SUNWAY

INT’L BUSINESS SCHOOL

Programme Name: **BCS HONS**

Course Code: **CSC 2734**

Course Name: **Information System Security**

Assignment No. **1**

Date of Submission: **4/14/2021**

Submitted By:

Student Name**: Dipesh Tha Shrestha**

IUKL ID: **041902900028**

Semester**: Third Semester**

Intake**: September 2019**

Submitted To:

Faculty Name**: Manoj Gautam**

Department**: LMS**

1. **Describe top-down strategic planning. How does it differ from bottom-up strategic planning? Which is usually more effective in implementing security in a large, diverse organization?**

Answer:

Top-down planning or retrograde planning is an approach that aims to gradually move from the top to the bottom level of a particular hierarchy. The organization's management provides a framework plan with company goals, for example, based on the expected market development and growth targets, which is broken down into sub plans and specified in detail in the subordinate levels of planning. These sub plans in turn serve as outline plans and goals for the subsequent planning levels. In top-down planning, the first global (framework) objectives are defined and ways of achieving them are determined. They are gradually moved to the lower levels of the organizational hierarchy to be developed and specified. This is a divergent approach.

Processing takes place from top to bottom as well as from bottom to top. Other than for planning, these processing methods are also used for defining company goals and the next strategic steps to achieve them.

In top-down processing, the main construction project objectives are defined and the tasks needed to support them are determined. The newly-defined activities are then divided into smaller tasks and spread across the different members of the team to begin their development. In that sense, top-down processing is a diverse approach.

With **bottom-up processing**, things are different as smaller goals are initially defined and activities start from the lower organizational levels of the company. These narrower goals will at a later stage be connected to the primary project goals and strategies, making it a convergent approach.

Traditionally, **top-down planning** involves the clear definition of construction project goals and their division into specific construction job goals, which are dealt with in different construction phases. Sometimes referred to as retrograde planning, top-down planning is a planning approach that focuses on gradually moving from the top to the bottom level of a particular project hierarchy.

The construction project management team usually provides the plan that includes the project goals based on the expectations and targets set by the project owner, the contractor and the rest of the project stakeholders. This construction plan is then broken down into sub-plans of smaller construction jobs and activities and specified in the subordinate levels of planning including detailed jobs for subcontractors. This approach provides a structured control over a construction project.

Bottom-up planning or progressive planning, on the other hand, aims to create a plan at a lower but meaningful level and then progress it to the next level up to the higher project levels. For example, bottom-up planning can focus on a particular desired functionality of a project and the entire build would be based around it.

The planning would start with small-scale organizations and piecing these smaller individual elements together to create a larger and more complex structure. This method would provide a more experimental approach that is open for restructuring and editing based on unpredicted impacts of the design.

Bottom-up planning is usually more effective in implementing security in a large, diverse organization because bottom-up planning can focus on a particular desired functionality of a project and the entire build would be based around it. The planning would start with small-scale organizations and piecing these smaller individual elements together to create a larger and more complex structure. This method would provide a more experimental approach that is open for restructuring and editing based on unpredicted impacts of the design.

2. **List and describe an organization’s three communities of interest that engage in efforts to solve InfoSec problems give three examples of who might be in each community**

Answer:

An organization’s three communities of interest that engage in efforts to solve InfoSec problems are given below:

1) Information Security Community
2) Information Technology Community
3) General Business Community

Explanation:

1) **Information Security Community:** This community protects the organization information assets from many threats they face. Example: This community comprises of the IT Professionals, Chief information security officer, and managers who bear the responsibility to secure the information.
    - **801 Labs Community Hackerspace:** 801 Labs is a Salt Lake City, Utah based hackerspace created by local information technology, electronics, and information security enthusiasts. 801 Labs is a physical space designed to be a center for peer learning and knowledge sharing in the form of workshops, presentations, and lectures
    - **AISA - Australian Information Security Association**; Established in 1999, AISA has become the recognized authority on information security in Australia with a membership of over 6000 individuals and corporate sponsors across the country.
    - **AISP - Association of Information Security Professionals**; they are an independent cybersecurity association that believes in developing, supporting as well as enhancing industry technical competence and management expertise to promote the integrity, status and interests of Information Security Professionals in Singapore.

2) **Information Technology Community**: This community supports the business objectives of the organization by supplying and supporting IT that is appropriate to the organization needs. Examples: IT Professionals, Chief information officer, and managers who acts as providers of information technologies.

