Fred Cohen & Associates - Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Change management: How should I handle it?

Changes are handled differently by different enterprises in different environments, depending on situational risks and program maturity. As a starting point, table 1 provides guidance as to when to use what approach to change management in information protection.

Risk	*Maturity*	*Change approach*
Low	Initial-	Just let change happen and hope you can handle it.
Low	Repeatable+	Make backups before changes in case you have to revert.
Medium	Initial-	Initial is not mature enough to operate at medium risk - increase maturity level
Medium	Repeatable or Defined	Make backups before changes in case you have to revert.
Medium	Managed+	Based on risk management and executive decision-making, Use change control prior to changes but move forward and count on your expertise to make it work **OR** Use sound change control with full reversion capabilities **OR** Make backups before changes in case you have to revert.
High	Defined-	Do not operate at high risk with this level of maturity.
High	Managed+	Use sound change control with full reversion capabilities.

Table 1 - What change management approach to take

As the risk increases, the need for stronger change control also increases. But when the change control scheme exceeds the capabilities of the maturity level of the organization, it creates significant overhead and cultural challenges. For example, for high risk situations where the maturity is Defined or lower, we advise that the risk be avoided by not operating in this mode. Similarly, when the risk is Medium and the maturity level is Initial or less, we advise against operation. For more information on maturity levels, look in the Standards section of the Library at http://all.net/. When the maturity level is commensurate with the risk, change management approaches identified here are reasonably suited to the need.

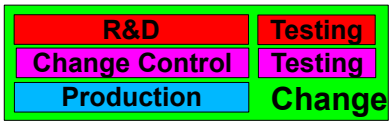
Just let change happen and hope you can handle it

Fast and loose is often the best approach for smaller businesses or for portions of businesses where risks are low. The cost of sound change control is often on the order of twice the cost of not having it, so low risk and low cost make sense together.

Make backups before changes in case you have to revert

Backups are used to provide a modicum of recoverability, and changes are made with the knowledge that reversion is, at least theoretically, possible. In reality, reversion is often problematic if sound change control is not used in the first place.

Research and development separated from change control separated from production, testing at each step



This is the standard approach taken across industries and over a long time frame. It uses independent testing to enforce separation of duties as well as to verify that the changes don't break operational systems. The most commonly experienced problem with this approach is that it takes substantial amounts of time to make changes.

Use change control without reversion and count on your expertise to make it work.

In forward-only environments, such as financial transaction systems, many enterprises choose to never go back once a substantial change is made. This means that they accept the risk of failure and save the cost of full reversion. It places additional pressure on testing and process to get it right, and means that experts have to be available to deal with the issues if and when they arise, and in real time. This "fast but not loose" approach is an risk tradeoff that, in highly professional organizations, seems to work reasonably well. There are starts and fits from time to time, but if properly managed, these don't produce unnecessary internal friction. Rather are knowingly accepted as a cost of doing business at this rate of change.

Use sound change control with full reversion capabilities

Sound change control implies:

- A system for requesting, specifying, implementing, testing, and implementing changes,
- A method for tracking and backing out of changes,
- Separation of duties between research and development, testing, change control, and operations,
- Databases that track these different elements of the process,
- Approval processes and work flows to assure operational execution,
- Integration of changes into the detection and response process to prevent false positives and potentially harmful responses,
- Notification of audit so they can adapt their auditing to meet the new requirements,
- Updated documentation to reflect operational changes and user changes,
- Training to adapt the people to the changes,
- HR and legal approval of changes impacting those areas, and
- Policies, standards, and procedures must be followed along the way.

Summary

The consequences of failures and management risk tolerance are used to select from a range of reasonable alternatives for change management, as long as risk doesn't exceed maturity.