Log Management Best Practices: A Delphi Study

Russel W. Havens
Brigham Young University
russel.havens@gmail.com

Justin Scott Giboney
Brigham Young University
justin_giboney@byu.edu

LOG MANAGEMENT BEST PRACTICES: A DELPHI STUDY

Abstract: Log management systems are used to ensure continuity of business systems. Administrators, managers, and users of log management systems have continual problems utilizing their systems to their full capacity. We performed a Delphi study to better understand the ways that stakeholders interact with and find value from their logs and the systems that manage them. Through the qualitative analysis of the Delphi study, we introduce nine propositions to begin to build a grounded theory for use of log management system. We present a blended IS Success and Task-technology Fit model. Our model shows how quality measures feed into technology and task-fit, which then drive use and organizational benefits. This study helps explain why they are widely used and how they are measured for quality.

Introduction

Applications, operating systems, hardware, network devices and other computing systems write out system log messages to provide information about their running state. Because computing systems are opaque to human perception, logs provide a critical understanding into the inner workings of information systems (Kabinna, Bezemer, Shang, Syer, & Hassan, 2018). Log management systems enable logs to be used for operational and security troubleshooting, debugging, and reporting (Likhita & Sahoo, 2016). They are also critical in the evaluation of confidentiality, integrity, and availability of information systems and data.

Poor log management system and service quality, in the form of unsystematic, ad hoc log management practices, are often cause challenges for digital forensics (Li, Bajramovic, Gao & Parekh, 2016; Shields, Frieder, & Maloof, 2011), database logging (Adedayo & Olivier, 2015), network management (Zhou, Yan, Fu & Yao, 2018), and large system scalability (Shang, 2014).

Ad-hoc, unscalable, unsystematic log approaches, poor default logging settings, and a lack of structure in log data (Wang, et al, 2017; Shang, 2012; Yuan, Park & Zhou, 2012; Adedeyo & Olivier, 2016) cause organizations to not realize the benefits of log management efforts (Döring & Steffens, 2015). Many organizations lack an understanding of how to properly use their logs using theoretical principles. There is also not a go theoretical understanding of log management.

Most academic literature that discusses log management considers the technical details of storing logs (c.f., Nakahara & Ishimoto, 2010). Others investigate analyzing logs from a computational and machine learning standpoint (c.f., Ambre & Shekokar, 2015). While there have been advances in these technical areas, the decision-making from logs by humans is still causing frustration and errors in critical services. The goal of this paper is to investigate the difficulties that still exist in the implementation of log management systems. Therefore, we ask the following research questions:

RQ 1: What are the theoretical principles to understanding how humans utilize log management systems?

RQ 2: What are the attributes of highly usable log management systems?

To answer these questions, we used an existing theory, the DeLone and McLean IS Success Model, to design a Delphi study, leading to a grounded theory of log management system use. Using a panel of log management system administrators and managers we explored to what extent log management system quality, information quality and service quality impact information systems organizational use, user satisfaction and net benefits of log management systems. We summarize our findings with a grounded theory of log management system use.

Literature Review

Log Management Systems

Log management systems include various log-related functionalities. These functionalities include: the collection of logs in a centralized or distributed way (DeConinck, 2017; Shaikh, Qi, Jiang, & Tahir, 2017; Rabkin, & Katz, 2010); log manipulation for standardization and use preparation (Vega, Roquero, Leira, Gonzales & Aracil, 2017; Sinha & Singh, 2016; Nagappan, 2011); storage of logs, utilizing simple file systems or various types of databases (Muthurajkumar, Ganapathy, Vijayalakshmi & Kannan, 2015); and log analysis tools (Zou et al., 2016; Miyamoto & Iimura, 2014; Zawoad, Dutta & Hasan, 2013; Xu et al, 2009). Log-related activities support critical IT governance activities, including IT infrastructure management (Coltman, Tallon, Sharma & Queiroz, 2015), security and system risk mitigation (ChePa, Jnr, Nor & Murad, 2015), and capacity planning (Ribeiro & Gomes, 2009; Sauvé, Moura, Sampaio, Jornada & Radziuk, 2006). The management of systems, as guided by an organization's IT governance principles, is key to organizations receiving value information systems while protecting the organization from information system-related risks (Weill & Ross, 2004). Log management systems and the logs they manage are used for troubleshooting, debugging and reporting (Zeng, et al, 2016; Likhita & Sahoo, 2016; Lemoudden, Bouazza, & Ouahidi, 2014), supporting the important IT governance activities including the management of IT infrastructure (Coltman, Tallon, Sharma & Queiroz, 2015), mitigating risk for system development and security (ChePa, Jnr, Nor & Murad, 2015), and planning capacity (Ribeiro & Gomes, 2009; Sauvé, Moura, Sampaio, Jornada & Radziuk, 2006).

Data governance of operational logs impacts IT security and operational effectiveness, for example, allowing security personnel to recognize and react to data breaches, or allowing IT operations personnel to more quickly and effectively deal with system failures, and operationally impacts IT governance, the effective utilization of IT resources in alignment with organizational priorities, which is associated with increased profitability (Choi, Cantor & George, 2017; Chong & Duong, 2017). Often, logs are not managed and utilized systematically in organizations, even though they are a rich and valuable resource for managing information systems (Wang, et al.,2017; Likhita & Sahoo,2016; Döring & Steffens,2015; Shang, 2012).

Log messages written by information systems are utilized by system administrators, software testers, developers, technical support personnel, system users and cybersecurity administrators. Access to these logs, however large the data set, is important for these roles (Karande, Bauman, Lin & Khan, 2017; Nagappan, 2011). Wang, et al. (2017) and Shang (2012) have stated that these log systems should be used more effectively. Companies are not realizing the benefits of log management efforts (Döring & Steffens, 2015) due to ad-hoc, unscalable, unsystematic log approaches, poor default logging settings, and a lack of structure in log data (Wang, et al, 2017; Shang, 2012; Yuan, Park & Zhou, 2012; Adedeyo & Olivier, 2016).

The lack of systematic- and best-practices have impeded IT governance in these areas. Understanding the perceptions and attitudes of IT professionals regarding log management systems and practices with regard to IT governance and security will help drive best practices.

The DeLone and McLean IS Success Model

In the 1990s, several influential theories on computer system usage were presented. DeLone and McLean (1992) first put forward the DeLone and McLean IS Success Model (DMISSM) to evaluate the success of information systems in organizations, putting forward aspects in which success can be assessed. Revised ten years later, this model has continued to provide useful insights for research (DeLone & McLean, 2003; Yakubu & Dasuki, 2018; Wanko, 2019). This study uses the DMISSM to investigate log system management to gain insight into how organizations currently measure the information quality, system quality, and service quality of log management systems and what benefits they perceive come from these systems (Ojo, 2017; Delone & McLean, 2016; Dembla, Flack, & Petter, 2015).

We limit our review of the DMISSM to how it applies to the effectiveness of log management systems. The first aspect of IS success deals with the information quality contained in or produced by the system. Information quality, in the context of log management, refers to the completeness, relevance, accuracy, and timeliness (Kisekka & Giboney, 2018) of the logs being collected by the system. Second, system quality refers to the usability, compatibility, reliability, and response time (Kisekka & Giboney, 2018) of the log management system. Lastly, service quality refers to the technical support provided with the log management system (DeLone & McLean, 2003).

The DMISSM explains that when log management systems are perceived highly in the three areas (information, system, and service), organizations are more likely to intend to use, use, and be satisfied with the use of logs (DeLone & McLean, 2003). For example, system logs collected to a log management system might be used to alert administrators when a server disk is nearly full or when a web application runs out of memory or when a user account is subject to a brute force password attack. For these to be effective, the system must provide the right data (information quality), in a consistent and stable way (system quality), with appropriate support when issues occur (service quality).