    - **Association for Computing Machinery (ACM):** ACM serves more than 75,000 computing professionals in more than 100 countries, with special interest groups (SIGs) on topics ranging from computer architecture to e-commerce. SIGs often sponsor conferences and produce e-newsletters.
    - **Association of Information Technology Professionals (AITP):** With local chapters everywhere from Birmingham to Milwaukee, AITP helps IT executives, academics and students expand their industry knowledge and connect with peers.

- **Association of Shareware Professionals (ASP):** For software developers creating products for use on a "try-before-you-buy" basis, ASP offers members-only newsgroups, help with development and marketing, and ways to connect with shareware brethren.

3) **General Business Community**: This community articulates and communicates organizational policy and objectives and allocates resources to the other group. This community includes: Non-IT Professionals, Users and Managers.
   - **SAP Communities:** SCN (SAP Community Network) epitomizes how a Corporate Social Network can evolve into a highly successful community for conducting Social Business. SCN has more than 2.5 million active members -- it's the largest aggregation of SAP customers, experts, partners and industry thought leaders anywhere. SAP's goal with SCN is to help customers maximize the value of their IT investments in ways that couldn't have been done without it -- and for this year, we're honing in on the aspects of social innovation, social intelligence and social commerce.
   - **Pitney Bowes Customer Support Forum:** The Pitney Bowes online customer forum is a powerful extension of our multichannel (including mobile) strategy to manage customer relationships. By creating a platform where engaged customers can help one another, and a much larger pool of customers can benefit from that exchange, Pitney Bowes can provide unique value. Forum participants also benefit from exclusive content we provide through this channel, which gives them an added incentive to visit the site and learn more.
   - **General Electric MarkNet (Internal):** GE's laser focus on innovation is how they have connected 8,000 global marketers together in one community called MarkNet. The purpose of this community is to accelerate innovation and improve knowledge sharing among their corporate marketers and set the gold standard for B2B marketing."

3. **Why is identification of risks, through a listing of assets and their vulnerabilities, so important to the risk management process?**

Answer:

Risk identification is the process of determining risks that could potentially prevent the program, enterprise, or investment from achieving its objectives. It includes documenting and communicating the concern. Risk identification is the process of identifying and assessing threats to an organization, its operations, and its workforce. For example, risk identification may include assessing IT security threats such as malware and ransomware, accidents, natural disasters, and other potentially harmful events that could disrupt business operations. Companies that develop robust risk management plans are likely to find they're able to minimize the impact of threats, when and if they should occur.

The objective of risk identification is the early and continuous identification of events that, if they occur, will have negative impacts on the project's ability to achieve performance or capability outcome goals. They may come from within the project or from external sources. Risk management is important because it allows a business to control – and often times prevent – the financial, political, social and cultural ramifications associated with risks. Not only does risk management allow a business to identify potential risks ahead of time, it also allows a business to react accordingly and minimize or even prevent losses. Without identifying risks using risk management, a business cannot successfully define objectives. By minimizing or even eliminating risks, a business should see an increase in productivity by now wasting time and resources, as well as protection from any possible legal repercussions.

There are multiple types of risk assessments, including program risk assessments, risk assessments to support an investment decision, analysis of alternatives, and assessments of operational or cost uncertainty. Risk identification needs to match the type of assessment required to support risk-informed decision making. For an acquisition program, the first step is to identify the program goals and objectives, thus fostering a common understanding across the team of what is needed for program success. This gives context and bounds the scope by which risks are identified and assessed.

There are multiple sources of risk. For risk identification, the project team should review the program scope, cost estimates, schedule (to include evaluation of the critical path), technical maturity, key performance parameters, performance challenges, stakeholder expectations vs. current plan, external and internal dependencies, implementation challenges, integration, interoperability, supportability, supply-chain vulnerabilities, ability to handle threats, cost deviations, test event expectations, safety, security, and more. In addition, historical data from similar projects, stakeholder interviews, and risk lists provide valuable insight into areas for consideration of risk.

Risk identification is an iterative process. As the program progresses, more information will be gained about the program (e.g., specific design), and the risk statement will be adjusted to reflect the current understanding. New risks will be identified as the project progresses through the life cycle.

The important advantage of risk identification is that it helps completely analyze and find out what risks need to be addressed which are based on likelihood and impact. Then they are quantified according to cost or the right time to address them.

Another advantage is risk identification requires the knowledge of the full scope of a project which helps to think thoroughly about it and weigh the pros and cons well in time. It helps while devising mitigation strategies to control the risks.

All risks that are identified can be resolved with a plan without compromising with the objectives of the project and the end result required. All the assumptions can be listed down and analyzed strategically, one at a time. The analysis helps in removing potential inaccuracies at the beginning of the project itself.

Therefore, the above paragraph shows the important of identification of risks, through a listing of assets and their vulnerabilities to the risk management process