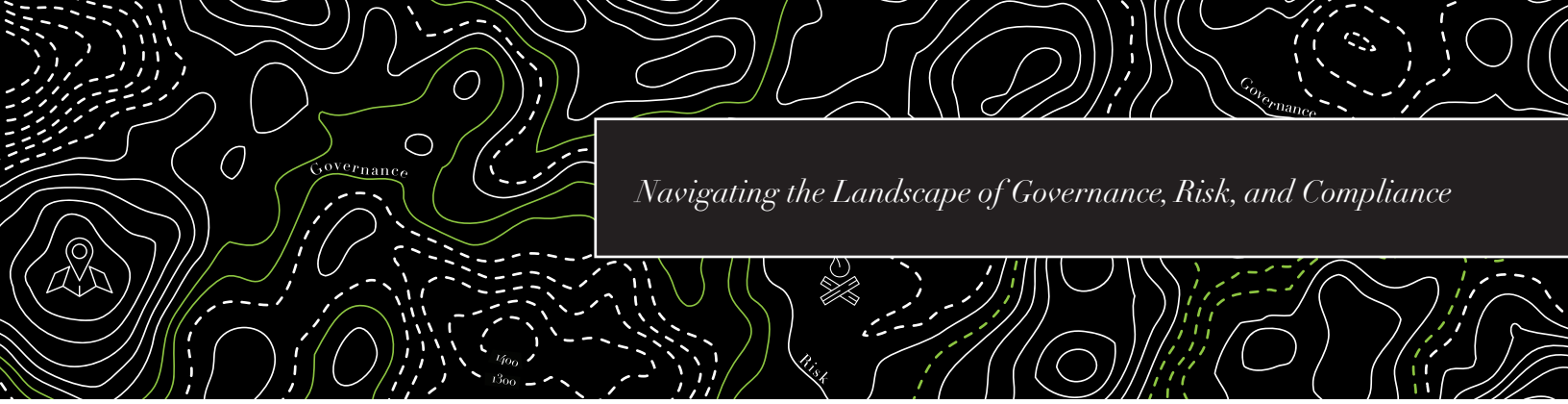


Navigating the Landscape of Governance, Risk, and Compliance

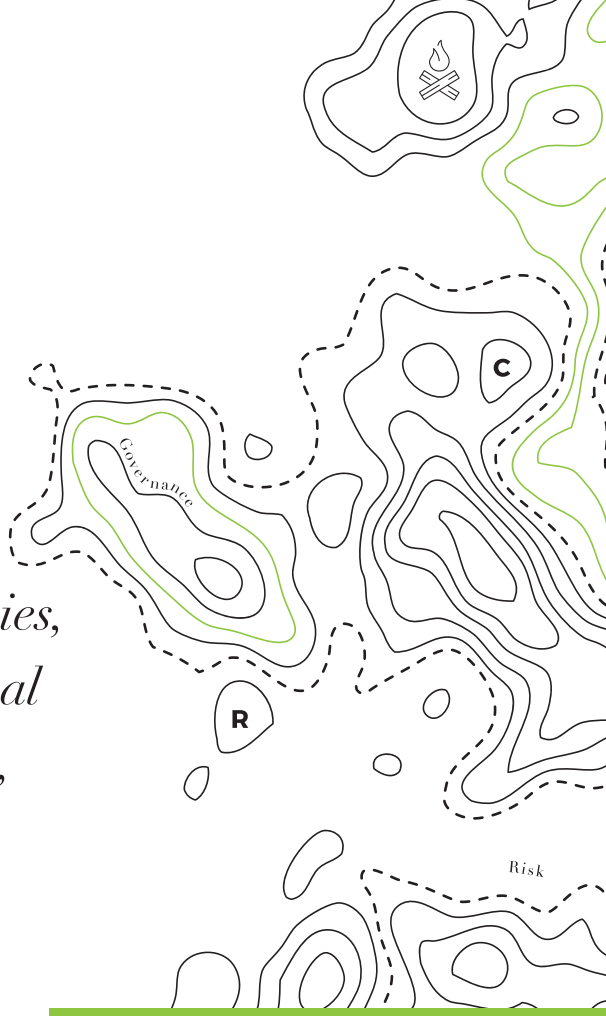
FRAMEWORK
NAVIGATING THE GRC LANDSCAPE

Whitepaper

Controls driving policies and policies inspiring processes

Jason P. Smith
BUSINESS DEVELOPMENT

https://www.linkedin.com/in/jason-p-smith-1999bb87



"This is out of control!" I've only heard this exclamation once in a real world setting with a positive connotation attached, and even then the cops soon showed up and made everyone go home. Control is a highly valued commodity in today's world. However, ask the average person to define control and you are likely to receive a wide variety of answers. ISACA defines control as:

"The means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of an administrative, technical, management, or legal nature." [1]

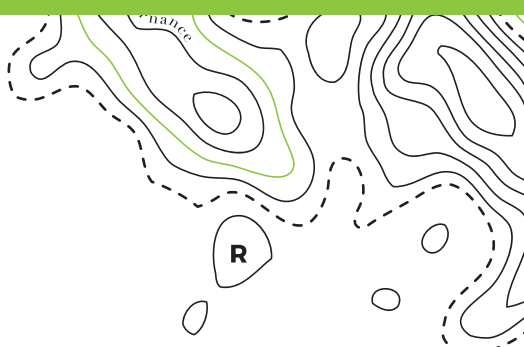
Control is expansive, but at its core, control is everything we do to accomplish our objectives. Controls are the guiderails that keep organizations on the productive path and away from risky detours.

Controls drive our policies and our policies inspire our processes. In other words, our controls are the root causes of what we do and how we do it. There are three commonly accepted types of controls and we all use them every day.

