David Wagle

School of Business, Northcentral University TIM-7040 V3: Technology Policy and Strategy Dr. Dani Babb

Jul 25, 20121

# Introduction

Information technology became linked to corporate governance due to the prominent role that it played within the realm of corporate finance and accounting (Holder et al., [2016;](#_bookmark3) Li et al., [2007).](#_bookmark4) Evaluating how well governance structures work in practice often utilize some form of maturity model or scoring matrix. This practice originated with ideas promulgated by Richard Nolan of Harvard University in 1973 (Nolan, [1973).](#_bookmark6)

Development on maturity models continued with military support, and a partnership between IBM, Carnegie-Mellon’s Software Engineering Institute, and the US Air Force. The end result was the Capability Maturity Model framework published in the late 1980s and extended in the early 1990s (Caralli et al., [2012).](#_bookmark1) The goal of such frameworks is to have an objective rubric to measure the quality and maturity of a governance policy.

Today it is common practice to utilize such systems and many have been developed.

# Proposed Policy Measurement matrix

In developing a matrix to evaluate a policy, one of the first decisions is what scale should be utilized for responses. The eponymous Likert [(1932)](#_bookmark5) scale, is one of the most widely used measurement scales in the social science, and seems appropriate for measuring maturity and effectiveness of a governance policy, as each statement can be categorized easily into: “never or rarely,” “infrequently” “neutral or not applicable,” “sometimes,” and “almost always or always” or some variant of that phrasing.

# Description of the Evaluation Matrix

The evaluation matrix is based on a few simple assumptions. The first is that governance is primarily a process management activity (Wilkin & Chenhall, [2020).](#_bookmark7) Thus, considerations common to quality process management are considered. Does the policy have an owner? Are the stakeholders known? Etc. Similarly, questions about the scope,

enforcement, exception paths, and monitoring are asked. As with any business process, if these elements are unclear, there is little reason to suspect that the outcomes will be as valuable as the business leadership might hope. Finally, there are questions regarding the regularity of review, if the policy considers legal and regulatory demands, it’s availability to those to whom it applies, and the frequency of updates. While relatively minimal, this short questionnaire provides a sound evaluation of the overall health and maturity of a policy.

# Example Application of the Matrix

Applying the matrix developed in the appendix to the Accenture, PLC Policy 0057 “Acceptable Use of Information, Devices, and Technology” (h[ttps://policies.accenture.com/policy/0057)](https://policies.accenture.com/policy/0057) we find that it scores reasonably well, achieving a score of 60 out of a total of 65 possible points. or just over 92%. Accenture is a consulting company based out of Dublin, Ireland with over 500,000 global employees. Last year they reported over $44B USD in revenue (Accenture PLC, [2020).](#_bookmark2)

# Policy objectives

As stated in the policy itself, the policy objectives are “The purpose of this policy is to set forth the requirements for the protection and use of Accenture, Client and other third-party information, devices and technology.” The policy achieves this goal by . . . “[setting forth] the minimum Accenture requirements when accessing any Accenture, Client, or other third-party information or technology, and when personnel use any device, while performing Accenture work.”

# Expected Improvements or controls to be mitigated by the Policy

This policy mitigates risk to Accenture and Accenture’s clients by minimizing risky or unwarranted use of Accenture owned devices for non-Accenture related purposes, as well

as limiting use of personally owned devices on which Accenture email or data may be located.

# Policy Contents

This policy content specifically addresses: provisioning of devices; their approved uses, including both uses for Accenture business and approved personal use of Accenture owned devices; passwords and Accenture provided credentials; utilization of Accenture and Accenture client information; communication of information using email, messaging tools, collaboration tools, social media, and cloud services; physical protection of paper documents; incident reporting; compliance verification for the policy; and activities to verify compliance.

# Stakeholders and users that need to observe the Policy

The policy owner is defined as the Accenture Chief Information Security Officer. Compliance enforcement is the concern of the Computer incident response team. Legal questions are divided between the data privacy team and teh legal intellectual property team. Security exceptions are handled by the security exception team. Data and device loss or compromise of passwords or data integrity issues are handled by the Accenture security operations center. Technical support is the responsibility of the operations support team. The policy applies to all global employees and contractors.

# Evaluators and approvers of the Policy

Policy evaluation and approval is governed by Accenture policy 0001: Policy compliance, development and approval.

# Distribution and Communication and User Awareness Sessions

Policy 0057 is part of every “new joiner’s” first week of orientation. It is also referenced in annual ethics and compliance training, and every employee is required to

acknowledge their awareness of the content of the policy and that they are in compliance with the policy. The policy is also referenced frequently as part of device security scan pop-ups, as well as being part of the installation instructions for required software tools

necessary for receiving Microsoft Teams instant messages and Exchange emails on personal phones. Additionally, it is of course published on the policy webpage. The one issue is that this policy applies to all global employees but like all Accenture policies it is translated into only a limited number of languages. This means that it is not always available in the primary language of every empoloyee to whom it applies.

# Revision History

Policy 0057 has been in continual use since July 25, 1997. All revisions since May 14, 2010 are available on-line with the policy. Revisions prior to that date are archived.

# Recommendations for Improvements

**Translations**

While translations of policies are expensive, Accenture does its global employees a disservice by not having its policies available in the primary native language of all employees. The first and most critical way this, and all Accenture policies, could be improved upon is to ensure that translations are available in the primary native language of all global employees.