Many organizations have logs, and some even have log management systems. Yet, as shown by the literature, organizations still have problems adopting strong log management strategies (Döring & Steffens, 2015). This paper will show how organization can increase the information, system, and service quality of their log management systems.

A better realization of how systems are measured and what benefits they provide will allow organizations to focus on those things that current practitioners count as most important, allowing administrators and managers to better focus their administrative efforts for greater benefits of system utilization. The organizational benefits of these system will ultimately be reflected in better IT governance, particularly in IT operations and security (Kurniawan, 2018; Zou, Qin & Jin, 2018; Anastopoulos & Katsikas, 2017; Likhita & Sahoo, 2016; Volchkov, 2013; Nicho, 2012).

Methodology

Delphi Study

The purpose of our Delphi study is to explore log management practices to learn to what extent log management information quality, system quality and service quality impact log management system organizational use, user satisfaction, and net benefits of log management systems, as described by log management system administrators and managers using the Information Systems Success model (Ojo, 2017; Delone & McLean, 2016),

A Delphi methodology continually asks a heterogenous panel of experts controlled questions to develop a consensus about a topic (Kasiri, Sharda, and Hardgrave, 2012; Linstone & Turoff, 2002). The Delphi methodology was created by the RAND corporation to gather opinions from a panel of subject matter experts in a field (Dalkey & Helmer, 1963; Dalkey, 1969; Okoli & Pawlowski, 2004). In a Delphi study a panel of participants is asked a set of questions in rounds, with summary feedback on the preceding round going back to participants, allowing them to update their answers as they deem appropriate. Keeping participants anonymous from each other controls for group dynamics which might otherwise allow one participant to dominate the conversation or keep participants from updating their opinions due to group dynamics (Sekaran & Bougie, 2016; Zartha, et al., 2018).

Delphi studies are appropriate for the practice-related studies, and for involving a community, as practitioners are involved in consensus-building data collection (Brady, 2015). A Delphi study is appropriate for this research because it asks experts to produce and validate links of information, system, and service features that are necessary for successful implementation of log management systems. Using their responses, we will create propositions for a ground theory of log management system use. A Delphi study requires the collection of best practices on log management from log management system administrators and managers, and the iterative inquiry approach, with controlled feedback and participant iteration, allows group consensus while controlling for group dynamics such as strong vs weak personalities and follow-the-crowd tendencies (Mankoff, Rode & Faste, 2013; Sekaran & Bougie, 2016; Paul, 2008).

The Delphi method has been used in IS research related to RFID use (Kasiri, Sharda, & Hardgrave, 2012), food risk assessment tools (Soon, Davies, Chadd, Baines, 2012), critical skills for managing IT projects (Keil, Lee, & Deng, 2013), web accessibility for persons with disabilities (Hong, Trimi, Kim, and Hyun, 2015), and expert systems for ventilation strategies in infants (Tan et al., 2010). Goldkuhl states that while qualitative methodologies are often associated with interpretivism, they are also appropriate for pragmatic information systems research (2012).

We followed 5 steps when performing the Delphi study. More detail about each step will come in the following paragraphs. The methodology steps are as follows:

1. Delphi study participants were recruited by Qualtrics.
2. Participants were presented with the study summary and informed consent.
3. Participants were presented with the questions related to the quality of the log management systems they work with.
4. At the end of each round, a researcher analyzed the responses, and determined what points need clarification for the next round.
5. Steps 3 and 4 were repeated a total of three times.

Population and Sample

The target population of this study was experienced system administrators and managers with at least 3 years of professional experience installing, maintaining, utilizing and managing log management systems in an organizational environment, such as a company, non-profit, school or government entity. This group will be referred to in this research as log management system administrators and managers. Exclusion criteria include the candidate not being an adult and the inability to read and write English. Qualtrics was hired to find participants via a purposive sample (Devers & Frankel, 2000).

While there is no clear-cut direction on the number of participants in a Delphi study (Pare, Cameron, Poba-Nzaou & Templier, 2013), Linstone (1978) suggests at least seven. De Villiers, De Villiers, & Kent (2005) suggest 15 to 30 participants. Thangaratinam and Redman (2005) state that panels can range from 4 to 3000, and that the panel size is driven by the pragmatic concerns of cost and manageability.

Panel members were anonymous to the researcher, only being identified by a system identifier. Qualtrics' original invitation email avoided mentioning the contents of the survey to avoid self-selection bias. The survey description included the above inclusion criteria. Filtering questions were provided to participants so that they would only be moved to the survey if they responded that they had the required experience and were willing to participate in a qualitative survey. The sample for rounds one and two consisted of 32 panelists. 18 panelists were randomly selected for round three.

Demographics were collected in round two. One of the participants from round one did not provide usable answers in round two and was dropped from the study. The remaining participants consisted of 58% organizational leadership (managers, directors), 19% system administrators, 10% programmers, 6% project managers, and 6% system users. 3% were from small organizations (1-100 employees); 23% were from mid-sized organizations (101-500 employees), 16% were from large organizations (510-1000 employees); and 58% were from enterprise-sized organizations (more than 1000 employees). They represented organizations in a variety of industries: education, government, healthcare, retail, telecommunications, finance, insurance, agriculture, wholesale, manufacturing, consulting and technology. 23% of respondents were female; 77% of respondents were male. Panelists averaged 17 years of professional experience in a computer- or information technology-related field.

From round-three demographic questions, we found that panelists had been utilizing their organizations' log management systems for an average of 7.7 years and had been managing these systems for an average of 7 years. Their log management systems were utilized by variously sized groups of individuals: 50% had from 1-25 users; 22% had 26-100 users; 17% had 101-500 users; and 11% had more than 500 users.

Round 1

For the first round of the Delphi study, eight open-ended questions were presented. The subsequent two rounds asked clarifying and consensus-building questions based on the responses to round one and round two.

Q1: Please give an overview of your log management system, including the processes, processing stages, hardware and software tools used.
Q2: Please explain how you describe and measure your log management system's information quality
Q3: Please describe how your log management system's information quality impacts system use and user satisfaction in your organization.
Q4: Please explain how you describe and measure your log management system service quality.
Q5: Please describe how your log management system's service quality impacts system use and user satisfaction in your organization.
Q6: Please explain how you describe and measure your log management system's overall system quality.
Q7: Please describe how your log management system's overall system quality impacts system use and user satisfaction in your organization.
Q8: Please explain how your log management system's use and user satisfaction impacts the net benefit of log management in your organization.

The data were downloaded, and QDA Miner Light was used for coding and in-depth analysis, in addition to the cursory analysis utilized in the Qualtrics platform. Further analysis was done using Freeplane, a mind-mapping software package useful for visualizing hierarchies and relationships. Three levels of coding were utilized, per guidance by Tracy (2019): descriptive coding, in which meaning units were marked in the responses; analytical coding, in which these meaning units were grouped into higher-level, more abstract meanings; and axial pattern coding, in which higher-level meta-codes are identified across lower-level codes and across all rounds of questions.

Log management systems. System descriptions were generally short and incomplete. For example, one respondent gave the response, "cloud based log management system was easy to build do not setting up hardware and software onsite" (coded as "Cloud-based (unspecified)").

Another responded, “It is logged into the logs of the system. If there is any error, it is then logged so that it can be diagnosed and fixed by the engineer” (coded as “Troubleshooting”). One of the more complete responses was, “In my organization we deal with large volumes of computer-generated log messages. In this capacity we do log collection, centralized log aggregation, long-term log storage and retention, perform log rotation, and do log analysis Log search and reporting. We use Splunk technology tools for these functions” (coded as “High volume,” “Centralized collection,” and “Splunk”). More analysis detail is given next.