When I was eleven years old, I got my first compact disc, "Cooleyhighharmony" by Boyz II Men. I've always been a bit of a romantic. I kept it in its thick plastic case and in my top dresser drawer, under my stereo and out of reach of my younger brother, **a preventative control.** That way I knew it was safe until I needed to close my door and practice my sweet dance moves or heartfelt ballad singing in the mirror. Whenever my brother had friends over, my mom would help me keep an eye on my room and alert me if any prowlers put the sweet sounds of "Motownphilly" in jeopardy,**a detective control.** Despite my best efforts, the cd eventually went missing, undoubtedly at the hands of a true music connoisseur, and I had to purchase another copy, **a corrective control.**

Types of controls:

- **PREVENTATIVE**
  the purpose of this control is to prevent deviations that could have negative effects
- **DETECTIVE**
  the purpose of this control is to discover deviations that have occurred, so they may be addressed and their effects minimized
- **CORRECTIVE**
  the purpose of this control is to restore things to their pre-deviation state



If putting controls into practice is something we do instinctively, even as children protecting our valuables, why would our organizations operate any differently?

They shouldn't, but having adequate controls in place is something that is often talked about, but rarely practiced. Fortunately, three questions can help us determine if our current controls are effective.

How to identify effective controls

Do they help maintain compliance?

