Business Continuity Plan

Owner: Ho Yeung, Lee

Classification: Secret

FIPS-199 SC administrative information = {(confidentiality, HIGH), (integrity, HIGH), (availability, HIGH)}

Standard: NIST 800-34

Continuity Planning Goals - Documentation use

Project scope and planning

Business impact assessment

Continuity planning

Approval and implementation

Project scope and planning

Business Organization Analysis

* Operational departments that are responsible for the core services the business pro- vides to its clients
* Critical support services, such as the information technology (IT) department, facilities and maintenance personnel, and other groups responsible for the upkeep of systems that support the operational departments
* Corporate security teams responsible for physical security, as they are many times the first responders to an incident and are also responsible for the physical safeguarding of the primary facility and alternate processing facility
* Senior executives and other key individuals essential for the ongoing viability of the organization

BCP Team Selection

* Representatives from each of the organization’s departments responsible for the core services performed by the business
* Business unit team members from the functional areas identified by the organizational analysis
* IT subject-matter experts with technical expertise in areas covered by the BCP
* Cybersecurity team members with knowledge of the BCP process
* Physical security and facility management teams responsible for the physical plant
* Attorneys familiar with corporate legal, regulatory, and contractual responsibilities
* Human resources team members who can address staffing issues and the impact on individual employees
* Public relations team members who need to conduct similar planning for how they will communicate with stakeholders and the public in the event of a disruption
* Senior management representatives with the ability to set vision, define priorities, and allocate resources

Resource Requirements

Legal and Regulatory Requirements

Business Impact Assessment

Identify Priorities

* drawing up a prioritized list that covers the business functions for which their department is responsible.
* the BCP team should sit down and draw up a list of organization assets and then assign an asset value (AV) in monetary terms to each asset. These numbers will be used in the remaining BIA steps to develop a financially based BIA.
* The second quantitative measure that the team must develop is the maximum toler- able downtime (MTD), sometimes also known as maximum tolerable outage (MTO). The MTD is the maximum length of time a business function can be inoperable without caus- ing irreparable harm to the business. The MTD provides valuable information when you’re performing both BCP and DRP planning.
* This leads to another metric, the recovery time objective (RTO), for each business func- tion. This is the amount of time in which you think you can feasibly recover the function in the event of a disruption. Once you have defined your recovery objectives, you can design and plan the procedures necessary to accomplish the recovery tasks.
* The goal of the BCP process is to ensure that your RTOs are less than your MTDs, resulting in a situation in which a function should never be unavailable beyond the maxi- mum tolerable downtime.

Risk Identification - Qualitative

* Violent storms/hurricanes/tornadoes/blizzards Lightning strikes
* Earthquakes
* Mudslides/avalanches
* Volcanic eruptions
* Man-made threats include the following events:
* Terrorist acts/wars/civil unrest
* Theft/vandalism Fires/explosions
* Prolonged power outages
* Building collapses
* Transportation failures
* Internet disruptions
* Service provider outages

Likelihood Assessment

* the likelihood that each risk will occur. To keep calculations consistent, this assessment is usually expressed in terms of an annualized rate of occurrence (ARO) that reflects the number of times a business expects to experience a given disaster each year.
* The BCP team should sit down and determine an ARO for each risk identified in the previous section. These numbers should be based on corporate history, professional experi- ence of team members, and advice from experts, such as meteorologists, seismologists, fire prevention professionals, and other consultants, as needed.

Impact Assessment

Quantitative:

* The exposure factor (EF) is the amount of damage that the risk poses to the asset, expressed as a percentage of the asset’s value. For example, if the BCP team consults with fire experts and determines that a building fire would cause 70 percent of the building to be destroyed, the exposure factor of the building to fire is 70 percent.
* The single loss expectancy (SLE) is the monetary loss that is expected each time the risk materializes. You can compute the SLE using the following formula: SLE = AV×EF
* The annualized loss expectancy (ALE) is the monetary loss that the business expects to occur as a result of the risk harming the asset over the course of a year. You already have all the data necessary to perform this calculation. The SLE is the amount of damage you expect each time a disaster strikes, and the ARO (from the likelihood analysis) is the num- ber of times you expect a disaster to occur each year. You compute the ALE by simply mul- tiplying those two numbers: ALE = SLE × ARO

Qualitative:

* Loss of goodwill among your client base
* Loss of employees to other jobs after prolonged downtime
* Social/ethical responsibilities to the community
* Negative publicity

Resource Prioritization

* create a list of all the risks you analyzed during the BIA process and sort them in descend- ing order according to the ALE computed during the impact assessment phase. This pro- vides you with a prioritized list of the risks that you should address. Select as many items as you’re willing and able to address simultaneously from the top of the list and work your way down

Continuity planning

Strategy development

Provisions and processes

Plan approval

Plan implementation

Training and education

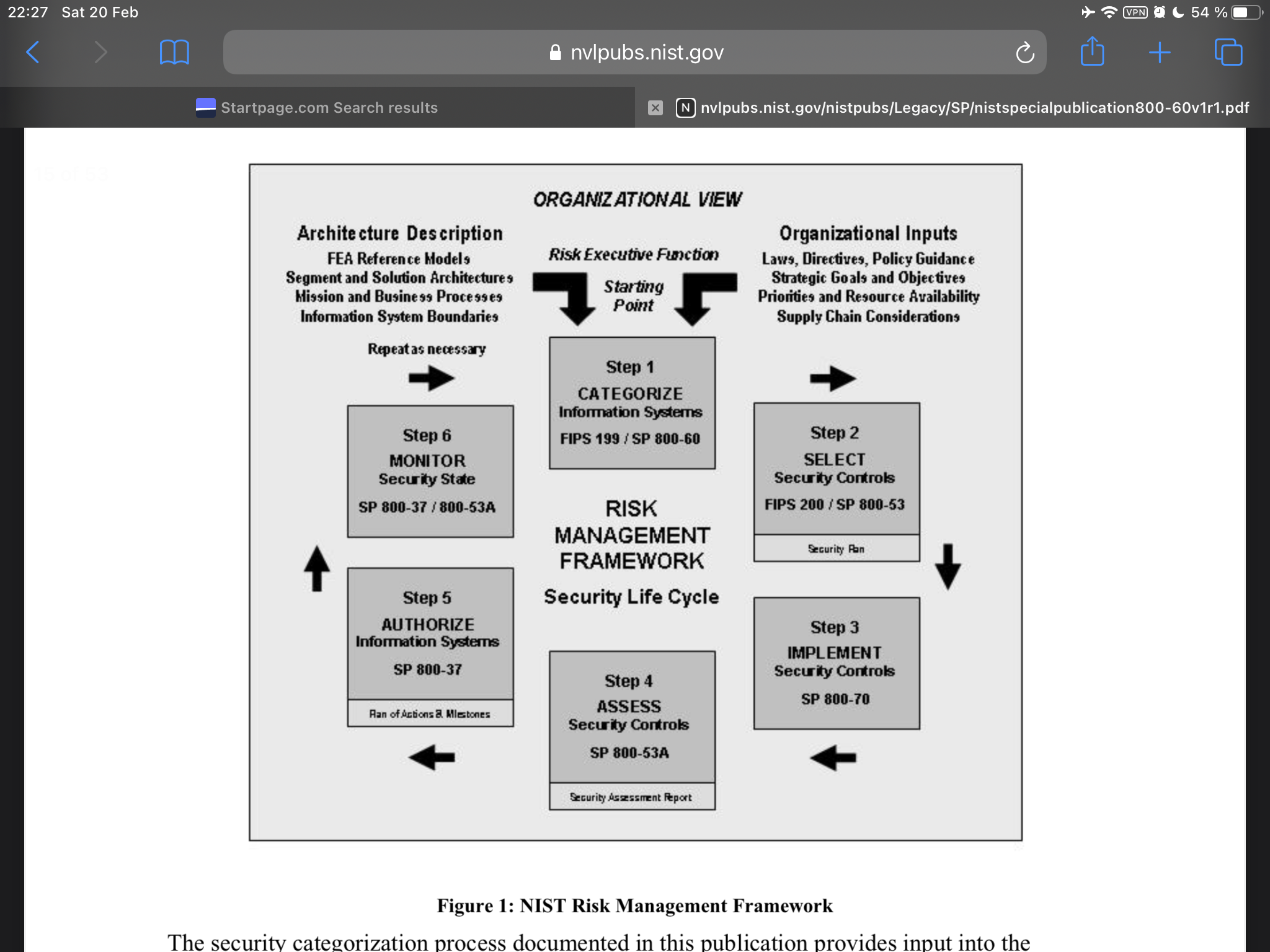
Approval and implementation

Plan approval

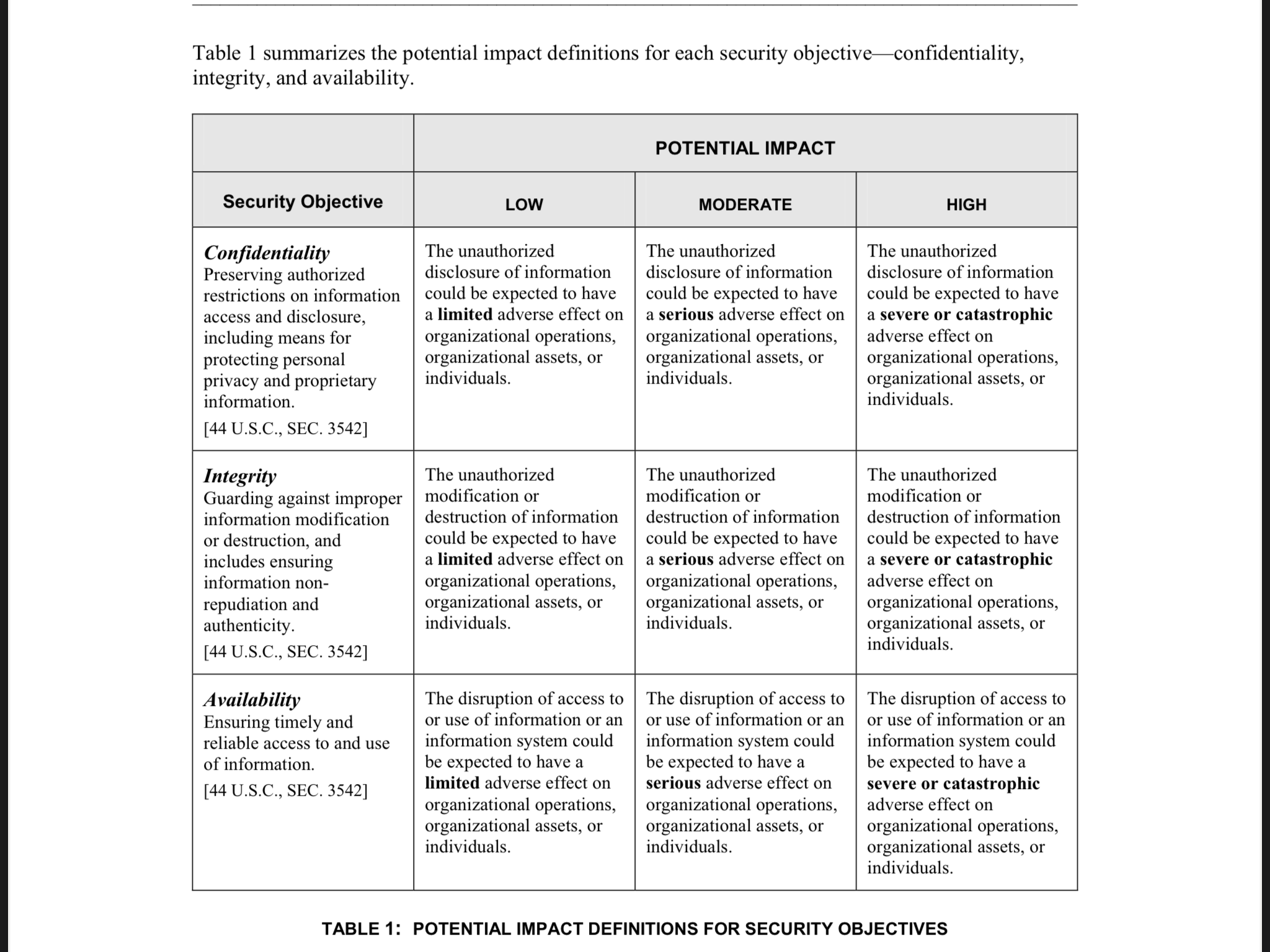
Plan implementation

Risk Acceptance/Mitigation

Appendix

RISK Management Workflow

**Appendix**

**FIPS-199**