Information, system, and service quality. The quality measurement theme garnered a wide variety of responses and response types. Separating out by question, 81 descriptive codes (see Appendix A) were created to represent quality measurement that panelists specified. Inside these 81 descriptive codes, the type and focus of responses were extremely varied. Further, responses for one quality measurement often could have as easily been applied to another quality measurement, either because the response was quite generic, or because the respondent did not differentiate between the information, system, and service quality areas. The following paragraphs give examples of both the response variety and response similarity, starting with response variety.

The interpretation of the questions varied widely. For example, some panelists described specific ways of measuring quality such as using questionnaires to measure service quality (e.g. “There are many types of questions that can be asked in a Service Quality Questionnaire,” Q4, coded as “Questionnaires-Service quality”) or auditing of information (e.g. “auditing checks for adherence to standards,” Q6, coded as “Auditing-System quality”). Another panelist, with a response different from the previous respondent, gave a multi-factor response describing attributes of success concerning information quality: “High quality data is determined by optimizing the completeness, consistency, accuracy, validity, and timeliness of the data collected." This was given seven different codes (Q2, codes "Actively measure information quality," "Completeness," "Consistency," "Accuracy," "Validity," "Timeliness," and "Best practices"). Still other respondents gave a judgment of the quality of their own systems. For example: "Quality is acceptable. Correlation and sharing of data is poor" (Q2, coded as "Current quality is good" and "Current correlation is poor"), or "It is pretty good" (Q2, coded as "Current quality is good"), or "The measurement is accurate and consistent across all platforms" (Q2, coded as "Current quality is good-Information quality"), or "…we never have issues with accuracy [sic] of the information" (Q2, coded as "Never have accuracy issues-Information quality").

As examples of response similarity, some panelists gave responses about quality from one question, for example, System Quality in Q6 (concerning system quality measurement) or even Q7 (concerning system quality benefits), that could be applied to another (or even multiple) quality areas: "If it is accurate, that is good" (Q6, coded as "Accuracy-System quality"), and "Always, accuracy and speed of queries makes user satisfaction raise higher with every transaction" (same candidate, Q7, coded as "Accuracy-System quality"). The first of these could easily apply to Information quality or even Service quality, but the second of these seems to be about system quality. Alternatively, in another example, "Our home grown [sic] system has been developed and continuously enhanced to implement facilities we deem useful" (Q6, coded as "Continuous improvement-System quality"). The words "system has been developed" suggests System quality, but potentially this "home grown [sic] system" includes the information and services as part of their "facilities."

Some panelists described the effects of system quality issues in Q6, rather than how they measure quality. For example, “This will lead to degration [sic] if certain applications due to downstream impacts” (Q6, coded as “Issues impact other systems-Service quality”) or “Because we have good support we are able to address any issues quickly, giving end users [sic] confidence in the platform” (Q6, coded as “Issued addressed quickly-Service quality,” and “End-user confidence in platform-Service quality”). Other panelists gave no information about system quality at all, but just described their systems: For example, as a response to Q2, “Various areas/applications define what logging information is pertinent to them and to management. That information is collected automatically and then used to monitor.” This describes the log management system but gives no measure of information quality.

Certain quality descriptions are very specific to the panelist’s system. For example, “our users who use the log systems are generally happy and satisfied with the performance since the hardware was upgraded” (from Q7, coded as “Happy users-System quality” and “Performance-System quality”), “No hard measurements. As data is displayed real-time in dashboards, the consumers would complain (Q6, coded as “No measurements-Service quality,” “Dashboards-System quality,” and “Happy users-System quality”) and “The current systems results in solutions that take too long, provide little root cause analysis, no proactive support or solutions, and reduced service quality” (coded as “They have problems in performance-Service quality”).

It is worth noting that one panelist, after stating that their systems are “Automated” and that “It has been working very well for the company so far and has been for a very long time,” went on to stated that they did not measure any quality type (Q2/Q4/Q6, coded variously as “No way to measure information quality”, “Do not measure”, “Do not measure-Service quality”) and that these quality types do not impact use in any way (Q3/Q5/Q7/Q8, coded variously as “No impact on user satisfaction-Service quality", No impact on user satisfaction-System quality", and No impact-Net benefit"). This one response was a stark counterexample to the many others that described measurement methods and impacts in many ways.

System benefits. Like the quality measurement topic, the benefits of quality elicited a broad range of responses. Separating responses by question, 86 descriptive codes (see Appendix A) related to quality and system benefits were created from panelist responses. Like the quality measurement theme discussed, the topic of information, system, and service quality benefits and overall system benefit was widely varied. In this case, though, system benefits and uses (i.e., how these systems are used and the benefits of having a log management system), and the benefits of information quality, service quality, and system quality, were often conflated in panelists' responses. Various aspects of this will be discussed here, with response quotes and researcher coding decisions.

Uses of logs, as elicited by Q1 and discussed above, are tied to system and quality benefits, but were considered separately in the first inter-round analysis. However, it was common for panelists to describe quality benefits in terms that sounded like use: e.g. "Focused reports and alerts allow admins to react timely, improving customer morale" (Q3, coded as "Reporting-Info quality," "Alerting-Info quality," and "Customer morale-Info quality"); "Provide monitoring on system performances and error reportings," (Q3, coded as "Performance-Info quality" and "Monitoring-Info quality"); "Reduce Risk of Audits" (Q8, coded as "Improve compliance-System quality").

In some ways, benefits-related responses were less variable than quality measurement responses, in that most stated benefits of the overall log system. There were fewer interpretations of the questions. For example, there were no complaints about the panelists' own systems. On the other hand, there were similar variabilities, such as respondents describing the benefits of the system in general in the information/service/system quality responses vs. respondents talking about those specific areas. For example, many responses, like these examples, appear to be about general system benefits: “Our log management system is able to pin-point server problem to alert us in a potential server problems in a timely manner” (Q3, coded as “Improve operations”) or “Our overal [sic] management systems quality is extremely important for susessful [sic] management” (Q7, coded as “System quality is important-System quality”) or “it…is very useful in making decisions” (Q5, coded as “decision-making-System quality”) or “Log management plays an important role in resource management, application troubleshooting, regulatory compliance & SIEM, business analytics, and marketing insights” in response to Q2, about information quality (Q2, coded as “Log management benefits described”) or “On the other hand, some panelists responded concerning the question’s area of quality in a way that made sense for that particular type of quality: e.g. “Focused reports and alerts allow admins to react timely” in response to Q2, concerning information quality (Q2, coded as “Alerting—Info quality”) or “it provides a level of service aggrement [sic]” in response to Q7, about system quality (Q7, “Provides service level agreement values-System quality”).

In some cases, the response to a question about one type of quality seemed to be discussing a different type of quality, for example, “Accurate data reduces the time to correct problems” in response to Q5, concerning service quality (Q5, coded as “Troubleshooting-Info quality), or “Service quality is measured as uptime” in response to Q4, concerning service quality, defined in that question section as to how the log management system is supported by the IT group (Q4, coded as “Uptime-Info quality”). Other responses were difficult to tie to any particular area of quality, e.g., “We periodically scan those logs that provide insight on system performance, productivity, and systems managings [sic]" in response to Q2, concerning information quality, but appearing to be more about overall system benefits (Q2, coded as "Improve operations").

Lessons learned. Round-one questions Q2 through Q8 were built around components of the DeLone and McLean IS Success model (2002). Q2 through Q7 were written to be very parallel to each other, asking about information, service, and system quality measures and benefits. Q8 asked about overall log management system net benefits. The codes from Q2-Q8 were very similar across these questions. When the responses to these questions were coded, many of the same quality and benefits codes appeared in these responses.