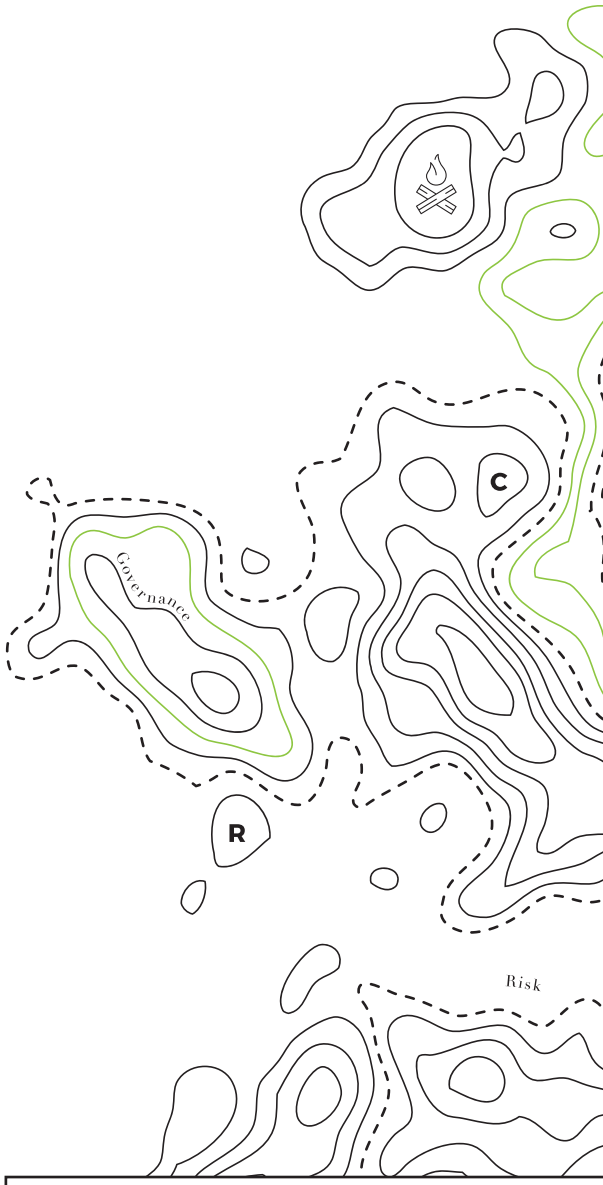
Effective controls equal less audit preparation and fewer audit findings because they affect all IS related activities. In fact, the IS Auditing Guideline states, "Weak management and monitoring of IS should alert the IS auditor to the possibility of a high risk that the controls designed to operate at the detailed level may be ineffective."[2]

Do they mitigate risk by preventing and quickly identifying deviations?

Effective controls are automated where possible, leaving less room for human error and less opportunity for a deviation to occur. In a 2007 ISACA journal Mukul Pareek explains, "...that while cost savings are an important outcome from automating controls, the longer-term benefit is obtained from improved risk management that comes from transparency of processes, visibility of exceptions, access to past events that are logged electronically and ease of implementation of management's governance directions."[3]

Do they allow corrective changes to be easily implemented?

Effective controls allow changes to be made more often, accurately reflecting the organization's strategy; and with fewer failures, resulting in less downtime. In his article, "Tips for Classifying Risk Controls", Leighton Johnson defines corrective control as, "...designed to limit the extent of any adverse event and usually is used and deployed in conjunction with detective controls. These controls are intended to limit the extent of any damage caused by an incident."[4] Obviously, faster, more accurate implementations go further to limit damage incurred by deviations.



To learn more call
1 844 FRAMEWK or visit
framework.juvotec.com

1. ISACA Glossary of Terms, ISACA Knowledge Center 2015, retrieved 05 February 2016 from www.isaca.org/Pages/Glossary.aspx
2. G11 Effect of Pervasive Controls, ISACA IS Auditing Guideline 2008, retrieved 05 February 2016 from www.csb.uncw.edu/people/ivancevichd/classes/MSA%20516/Extra%20Readings%20on%20Topics/COBiT/Effect%20of%20Pervasive%20IS%20Controls.pdf
3. Mukul Pareek, CA, "Automating Controls", ISACA Journal 2007 Volume 3, retrieved 05 February 2016 from http://www.isaca.org/Journal/archives/2007/Volume-3/Pages/Automating-Controls1.aspx
4. Leighton Johnson, CISA, CISM, CIFI, CISSP, "Tips for Classifying Rick Controls", ISACA Newsletter 2014 Volume 22, retrieved 05 February 2016 from http://www.isaca.org/about-isaca/-isaca-newsletter/pages/at-isaca-volume-22-22-october-2014.aspx