Risk Acceptance Process [1]

Background

So that the University of Colorado is able to fulfill it fiduciary responsibilities it is critical that all employees and affiliates comply with University information security policies, procedures, standards and guidelines. Additionally, when the University is aware of a risk to information assets it is imperative that the University exercise positive control to manage risk. However, there are circumstances that fall outside the ability to conform to a University policy, procedure, standard or guideline or mitigate risk. In such instances, the risk must be documented and approved.

Process

The risk acceptance form is to be used in instances where the institutional risk is likely to exist for more than three (3) months and a risk analysis has been performed, identifying the potential impact of the risk as high to the University. The potential impact is high if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (1) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (2) result in major damage to organizational assets; (3) result in major financial loss; or (4) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

CU uses the following as guides for defining impact:

- Financial – direct or indirect monetary costs to the institution where liability must be transferred to an organization which is external to the campus, as the institution is unable to incur the assessed high end of the cost for the risk; this would include for e.g. Use of an insurance carrier
- Reputation – when the impact results in negative press coverage and/or major political pressure on institutional reputation on a national or international scale
- Safety – when the impact places campus community members at imminent risk for injury
- Legal – when the impact results in significant legal and/or regulatory compliance action against the institution or business.

The risk analysis must be documented by a written risk assessment, prepared jointly by the responsible department and campus information security officer. Only an Administrative officer, director, or department chair can accept risk.

If the risk acceptance involves an exception from the University Information Security Program APS or Office of Information Security procedures, standards, or guidelines the Chief Information Security Officer must sign the acceptance form. If the risk acceptance involved an exception to campus policies, procedures, standards, or guidelines then the campus information resource oversight authority must sign the risk acceptance form. If regulatory compliance obligations exist the appropriate University compliance authority must also approve the acceptance.

All risk acceptance decisions shall be presented to the Security Advisory Committee for review.

Attachments:
risk-acceptance-template.docx [2]
Groups audience:
Office of Information Security

Links
[1] https://www.cu.edu/security/risk-acceptance-process [2] https://www.cu.edu/doc/risk-acceptance-templatedocx-1