When the codes for all three rounds of responses were organized by topic, both quality measures and benefits were commonly described in terms of tasks to be accomplished rather than in terms of a measure of quality for the system. How well the log management system supported business tasks was mentioned in many responses. It was common for panelists to describe quality benefits in terms that sounded like use: e.g. "Focused reports and alerts allow admins to react timely, improving customer morale" (Q3, coded as "Reporting-Info quality," "Alerting-Info quality," and "Customer morale-Info quality"); "Provide monitoring on system performances and error reporting [sic]," (Q3, coded as "Performance-Info quality" and "Monitoring-Info quality"); "Reduce Risk of Audits" (Q8, coded as "Improve compliance-System quality").

These responses suggest that practitioners think in terms of the practical business tasks to be holistically accomplished rather than in terms of arbitrary quality measurements. Leading to our first proposition:

P1. Practitioners do not readily differentiate between information, system, and service quality when thinking about the overall quality and benefits of the systems they interact with.

Round 2

Upon initial analysis of the round-one results, and in reviewing the purpose and research question of the research, to investigate how the quality of information, systems, and services impact the use and net benefits of log management systems, the round two questions were developed.

Q1. Many panel members described different attributes of a high-quality log management system. In your case, how would you measure your log management system's success?
Q2. Some panel responses suggested that current systems could be made more useful. What would you change about your organization's log management system to make it more useful and successful?
Q3. Most panelists described well-established systems, describing a wide variety of needs being met. How was your log management system chosen? What should have been considered in that decision?
Q4. Not much information was given about how utilized your log systems are. Do you consider your log management fully utilized? Why or why not?

The first two questions were developed to gain more consensus on some of the responses found from round one data. The first question was asked to clarify the wide variety of quality measurement-related responses from round one. Because of the requisitely loose organization of these codes around the wide variety of responses, the second-round question was formulated to ask about overall system success measurements in panelist’s organizations.

The second question was driven by another theme that arose: shortcomings in panelists’ log management systems were often mentioned. Some quotes that suggested this, along with descriptive codes and some researcher interpretation, include: “Its [sic] an added hassle to follow the standards but it greatly assists the IT staff to troubleshoot and resolve issues” (Q8, coded as “Inconvenient,” and “Troubleshooting-Net benefits”—interpreted to mean that setup is difficult, but that they put up with that because of the benefits of using the system); “if the thorough log has been generated, then it is easier to trace the error and resolve" (Q3, coded as "Completeness," "Bug fixing-Info quality"—interpreted to mean that thorough logs are not always generated but are useful when they are); "We do not measure so nothing in this case" (Q2, coded as "No way to measure information quality"—interpreted to mean that either they do not care or have not built a way to measure information quality); "The systems/applications are the main driver as far as quality goes. Some are better than others and some require in-depth application knowledge in order to set things up" (Q3, coded as "Drive by systems and applications"—interpreted to say that their service quality is inconsistent, requiring more knowledge to set up system logging for some people); "when data is incomplete, requests for information cannot be satisfied. This can be our own end-users as well as for audits, both internal and external" (Q7, coded as "Incomplete data-System quality"—interpreted as a current issue in their system); "If anything we are overwhelm [sic] with high quality data." (Q2, coded as "Too much high quality data"—interpreted as stating that even successful systems overwhelm users). Since this information would feed into the discussion on quality and use, a specific question was developed on this topic for round two.

Many respondents did not address two areas of interest to the use and benefits of these log systems: system selection and system utilization. Only a few comments touched on how these systems were selected. This information relates to how and why organizations use these systems, so a third question asked about this aspect of their systems; this included asking these expert panelists' opinions on what else should have been considered so that shortcomings in their current systems might be avoided for readers of this study.

Finally, we realized that very little information was given about the utilization of these systems: whether they are used by only a tiny group of people or by entire enterprise IT departments, whether they were utilized to their full potential, would be meaningful and important in describing the net benefits of these systems. Thus, a question around use was developed, including asking why they felt their systems were or were not fully utilized.

Question 1. Various methods of measuring system success were given by panelists. Most of these were related to the functionality of the system (eight panelists), the data provided by the system (seven panelists), and the business results (ten panelists). Many panelists suggested multiple things, and those things were grouped into multiple higher-level themes. For example, one panelist responded to Q1 with "easy and fast in finding data needed for investigations, audits, etc." This was categorized into "Performance", under the "System-related" theme and "Data Access" under the "Data-related" theme. Another panelist responded, "I would measure it a success if it quickly and efficiently generates, transmits, analyzes stores, archives, and disposes of our volumes of log data." This was coded with "Performance"; it was not coded with "Efficiency of use", as that tag was considered related to usability rather than system efficiency.

Half of the ten entries coded under "Business results" were grouped under "Good results", but as might be expected, the actual text of these responses was varied. For example, "our company keeps a good record of all the data entered", "Deliver operational visibility", "Gets the job done", and simply "GOOD RESULTS" and "Results". Two panelists responded that they did not know how to measure success. The more plain-spoken of these stated, "I don't think I have any insight to say anything about it. I don't know what to say about this one."

Under the theme of "system-related" codes, system performance was the most commonly mentioned success criteria, as was mentioned earlier. Reliability was given by two panelists who mentioned other success criteria: "low total cost of ownership, **reliable** and easy to maintain" and “we are very happy with it’s [sic] ease of use and **reliability**” (Q1, emphasis added to reflect coding as “Reliability”).

Other system-related success measures measured by respondents included the following: The ability to filter out non-relevant values, “provide utilities to filter out log data for relevant information for a [sic] specific particular log details, less false positives” (Q1, coded as “Able to filter out non-relevant values”); configurability, “It should be configurable” (Q1, coded as “Configurability”); maintainability, “low cost of ownership, reliable and **easy to maintain**” (Q1, emphasis added, coded as “Easy to maintain”); and the ability to centralize logs, “We centralize all your logs” (Q1, coded as “Log centralization”). Two related success measures, grouped under a theme of usability, were ease of use and efficiency of use, for example four entries like this one: “The ease of the system” (Q1, coded as “Ease of use”), and this use-related entry, “EFFICIENCY OF SEARCHING” (Q1, coded as “Efficiency of use”). Combined with the earlier system-related success measures, these cover a wide gamut of functionality and usability, and appear to represent the concerns of panelists in the success of their systems.

From the themes from question 1, we propose:

P2: Log management system users think about their systems in terms of functionality, business results, system performance, and success measures.

Question 2. Q2 attempted to gain more clarity around what makes a successful log management system by asking what panelists would change to make their systems more useful and successful. Most of this was categorized in the theme “What would you change?” This open-ended question elicited responses around the log management products themselves, the implementation of these systems, training, and a lower total cost of ownership (TCO). Five respondents said they would make no changes, and one did not know what they would improve.

These latter responses could be interpreted as counterexamples compared to more than two dozen responses suggesting things to change.

In the product improvement area, several areas for improvement were suggested by multiple panelists: Five responses wished for greater usability, for example, “Ease of use is top concern otherwise it is not widely accepted and used” (Q2, coded as “Make it easier to use”), and “easier ‘query’ capability” (Q2, coded as “Make it easier to use”) “less cryptic” (Q2, coded as “Make it easier to use”). Five others suggested that their systems need improved performance; examples include “faster access, better indexing” (Q2, coded as “Improve performance”), and “the speed and efficiency in which it performs these functions” (Q2, coded as “Improve performance”). Two panelists would have improved their systems’ ability to send notifications: “Automated emails on seeing failures, a phone alert would help” (Q2, coded as “Enhance for notifications”), and “it can be enhanced to send out text messages to our cell phones in addition to sending out emails [sic] alerts” (Q3, coded as “Enhance for notifications”).

