G00211189

Understanding IT Controls and COBIT

Published: 28 March 2011

Analyst(s): George Spafford

IT organizations seeking to deliver predictable IT services to enable the business are also confronted with the need to comply with government regulations, meet contractual obligations and better manage risks in general. They can benefit by better understanding how effective and efficient controls can help make these things possible.

Key Findings

- Risks cause variations in outcomes that IT must deal with through the implementation of appropriate controls.
- IT organizations are not effectively leveraging controls to create more-predictable services.
- There are three broad categories of controls (preventive, detective and corrective) that can be layered to mitigate risks.

Recommendations

- Leverage controls to reduce variation and deliver IT services that more predictably meet the needs of the business.
- Use layers of controls to have more options in terms of resulting effectiveness, efficiency and economy.
- Leverage COBIT for guidance on controls that can help mitigate risks and reduce variation.

Analysis

Often, we hear IT auditors and information security personnel discussing controls, but not always with a succinct definition. We can think of a control as something done to mitigate some broad type of foreseen risk. The need to reduce variation and have predictable outcomes is something that IT as a whole, including infrastructure and operations, is very concerned about. To design and deliver reliable services that meet the needs of the business necessitates understanding not just people,

process and technology, but also how controls are leveraged to mitigate risks, including operational risks.

Understanding Controls

To set levels, controls are designed and implemented with organization-specific "process wrappers," to better manage various types of risks and reduce the level of risk left after mitigation (known as residual risk) to a level that management deems acceptable. This is an important distinction — controls do not eliminate risks; they mitigate, or reduce them, to a level that management identifies as acceptable.

Broadly speaking, there are three categories of controls, and each can be further segmented in terms of being automated or manual:

- **Preventive controls.** These controls are intended to proactively mitigate the occurrence and/or impacts of risks. Examples include policies and procedures, because they are authored, approved and implemented by management preemptively to avert foreseen risks. Workflow tools can help automate these controls.
- **Detective controls.** These controls operate after the fact to identify if a predefined event occurred. Activities such as log file reviews, or scanning current configurations for unauthorized changes and to better enable incident and problem management, are detective in nature. It should be noted that data from detective controls can feed predictive analytics tools and processes to enable preventive controls.
- **Corrective controls.** These controls are tasked with restoring the current state to an approved state. It may be that a hacker has compromised a system or something has impaired data integrity. Examples include restoring a system and corresponding data from a backup service, or reloading a system image.

Diminishing Returns

Controls tend to follow a diminishing returns curve, where, at a certain point, the returns for each unit of investment becomes less and less. This is part of the trade-off that management must understand. At some point, accepting the level of residual risk may make more business sense than continued mitigation, because the total costs to reduce the risks further may not be justifiable. Spending $100,000 to avoid a risk that could cost $10 is an extreme example, and perspectives will vary. This is known as management's risk tolerance — the amount of risk that management is willing to accept in terms of the organization's goals, and necessary conditions to the goals, including brand reputation, human factors, customer satisfaction, etc.

For some in IT, controls are viewed as burdensome overhead. When designed and implemented correctly, the value of more-predictable outcomes must justify the cost. In some cases, the design of a single control can only be modified to a certain extent until diminishing returns are experienced. Also, in certain cases, the use of multiple layers of controls can be used to more effectively and efficiently mitigate risks.

Layered Controls

Multiple overlapping controls designed to mitigate one or more risks can be implemented in an approach known as layering. An effective and efficient layered-control design uses intentional combinations of preventive, detective and corrective controls to mitigate risks. In addition to potential improvements in effectiveness, appropriately designed and implemented layered controls may present opportunities for lower implementation costs and may prove less burdensome than a single control.

From a process maturity perspective, immature processes can be defined without adequate controls, and, therefore, may not always meet objectives. As organizations and their processes mature, so does their utilization of controls to achieve more-predictable results.

The concepts covered thus far provide an opportunity to look at risks from an operational perspective, and how layered controls provide more mitigation options than a single control alone. To help illustrate controls and how they can be layered, Table 1 provides some sample risks and control measures.