# Support Documentation

For most all statements, the policy provides adequate linkage to supporting documentation. However, in a few cases there are no supporting documents. This may be because supporting documents do not exist, but in many cases, such documents do exist but links are simply not provided. For example, Policy 0056 defines password standards and should be linked to the section of this policy that requires compliance with said standards.

# Defining How Compliance Will Be Monitored.

The section on monitoring of compliance is frankly rather light weight and simply doesn’t provide enough detail to determine if or how compliance with the policy should be determined. It is not clear from within the policy document itself how an interested party would determine if any given employee was in compliance with most of the provisions.

# How Does Accenture Use Policies Strategically

This is an example of a strategic policy. By having a global policy that lays out in very concrete terms how Accenture protects client information, Accenture creates an atmosphere of trust with their clients. Since Accenture must be trusted by their clients with sensative information in order to perform their role effectively, having policies that strongly outline why Accenture should be considered trustworthy is not only prudent but can be seen as a strategic.

# Appendix A Matrix Tool

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Item | Never/No | Infrequent | NA | Sometimes | Always/Yes |
| Does the policy have a |  |  |  |  | 5 |
| defined owner? |  |  |  |  |  |
| Are the policy |  |  |  |  | 5 |
| stakeholders defined? |  |  |  |  |  |
| Is the policy purpose |  |  |  |  | 5 |
| defined? |  |  |  |  |  |
| Does the policy have |  |  |  |  |  |
| any defined exceptions |  |  |  |  | 5 |
| or exclusions? |  |  |  |  |  |
| Does the policy have |  |  |  |  |  |
| defined repercussion |  |  |  |  |  |
| for failure to comply |  |  |  | 4 |  |
| with each requirement? |  |  |  |  |  |
| Does the policy define |  |  |  |  |  |
| who is responsible |  |  |  | 4 |  |
| for enforcement of each |  |  |  |  |  |
| element? |  |  |  |  |  |
| Is the policy scope |  |  |  |  |  |
| clear? |  |  |  |  | 5 |
| Does the policy link |  |  |  |  |  |
| to appropriate |  |  |  |  |  |
| supporting documents |  |  |  | 4 |  |
| for each requirement? |  |  |  |  |  |
|  |  |  |  | Continued | on next page |

Continued from previous page

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Item | Never/No | Infrequent | NA | Sometimes | Always/Yes |
| Does the policy define |  |  |  |  |  |
| how compliance will be |  |  |  |  |  |
| monitored for each |  |  |  | 4 |  |
| requirement? |  |  |  |  |  |
| Is the policy regularly |  |  |  |  |  |
| updated as technology |  |  |  |  | 5 |
| or environments change? |  |  |  |  |  |
| Is the policy readily |  |  |  |  |  |
| available to those to |  |  |  | 4 |  |
| whom it applies? |  |  |  |  |  |
| Is the policy overall |  |  |  |  |  |
| coherent and fit |  |  |  |  |  |
| organically with the |  |  |  |  | 5 |
| rest of the governance |  |  |  |  |  |
| structure? |  |  |  |  |  |
| Does the policy take |  |  |  |  |  |
| into account legal and |  |  |  |  |  |
| regulatory as well as |  |  |  |  |  |
| technological |  |  |  |  | 5 |
| limitations and |  |  |  |  |  |
| implications? |  |  |  |  |  |

# References

**Appendix B**

**\***

Accenture PLC. (2020, August). Accenture 2020 annual report.

Caralli, R., Knight, M., & Montgomery, A. (2012, November 1). *Maturity models 101: A primer for applying maturity models to smart grid security, resilience, and interoperability:* Defense Technical Information Center. Fort Belvoir, VA. <https://doi.org/10.21236/ADA610461>

Holder, A., Karim, K., Lin, K. (, & Pinsker, R. (2016). Do material weaknesses in information technology-related internal controls affect firms’ 8-k filing timeliness and compliance? *International Journal of Accounting Information Systems*, *22*, 26–43. <https://doi.org/10.1016/j.accinf.2016.07.003>

Li, C., Lim, J.-H., & Wang, Q. (2007). Internal and external influences on it control governance. *International Journal of Accounting Information Systems*, *8* (4), 225–239. <https://doi.org/10.1016/j.accinf.2007.09.002>

Likert, R. (1932). A technique for the measurement of attitudes. *Archives of Psychology*, *22 140*, 55–55. Retrieved July 25, 2021, from [https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,sso&db=](https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip%2Csso&db=psyh&AN=1933-01885-001&site=eds-live&custid=s1229530&authtype=sso) [psyh&AN=1933-01885-001&site=eds-live&custid=s1229530&authtype=sso](https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip%2Csso&db=psyh&AN=1933-01885-001&site=eds-live&custid=s1229530&authtype=sso)

Nolan, R. L. (1973). Managing the computer resource: A stage hypothesis. *Communications* *of the ACM*, *16* (7), 399–405. <https://doi.org/10.1145/362280.362284>

Wilkin, C. L., & Chenhall, R. H. (2020). Information technology governance: Reflections on the past and future directions. *Journal of Information Systems*, *34* (2), 257–292. <https://doi.org/10.2308/isys-52632>