Process and implementation suggestions were more varied, with no two records suggesting the same things. Some of these suggestions included improving security and controls, better accessibility, and with more rights to users, fewer processes, and consolidation to a single system. These are all implementation details that many log management systems can be made to employ with sufficient time, energy, money, and knowledge.

P3. Log management system users seek to improve usability, performance, and operations in their systems.

Question 3. To better understand the current state and organizational details about the panelists’ log management systems, Q3 asked how the panelist’s system came to be, eliciting more details of the organizational fit by asking about selection criteria that the panelist felt should have been considered. Interestingly, Q3 was interpreted in two different ways by panelists: who in the organization made the system, and how was the decision made.

With the former interpretation in mind, three panelists stated that their log management system was chosen by an IT committee, e.g., “We had a committee in our IT department and discussed options” (Q3, coded as “IT committee”); two panelists stated their systems were chosen by a dedicated team, e.g., “By the group of data management” (Q3, coded as “Chosen by dedicated team”); and one stated that their parent company dictated their system: “It was dictated by our parent company based in the UK because they are already using it” (Q3, coded as “Chosen by parent company”).

With the latter interpretation (how the decision was made), four panelists stated different methods of consensus: “According to the reviews of people of the company” (Q3, coded as “Community decision”); “By group decision involving input from multiple business units and individuals” (Q3, coded as “Multi-organizational group decision”); “chosen by Govt [sic] best value selection process” (Q3, coded as “Government best value selection process”); and “Our log management system is a home grown system” (Q3, coded as “Home grown”). Two panelists simply stated that their systems had been in place a long time and that they were not involved, e.g. “Had been in use already a long time” (Q3, “In place for a long time”).

Many choice considerations were shared, with about half stated in past tense, and half in present or future tense, suggesting considerations that were taken vs considerations that should be taken. For the past tense group, three major themes: ease of use was mentioned four times, e.g., “It was chosen based on how it is intuitive to use” (Q3, coded as “Ease of use-choice considerations”) product features mentioned in four responses, e.g., “We needed a broad scoped tool” (Q3, coded as “Features”); and cost, e.g., “it was chosen according to cost and user friendliness” (Q3, coded as “Cost” and “Ease of use-choice considerations). Some other considerations included vendor support, a dashboard feature, and direction by team or organizational leadership being considered. For the present/future-tense group, each of the following were found in two responses: company-specific needs, e.g., “It’s important to get a centralized log management system that fits your company’s unique needs” (Q3, coded as “Company-specific needs”); usefulness for daily work, e.g., “usefulness in day to day work” (Q3, coded as “Daily work usefulness”); and multi-team considerations, e.g., “needs of multiple areas should have been considered” (Q3, coded as “Multi-team needs”). The ability of a product to provide insights, to grow as needed, to resolve issues, to improve work efficiency, and to be easily implemented were specifically mentioned, as was the importance of doing product evaluations, but each of these only had one panelist’s response.

P4. When thinking about the past selection of a product, selection details are quickly forgotten, with only the organizational “who” and “how” remaining in mind.

P5. While ease-of-use, feature set, and cost have been used as major selection criteria in the past, forward-looking decisions are more likely to include task fit, ease of implementation, organizational fit, and multi-team needs.

Question 4. For Q4, panelists were asked whether they felt that their log management system is fully utilized and why or why not. Fourteen panelists said yes, their systems are fully utilized. Ten panelists said they are not. Seven gave hedged answers, such as “No, there could be more done to make it better” (Q4, coded as “Room for improvement”), and “we still are not getting the basic data out of our logs, and we are still not able to fully and successfully view full application error details” (Q4, coded as “Room for improvement”), and “It is in process and being observed” (Q4, coded as “Still being determined”), and “for some applications, yes, other applications need some work" (Q4, coded as "Yes in some areas, no in others"). One respondent said, "I think it is fully utilized at this time because there is no other option" (Q4, coded as "Yes because there is no other option"), which is open to interpretation, but suggests more nuance than a simple "yes." Our interpretation of this is that utilization is highly dependent upon the implementation or the system user's opinion, which has implications for the IS Success model interpretation per responses by these individuals.

In terms of why the system is being fully utilized there are two main themes when people consider utilization. The first is whether the team is organized around the tool for example, we received responses about whether there were full-time staff dedicated to using the tool, how people work together using the tool, whether they have resources to utilize the LMS, and whether the team has time or not. The second is whether all the functions of the tool are available and/or in use. We received responses about whether the functionality is what they paid for, they receive the results they expect, whether they could gather logs from other sources, and whether they use all the features from the LMS. From this we posit:

P6. When considering utilization, users have two mindsets: team orientation and feature usage.

Round 3

For the final round of questions, the responses to these questions were considered, along with the original problem statement and research question. Round-three questions were focused on summarizing and clarifying the responses received in rounds one and two. Suggestions for system improvements came through in both previous rounds, most particularly in round-two Q2 (but also in Q3), so more specific details were elicited concerning the system improvements. These are system users with insights into what is or is not working in their log management systems, so their opinions were asked, with examples:

Q1a. Which of the following do you feel is the most important area for system improvements in your:

1. log management implementation?
2. product features
3. the product implementation in your organization
4. the business processes that use the tool

Q1b. Can you give an example that explains why you feel this way?

Q2: For your log management system, how would you rank the importance of the following for yourself vs other system users?

- Information quality (cleanliness, timeliness, completeness of data)
- System quality (system stability, system performance, system features such as powerful filtering or data visualizations)
- Service quality (help desk support, training, response-time for log system outages)

Q3: Why did you choose that ranking?

Q4: Many specific uses for the log management system were described in Wave 1. Thinking at a higher organization level, in what ways does your log management system support IT governance or high-level business processes in your organization?

As was seen in the round-one analysis, there appeared to be a considerable amount of cross-question response bleed-over in round one. Many of the same answers appeared in responses about areas of quality, but particularly in system quality and information quality. To better understand where respondents' priorities are with these three measures of quality, panelists were asked to rank the importance of information quality vs. system quality vs. service quality for their log management system and to explain their choice. This information would help weight those quality areas which are central to the IS Success model.

Many of the previous round questions focused on specific details on these systems. In the final question, an organizationally higher-level view of the log management system was inquired after. Panelists were asked how these log management systems support IT governance or high-level business processes. While earlier responses provided many technical benefits of log management systems for their organizations, this question was hoped to allow panelists to explain how these systems support and provide value to their organizations on a business level, either directly relating to IT governance, or indirectly through high-level business processes.

Question 1. Round-three Q1 sought for more clarity in product vs. implementation vs. organization vs. business process improvements for the panelists' organizations' log management systems. It asked how the panelist would improve their log management systems but did so by asking about areas for improvement.

Twenty-one codes were identified from these responses. The majority of these, thirteen, were directly related to product features. Four were related to business outcomes. One code represented a response stating that their system was under continuous improvement, and another represented a response stating that their current implementation was poor, pointing out access speed as an issue: "The implementation because the current implementation just doesn't allow for quick access." Despite the number of codes that fall into product vs. other categories, two panelists stated that product features were most important while five stated that product implementation was most important. This is likely an artifact of the difficulty of categorizing a feature as a "product feature" vs. an "implementation feature"—for example, is reporting slow because the product is slow, or because it was not implemented well? Or is reporting difficult because the product makes it difficult, or because it was implemented in a way that makes reporting difficult. This would be an interesting area for future research.

