Discussion-2 circumstances where risk control strategies and-or risk acceptance strategies apply

Discussion Topic:

Risk acceptance and risk control are two strategies that organizations utilize to deal with risk. Risk control focuses on eliminating, reducing, or mitigating risk, while risk acceptance strategy determines and specifies the level of risk that an organization is willing to accept. As one can imagine, it is not possible to prevent or protect against all risk.

Taking into consideration the material from this module, under what circumstances should risk control strategies and/or risk acceptance strategies be applied?

My Post:

Hello Class,

Risk control strategies should be applied when trying to manage and reduce threats (uCertify , n.d.a). For example, when an organization wants to prevent a vulnerability from being exploited, this concept is defined as a defense or avoidance strategy. This can be implemented by countering threats, by just removing the vulnerability, by limiting access to the system, or by adding safeguards such as digital firewalls for digital assets/systems or heavy steel fire doors/dead-bolt locks for physical assets/systems.
Risk control strategies can also be applied when an organization wants to shift the risk to another organization. This concept is defined as a transferal strategy, and it is when an organization transfers risk, such as the responsibility for maintaining a network or protecting a building, to another organization, or purchasing insurance to cover losses from incidents such as a fire or flood.
Additionally, risk control strategies can be applied to mitigate risks after an incident or damage has already happened, or when an organization decides that an asset/system that did require protection no longer requires it.

Risk acceptance strategies should be applied when it is impossible to eliminate all risks, and the occurrences of these risks are acceptable. It is a strategy that involves deciding to do nothing to protect a specific asset from risk and simply accepting the outcome (uCertify , n.d.b).
Risk acceptance strategies should be applied, for example, when a cost-benefit analysis (CBA) determines that the cost of controlling the risk outweighs the value of the asset/system being protected.
Or, when vulnerabilities have a low probability of occurrence or the result of their occurrence has a low impact.
Additionally, risk acceptance strategies should be applied when the costs of mitigating or transferring the risk (to another organization) are too expensive for the organization.

A combination of risk control and risk acceptance strategies can be applied when an organization implements (risk) controls to reduce a risk; however, afterward, a residual amount of risk remains that cannot be managed by the risk controls, but this residual amount of risk is acceptable.
In other words, most risk controls (strategies) do not eliminate 100% of a risk, and the remaining amount of risk is known as residual risk (uCertify , n.d.b). Then, an organization can choose to accept the residual risk if it aligns with the organization's risk appetite or tolerance, or apply more controls.

-Alex

References:

uCertify (n.d.a). Lesson 3: Integrated Information Risk Management. *(ISC)² SSCP Certification Training Guide. uCertify*. ISBN: 976164493776.

uCertify (n.d.a). Lesson 4: Operationalizing Risk Mitigation. *(ISC)² SSCP Certification Training Guide. uCertify*. ISBN: 976164493776.