Table 1. Examples of IT Operational Controls

Risk	Preventive	Detective	Corrective
Excessive heat causing premature component failure	▪ Data center designed with power and cooling requirements in mind ▪ Hardware standards defined, and with power and cooling in mind ▪ Policy requiring temperature probes in zones and cases	▪ Analysis of zone probe data logs for trends ▪ Analysis of server/ chassis probe data logs ▪ Alert and alarm threshold triggers for operator intervention	▪ Reroute air flow. ▪ Implement liquid-based cooling. ▪ Reconfigure hardware to a lower density.
Uncontrolled changes negatively impacting availability	▪ Change management policy ▪ Defined roles and responsibilities ▪ Job descriptions reflect change management compliance as mandatory ▪ Performance reporting includes change management compliance, as well as exception metrics	▪ Configuration integrity tool used to compare current state to approved state, and to flag exceptions ▪ Root cause analysis performed based on trend data and after major incidents	▪ Use tools to restore systems to an approved state. ▪ Take disciplinary action with staff that intentionally chooses to bypass the change management process.
Unmanaged demand exceeding capacity causing availability and performance problems	▪ Design and implementation of a capacity management process ▪ Staff and budgets allocated to perform capacity management ▪ Formal meetings between business and IT to review upcoming capacity requirements	▪ Analysis of historical utilization ▪ Comparison of expected to actual utilization ▪ Alert and alarm threshold triggers for operator intervention	▪ Provision additional capacity following defined processes. ▪ Reallocate jobs to reduce demand during problem period. ▪ Utilize demand management to influence consumption of IT resources.

Risk	Preventive	Detective	Corrective
Projects failing to deliver on time, within budget and with expected features	▪ Implement program management ▪ Implement project management ▪ Staff and budgets allocated for formal oversight of programs and projects ▪ Definition of meetings and reports to gauge the health of projects	▪ Review of progress reports ▪ Review of risk reports ▪ Review of project change requests ▪ Weekly or on-demand reports provided to stakeholders	▪ Follow corrective action process to evaluate the problem(s) and implement corrective actions.
Hardware failure causing availability problems	▪ Defined hardware standards ▪ Definition and implementation of procurement processes and vendor management ▪ Design and implementation of hardware refresh programs	▪ Review of case temperature logs ▪ Review of power consumption logs ▪ Review of hardware aging logs ▪ Review of incident logs for trends via problem management	▪ Replace outright failed hardware. ▪ Replace hardware with an unacceptable probability of failure to return to a predictable operations state.
Sales data loss or corruption negatively impacting the business	▪ Backup and restoration policies and procedures ▪ Investment in appropriate technology ▪ Training conducted on tools and processes ▪ Routine formal testing to validate that restoration is still feasible	▪ Review of backup job logs to ensure there weren't any problems ▪ Review of administrator daily log sheet to validate that log review was performed	▪ In the event of data loss or corruption, data/ images will be restored per policy.

Source: Gartner (March 2011)

Similarly to the way that people learn throughout their careers that things can go wrong, the designers of processes and managers responsible for stable operations can utilize controls to better manage variation introduced through risks. The challenge is to better-understand what controls are, and have a method to organize and methodically audit for compliance, effectiveness, efficiency and economy. COBIT is a controls framework that personnel tasked with the management of controls and processes can leverage.

Leveraging COBIT

The Information Systems Audit and Control Association (ISACA) was formed in 1969 by auditors concerned about information systems. In 1996, ISACA released the first version of COBIT to assist auditors. It is now in v.4.1, with a new release planned for later in 2011.

As information security and operations staff interacted more with auditors, there was a realization that controls and control theory could benefit all areas, not just auditing. Thus, there is a growing awareness that COBIT can help management gain better control of IT through the improved management of risk.

COBIT v.4.1 is organized in four broad domains:

- **Plan and Organize (PO) —** controls that help IT enable and protect business objectives. In turn, outputs from PO are inputs to the next two domains. Examples include:
  - PO1: Define a strategic IT plan.
  - PO2: Define an information architecture.
- **Acquire and Implement (AI) —** controls that are tasked with converting the strategy and tactics from PO into new and changed IT services that are then integrated with the business. Examples include:
  - AI1: Identify automated solutions.
  - AI2: Acquire and maintain application software.
- **Deliver and Support (DS) —** controls involving the actual delivery and operations of IT services. Examples include:
  - DS1: Define and manage service levels.
  - DS2: Manage third-party services.
- **Monitor and Evaluate (ME) —** controls that are used to assess the performance of IT processes. Examples include:
  - ME1: Monitor and evaluate IT performance.
  - ME2: Monitor and evaluate internal control.

Within each of these domains are high-level controls, and within each high-level control are detailed control objectives that can be leveraged during the design of processes. For each high-level control

objective, there are definitions of inputs, outputs, goals, metrics and responsibilities via a responsible, accountable, consulted, informed (RACI) chart and a maturity model.

As with all frameworks, clients must pragmatically leverage COBIT to address the needs of the organization. The goal isn't to adopt COBIT, but to use COBIT as a reference to improve the controls and processes of the organization so that goals can be better-pursued. IT staff tasked with process improvement should develop knowledge about controls and COBIT, and how they can be used to benefit the organization.

Bottom Line

IT organizations seeking to better manage risks to have more predictable enablement of the business will benefit by better understanding controls and how to embed them in processes. COBIT is a mature control framework that provides a wealth of guidance that organizations can draw from as part of their quality improvement efforts. To improve knowledge about controls and COBIT, IT organizations can pursue training, hire experienced staff, attend industry events, etc.

Regional Headquarters

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600