Some examples of product feature improvements suggested by panelists include: "I would make it more like the Splunk tool – easier to read and easier to build reporting around it" (Q1, coded as "Easier reporting", and "Usability"); "I think product features are important as we (the users) want to know what are the main features that we can do with the product and get the results that we want. Also including as part of the product, a good online documentation on the features.(on the same page as we are using) with a quick URL link to get more details. A quick guide for tips and suggestions." (Q1, coded as "Product features," "Good documentation," and "Quick guide"); "Log mgmt systems are notorious for eroding on the user input side. What comes in mist [sic] be accurate and timely. Thst [sic] needs to somehow be enforced better" (Q1, coded as "Data accuracy," and "Data timeliness"); "Adding additional alerting is a great idea" (Q1, coded as "Additional alerting"); and "log access and interpretation" (Q1, coded as "Analysis tools," and "Access to logs"). These kinds of product-specific responses could be expected of system users, but with the number of managers, the number of responses was surprising.

Business outcomes formed another theme from the data, with responses like: "The business processes are most important" (Q1, coded as "Business process most important"). Or, as another example, "It will make us more efficient and cut down on costs" (Q1, coded as "Increased efficiency"). Or, "To implement a product that will increase security and minimize risk" (Q1, coded as "Product increases security" and "Product minimizes risk"). Again, considering the high number of managers in the sample, the researcher was surprised that these business-level responses were not more common.

P7. When considering system improvements for an existing log management system, users most readily think about product features.

Question 2 and 3 – Quality-type rankings. Q2 and Q3 were implemented as a pair of tightly related questions, an order-ranking question and an open-ended text question, about why they chose that order. Q2 asked panelists to rank their priorities for information quality vs. system quality vs. service quality. Perhaps owing to the wide variety of backgrounds of the panelists, every possible ordering of priority was given. Table 1 shows these orderings and counts.

Table 1: Relative Importance of Quality Measures

Ordering	Response count
Information / Service / System	4
Information / System / Service	5
Service / Information / System	2
Service / System / Information	1
System / Information / Service	4
System / Service / Information	2

Note that the two lowest response-count orderings put Information quality last, while 2 of the 3 highest response-count orderings put Information quality first. A larger sample would likely have brought out more differentiation here.

Q3, which asked why panelists chose that ordering, gave as varied results as the orderings themselves. Some panelists gave very little information in the "why choose that ordering" response: "by imprtance [sic]" (Q3, not coded), and "I believe this is vital in regards to success" (Q3, not coded). Others gave simple restatements: "Info quality is paramount in a log system first and foremost" (Q3, coded as "Info quality most important") , and "I thing [sic] service quality is the primary concern. If you have good software but in case of issues yu [sic] do not have team to support it then it is useless. Second is the information system which is generated and thirds [sic] comes the system quality, it matters very less if the report takes 5- 10 min to generate. a [sic] person can live with it but not with other [sic]." Still others gave more reasoning: "I think giving us the proper information along with guidance when a certain situation arises and making us productive in understanding and troubleshoot [sic] certain issues and events" (Q3, coded as "Information quality most important" and "Documentation also important"), and "For me is the reason for having a log management system is to have accurate data. That's why I feel that the quality of the information is crucial. Without that there really is no purpose and having a log management system." (Q3, coded as "Info quality most important"), and "The quality of the data is most useful for accuracy, completeness, consistency, uniqueness, and timeliness." (Q3, coded as "Info quality most important").

It is worth noting that four of the 18 panelists gave a particular ordering, and then in the "why" response, explained the importance of a quality type that was not their first choice. For example, one respondent with system/service/information quality as their ordering subsequently stated "Service quality. Product chosen after evaluation but the after sale [sic] service is crucial as/when problems arise" (Q2, coded as "Service quality is most important" and "Inconsistency between order and description"). As other examples, a panelist with system/information/service quality as their ordering gave this answer to why: "Quality data is key" (Q3, coded as "Info quality most important" and "Inconsistency between order and description"); and a panelist with service/information/system quality ordering stated, "system quality is crucial since it is the heart of product [sic]" (Q3, coded as "System quality most important" and "Inconsistency between order and description"). As a final example of this inconsistency, one panelist selected information/system/service ordering, but gave a "why" response of "BEST EFFICIENCY" (Q3, coded as "System quality (efficiency)" and "Inconsistency between order and description").

When codes were grouped by information vs service vs system quality, about the same number of responses were given for each area, with 6, 5, and 7, respectively. As for response inconsistency, these were spread across four different orderings, one of each for service/information/system-ordered responses, system/information/service-ordered responses, system/service/information-ordered responses, and information/system/service-ordered responses falling in this category. In three of these four inconsistencies, the second-ordered quality was the one mentioned in the "why" question response. These responses, and the facts that every possible ordering was chosen and that about the same number of panelists chose each quality area as most important, all taken together, suggests that picking an ordering to these is either difficult (e.g. because they are all about the same in importance) or very subjective (e.g. based on individual preference or experience). Further study may be able to tease out the details of this area, such as whether this is specific to log management systems or IT systems more generally.

P8. As with P1, practitioners do not readily differentiate between information, system, and service quality when thinking about the overall quality and benefits of the systems they interact with.

Q4 – IT Governance/Business Benefits

Q4 asked panelists to take a step back and consider the IT governance and high-level business benefits of their log management systems. The tactical benefits of such systems was well-discussed in rounds one and two, so this question elicited higher, business-level benefits of these systems. Ten codes came from responses to this question.

Four of these ten codes represented 12 out of 18 responses, with three responses each. These codes were: “Improve support,” e.g. “Streamlines IT processes and support the foundation of getting quality service to the company” (Q4, coded as “IT process efficiency” and “Improve support”); “Improved business decisions,” e.g. “It is important to help us make decisions about Houser and [sic] areas of our business are run” (Q4, coded as “Improved business decisions”) and “it does help upper management determine resource allocation” (Q4, coded as “Improved business decisions”); “SLA visibility,” e.g. “It gives us visibility in how well our organization is managing our computing resources in a way to provide a high level of service agreement to our users to minimize outages and improve support” (Q4, coded as “SLA visibility”, “System stability," and "Improve support"); and "System stability," e.g. "to make everything work in order" (Q4, coded as "System stability"). One panelist stated that "High level business processes and governance are designed in from the very beginning," which could be interpreted as saying that "these systems are intended to support IT governance and business processes" or that "these systems are governed by IT governance and business processes." Another panelist stated that this system "Streamlines IT processes and support[s] the foundation of getting quality service to the company" (Q4, coded as "IT process efficiency" and "Improve support").

P9. Practitioners perceive log management systems as improving IT decision-making, systems stability, and visibility.

Discussion

Through the analysis process, three major themes and subthemes were developed from the response data analysis. Two of these were around the major research topic, quality measures and net benefits, while the third surrounds a model that developed from the response data. These themes were developed through a cross-round pattern analysis of the overarching themes visible in panel responses.

Practical Implications

The two primary practical contributions of this study are in identifying quality measures that are in common use, and in identifying the specific organizational benefits of log management systems. The panel's consensus responses gave several areas in which practitioners should focus. These themes are discussed next.

Theme 1: Measurements of quality and success focus on business benefits and product features

A cross-round pattern coding analysis for quality or success measures showed that business impacts and product features were most important areas for measuring system quality. Each of the following subthemes was discussed by multiple panelists across the three rounds:

Subtheme 1a: Business results measures

When determining the quality of a log management system, business results matter. In particular, the following business-driven areas were given by many respondents:

• Business process improvement – log management systems were expected to improve business processes, including system management, customer experience, reporting capability, and SLA transparency. This was mentioned more than all the other business measures together.

• Low TCO – System cost, the total cost of ownership, and return on investment were other business-related measures mentioned.

Subtheme 1b: Product features

Product features were another large area focus on respondents. The features mentioned were often tied to the ability to accomplish a task, such as producing reports or troubleshoot problems. The most commonly mentioned features were:

• Usability – The usability of the log management system was mentioned more than any other the other product feature.

