewed to develop the framework described in this program include: ISO 27001 / 27002, COBIT (v. 4.1, 5.0), NIST SP800-53, and the SANS 20 Critical Controls. Drawing from these framework standards, The Information Security office at Smith has developed the Small Institution Information Security Domain Framework of security control domains to more directly address both the institutional processes and the resources available for a comprehensive and implementable security program. This written program is based on version 5 of the Small Institution Information Security Domain Framework.

6.2 Frameworks Note 2 : The **governance role**

serves to vet security initiatives, parameters and controls to confirm they are in line with the mission of the institution and the direction of senior leadership. *Governance is manifest as any process that allows for issues to be addressed in a timely manor by the correct decision-making entity*, such as a senior staff group, a senior management individual, a governance committee, or some other authoritative resource. The exercise of "governance" may be formal committee acceptance, and equally may be a verbal recommendation from a single individual with the authority to make that decision. The role of governance appears most prominently in the review of the strategic domains of Risk Analysis / Audit, and Policy / Compliance.

6.3 ***Data Classifications*** : in more detail :

PII :

Personally Identifying Information (aka PI) is defined by MA General Law 93H as a person's first name and last name or first initial and last name in combination with any one of the following: Social Security number, or driver's license number, or state-issued identification card number, or financial account number, or credit card number, or debit card number.

Personal Information shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

Protected Information :

Protected Information is data whose loss, corruption or unauthorized disclosure would be a violation of federal or state laws and regulations or institutional contracts (i.e., protected data); Personal Information data; data that involves issues of personal privacy; or data whose loss, corruption or unauthorized disclosure may impair the academic, research or business functions of the college, or result in any business, financial, or legal loss.

Examples: Any data explicitly identified as protected under law; data protected by contract or grant authority, such as grant funded research data; copyrighted information; medical information or personal health information (PHI); staff or personnel information; donor information; account and financial information of the college.

Sensitive Information :

Sensitive information is data whose unauthorized disclosure is not a violation of law, does not impair business or result in a financial loss but may be damaging to our students, employees, or alumnae or to the college's reputation and thus require a higher degree of security than other information.

Examples: a list of donors' names and contributions, a list of employees names and salaries, detailed building plans for buildings that contain secure locations, data network maps, or Board of Trustees notebooks.

For questions about this program, or for additional information, please contact :

Ben Marsden, Information Security Director
Stoddard Hall, Smith College
Northampton, MA 01063
413-585-4479
bmarsden@smith.edu