*Setting a **Higher Level of Excellence** in Information Security & Compliance Services.*

We Accept the Risk | by Kyle Stelly, CISSP PCIP

Whether you find them in a risk assessment, we find them in an audit, regulators uncover them as part of an exam, or you hear something scary and familiar on the news, IT risks require ACTION. There are generally four things you can do once a risk is identified within your environment:

- Avoid it. No one likes being told, *"You can't do that. It's too dangerous."* Risk avoidance is when management determines that the risk outweighs the benefit of an asset (like a product offering, practice, or IT system) and decides not to go forward with implementation. Avoidance is much more palatable when it occurs in an asset's evaluation phase, but occasionally must be considered for a risky existing asset. Taking something away from customers or employees never gets a great response but is sometimes necessary.
- Mitigate it. Fix the problem or slap on some compensating controls to reduce the risk, test it, and you're ready to go! Auditors and examiners love to see this route taken, especially if the "test it" portion is well-documented.
- Transfer it. Often, risk transference is associated with insurance policies that pay-out if the risk is realized, but that's not the only way. Outsourcing a system or process to a third party is also a form of transference, but beware; that can present a whole new set of risks. (A risk at a third party that affects you or your customers is still your risk. Plus, you will then have to take that additional risk responsibility into account during vendor management reviews.)
- Accept it. Sometimes this option makes sense for risks that have exorbitant cost or complexity to mitigate, are uninsurable because the affected system is managed/hosted by a third party, or avoidance is an unreasonable consideration. Many think risk acceptance means *"do nothing,"* but there's a lot more that should go into this process...

When it comes to accepting IT risk, or any risk for that matter, the first step should be a consultation of your organization's Risk Management Policies. That already covers the risk acceptance process, right? It should, and if it doesn't, here's a brief policy starter:

Occasionally, management may choose to accept risks identified in audits, exams, and assessments due to infeasibility of implementing mitigating controls or when there is a foreseeable change that may consequentially reduce or eliminate the risk. Such a decision by the Board of Directors will not be entered into lightly and will factor details of the associated risk, provisions of associated transference controls, challenges of mitigation, and additional interpretations by the Information Security Officer. All risk acceptance activities will be formally communicated to and authorized by the Board, and associated documentation will include an expiry date of all acceptances that will prompt management to revisit and represent the risk at a future date with information on current applicability and mitigation feasibility.

Now that you have a policy, let's use it as a guide for the next steps of the IT risk acceptance process.

Present your case to stakeholding management, ideally the Board of Directors or a committee with Board member participation. Explain the purpose of the affected asset, how the risk was identified, a conservative estimation of potential impacts if the risk were realized (reputational damage, data breach, monetary loss), likelihood of realization, what's been done for mitigation so far, and what remains to be done. In conclusion, presenters may wish to recommend a course of action. (i.e., Avoid. Mitigate. Transfer. Accept.) This presentation should be given jointly by internal subject matter experts and the Information Security Officer.

Prior to or just following this presentation, documentation that highlights details from the presentation (often in the form of a risk assessment or action document) should be provided to stakeholding management where their chosen response is recorded. If they choose to accept the risk, a Board-signed document of acceptance should be produced and include an expiration for when the risk is to be reassessed and represented. In lieu of a formal *document of acceptance*, Board minutes of a risk acceptance should suffice.

Be sure that risk acceptance expirations are addressed and documented. Circumstances change over time. An advanced feature that would provide better authentication to your online banking platform may cost $20,000 today; however, next year it may be built in and included by default. As time progresses and assets or controls evolve, accepted risks should be re-evaluated during normal risk assessment cycles and on or before their date of expiration to determine if acceptance is still the most reasonable action. If acceptance is still the right choice, the process (and associated documentation!) should be repeated.