• Performance – Speed of queries and reporting performance were a common theme in responses.

• Alerting – Multiple respondents emphasized the ability to monitor and alert on issues discovered in system logs to provide for proactive work.

• Analysis tools – Several other respondents discussed the need for rich analysis tools, better reporting, and even artificial intelligence (AI) support.

Though mentioned by fewer respondents, a few information- and service-related quality measures were also mentioned. Access, accuracy, and timeliness of information were mentioned. In alignment with the usability theme that was widely mentioned, training was discussed as a measure of high service quality.

Theme 2: Log management systems provide many organizational benefits

Like the quality measurement topic, the benefits of quality elicited a broad range of responses, especially in round one. Separating responses by question, 86 descriptive codes related to quality and system benefits were created from panelist responses. Like the quality measurement theme discussed, the topic of information, system, and service quality benefits and overall system benefit was widely varied. A cross-round, pattern analysis of benefits showed that benefits fall into three areas: business benefits, system benefits, and security benefits; security benefits were mentioned by the panel less frequently than business and system benefits.

Subtheme 2a: Log management systems provide business benefits

According to panelists, business benefits provided by log management systems include:

- Customer benefits: including reporting and service level agreement (SLA) visibility, customer trust, better end-user experiences of systems, satisfaction with the help desk
- Improved efficiency for IT processes, better utilization, and prioritization of resources.
- Compliance benefits with improved compliance reporting
- Improved decision-making

Subtheme 2b: Log management systems provide IT system benefits

Panelists shared many system benefits for their log management systems, which fit into the following major areas:

- Increased reliability: better troubleshooting, monitoring, and performance
- Improved system view: unified system view, better application and data understanding, and a better understanding of the impact of issues
- Software development benefits: better code quality, easier troubleshooting, supports software development lifecycle (SDLC)

Theory Implications

In addition to practitioner implications, this research suggests some things about the theoretical frameworks used, namely, the DeLone & McLean IS Success model and the Task-technology Fit model, and how they might be advantageously combined.

Theme 3: Theory Framing

Round-one questions Q2 through Q8 were built around components of the DeLone and McLean IS Success model (2002). Q2 through Q7 were written to be very parallel to each other, asking about information, service, and system quality measures and benefits. Q8 asked about overall log management system net benefits. The codes from Q2-Q8 were very similar across these questions. When the responses to these questions were coded, many of the same quality and benefits codes appeared in these responses.

When the codes for all three rounds of responses were organized by topic, both quality measures and benefits were commonly described in terms of tasks to be accomplished rather than in terms of a measure of quality for the system. How well the log management system supported business tasks was mentioned in many responses. It was common for panelists to describe quality benefits in terms that sounded like use: e.g. “Focused reports and alerts allow admins to react timely, improving customer morale” (Q3, coded as “Reporting-Info quality,” “Alerting-Info quality,” and “Customer morale-Info quality”); “Provide monitoring on system performances and error reporting [sic],” (Q3, coded as “Performance-Info quality” and “Monitoring-Info quality”); “Reduce Risk of Audits” (Q8, coded as “Improve compliance-System quality”).

These responses suggest that practitioners think in terms of the practical business tasks to be holistically accomplished rather than in terms of arbitrary quality measurements. This holistic and practical view could be mapped to a model that combines the IS success and Task-technology fit models as seen in Figure 1.

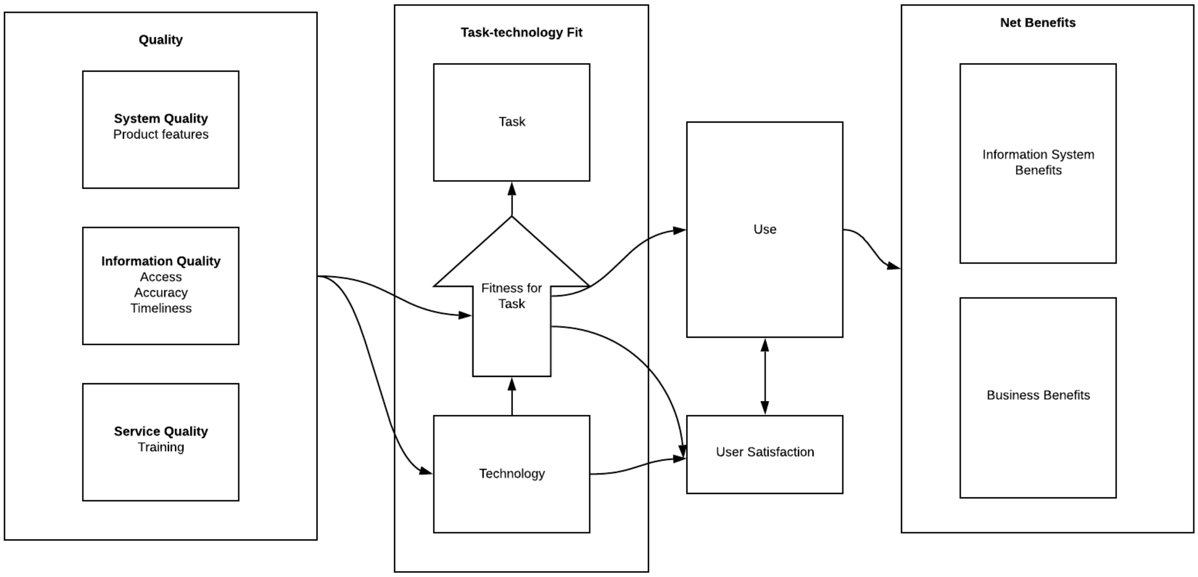

Figure 1. Blended IS Success/Task-technology Fit models

Thinking practically, organizations do not use information systems simply because they are of high quality, but because they meet organizational needs. Specific systems are selected or maintained because their quality, as related to accomplishing the task, is high. The actual fitness for the given task, in combination with the technology (as affected by system, information, and service quality) then drive use and user satisfaction, which then allow the organization to derive information system and business benefits from the technology. The other two themes from this study describe both quality measures and organizational benefits, as described by this Delphi panel.

Conclusions

Information systems are used by organizations for accomplishing many tasks. These systems emit logs to provide information about their inner workings, and log management systems manage these logs, making them available for use in a variety of tasks, such as software and system troubleshooting, or business and security reporting (Likhita & Sahoo, 2016). This study has found that system administrators and managers describe their systems in ways that reflect this task-oriented mind-set, reflecting the business- and system benefits provided and system- and business measures that describe the quality of these log management systems.

Through the qualitative analysis of the Delphi study, we introduce nine propositions to begin to build a theory for use of log management system. We presented a blended IS Success and Task-technology Fit model. Our model shows how quality measures feed into technology and task-fit, which then drive use and organizational benefits. Log management systems are widely utilized in the information systems, and this study helps explain why they are widely used and how they are measured for quality.

References

Adedayo, O. M., & Olivier, M. S. (2015). Ideal log setting for database forensics reconstruction. Digital Investigation, 12, 27–40. https://doi.org/10.1016/j.diin.2014.12.002

Ambre, A., & Shekokar, N. (2015). Insider threat detection using log analysis and event correlation. Procedia Computer Science, 45, 436–445.

Anastopoulos, V., & Katsikas, S. (2017). A structured methodology for deploying log management in WANs. Journal of Information Security and Applications, 34, 120–132.

Brady, S. R. (2015). Utilizing and adapting the Delphi method for use in qualitative research. International Journal of Qualitative Methods, 14(5), 1609406915621381.

ChePa, N., Jnr, B. A., Nor, R. N. H., & Murad, M. A. A. (2015). A review on risk mitigation of IT governance. Information Technology Journal, 14(1), 1.

Choi, I., Cantor, D. E., & George, J. (2017). Does IT Capability and Competitive Actions Shape Firm Profitability?

Chong, J. L. L., & Duong, L. N. K. (2017). Understanding IT Governance.

Coltman, T., Tallon, P., Sharma, R., & Queiroz, M. (2015). Strategic IT alignment: twenty-five years on. Springer.

Dalkey, N. C. (1969). The Delphi method: An experimental study of group opinion. RAND CORP SANTA MONICA CALIF.

Dalkey, N., & Helmer, O. (1963). An experimental application of the Delphi method to the use of experts. Management Science, 9(3), 458–467.

DeConinck, A., Nam, H. A., Morton, D., Bonnie, A., Lueninghoener, C., Brandt, J. M., … Vaughan, C. T. (2017). Runtime collection and analysis of system metrics for production monitoring of trinity phase ii. Sandia National Lab.(SNL-NM), Albuquerque, NM (United States).

DeLone, W. H., & McLean, E. R. (1992). Information systems success: The quest for the dependent variable. Information Systems Research, 3(1), 60–95.

Delone, W. H., & McLean, E. R. (2003). The DeLone and McLean model of information systems success: a ten-year update. Journal of Management Information Systems, 19(4), 9–30.

DeLone, W. H., & McLean, E. R. (2016). Information systems success measurement. Foundations and Trends® in Information Systems, 2(1), 1–116.

Dembla, P., Flack, C., & Petter, S. (2015). Extending the DeLone and McLean IS Success Model to Cloud Computing.

Devers, K. J., & Frankel, R. M. (2000). Study design in qualitative research--2: Sampling and data collection strategies. Education for Health; Abingdon, 13(2), 263.

De Villiers, M. R., De Villiers, P. J., & Kent, A. P. (2005). The Delphi technique in health sciences education research. Medical Teacher, 27(7), 639–643.

Döring, J. S., & Steffens, A. (2015). Towards Systematic Logging. Full-Scale Software Engineering, 7.

Goldkuhl, G. (2012). Pragmatism vs interpretivism in qualitative information systems research. European Journal of Information Systems, 21(2), 135–146.Goodhue, D. L., & Thompson, R. L. (1995). Task-technology fit and individual performance. MIS Quarterly, 213–236.

Hong, S. G., Trimi, S., Kim, D. W., & Hyun, J. H. (2015). A Delphi study of factors hindering web accessibility for persons with disabilities. Journal of Computer Information Systems, 55(4), 28–34.

Kabinna, S., Bezemer, C.-P., Shang, W., Syer, M. D., & Hassan, A. E. (2018). Examining the stability of logging statements. Empirical Software Engineering, 23(1), 290–333.

Karande, V., Bauman, E., Lin, Z., & Khan, L. (2017). Sgx-log: Securing system logs with sgx. In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security (pp. 19–30). ACM.

Kasiri, N., Sharda, R., & Hardgrave, B. (2012). A balanced scorecard for item-level RFID in the retail sector: A Delphi study. European Journal of Information Systems, 21(3), 255–267.

Keil, M., Lee, H. K., & Deng, T. (2013). Understanding the most critical skills for managing IT projects: A Delphi study of IT project managers. Information & Management, 50(7), 398–414.

Kisekka, V., & Giboney, J. S. (2018). The effectiveness of health care information technologies: Evaluation of trust, security beliefs, and privacy as determinants of health care outcomes. Journal of Medical Internet Research, 20(4), e107.

Kurniawan, K. (2018). Semantic Query Federation for Scalable Security Log Analysis. In European Semantic Web Conference (pp. 294–303). Springer.

Lemoudden, M., Bouazza, N., & Ouahidi, B. E. (2014). Towards achieving discernment and correlation in cloud logging. Proceedings of the Applications of Information Systems in Engineering and Bioscience, 202–207.

Li, J., Bajramovic, E., Gao, Y., & Parekh, M. (2016). Graded security forensics readiness of SCADA systems. Informatik 2016.

Likhita, G. G., & Sahoo, P. K. (2016). Log Management In Cloud Through Big Data. IJACTA, 4(1), 198–204.

Linstone, H. A. (1978). The Delphi technique. IN FOWLES, RB (Ed.) Handbook of Futures Research. Westport, CT., Greenwood.

Linstone, H. A., & Turoff, M. (1975). The delphi method. Addison-Wesley Reading, MA.

Mankoff, J., Rode, J. A., & Faste, H. (2013). Looking past yesterday’s tomorrow: using futures studies methods to extend the research horizon. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 1629–1638). ACM.

Miyamoto, D., & Iimura, T. (2014). PACKTER: implementation of internet traffic visualizer and extension for network forensics. Computing. Archives for Informatics and Numerical Computation; Wien, 96(1), 79–80. http://dx.doi.org.library.capella.edu/10.1007/s00607-013-0289-1

Muthurajkumar, S., Ganapathy, S., Vijayalakshmi, M., & Kannan, A. (2015). Secured temporal log management techniques for cloud. Procedia Computer Science, 46, 589–595.

Nakahara, S., & Ishimoto, H. (2010). A study on the requirements of accountable cloud services and log management. 8th Asia-Pacific Symposium on Information and Telecommunication Technologies, 1–6. IEEE.

Nagappan, M. (2011). A Framework for Analyzing Software System Log Files (Ph.D.). North Carolina State University, United States -- North Carolina. Retrieved from https://search-proquest-com.library.capella.edu/pqdtglobal/docview/881621601/abstract/5401B2E392534F89PQ/2

Nicho, M. (2012). An Optimized Dynamic Process Model of IS Security Governance Implementation. In CONF-IRM (p. 38).

Ojo, A. I. (2017). Validation of the DeLone and McLean Information Systems Success Model. Healthcare Informatics Research, 23(1), 60–66.

Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: an example, design considerations and applications. Information & Management, 42(1), 15–29.

Pare, G., Cameron, A.-F., Poba-Nzaou, P., & Templier, M. (2013). A systematic assessment of rigor in information systems ranking-type Delphi studies. Information & Management, 50(5), 207–217.

Paul, C. L. (2008). A modified delphi approach to a new card sorting methodology. Journal of Usability Studies, 4(1), 7–30.

Rabkin, A., & Katz, R. (2010). Chukwa: A system for reliable large-scale log collection. In Proceedings of LISA'10: 24th Large Installation System Administration Conference (p. 163).

Ribeiro, J., & Gomes, R. (2009). IT governance using COBIT implemented in a high public educational institution: a case study. In Proceedings of the 3rd international conference on European computing conference (pp. 41–52). World Scientific and Engineering Academy and Society (WSEAS).

Sauvé, J., Moura, A., Sampaio, M., Jornada, J., & Radziuk, E. (2006). An introductory overview and survey of business-driven IT management. In Business-Driven IT Management, 2006. BDIM'06. The First IEEE/IFIP International Workshop on (pp. 1–10). IEEE.

Sekaran, U., & Bougie, R. (2016). Research methods for business: A skill building approach. John Wiley & Sons.

Shaikh, A. A., Qi, H., Jiang, W., & Tahir, M. (2017). A novel HIDS and log collection based system for digital forensics in cloud environment. In Computer and Communications (ICCC), 2017 3rd IEEE International Conference on (pp. 1434–1438). IEEE.

Shang, W. (2012). Bridging the divide between software developers and operators using logs. In Proceedings of the 34th International Conference on Software Engineering (pp. 1583–1586). IEEE Press.

Shang, W. (2014). Log engineering: towards systematic log mining to support the development of ultra-large scale systems (PhD Thesis).

Shields, C., Frieder, O., & Maloof, M. (2011). A system for the proactive, continuous, and efficient collection of digital forensic evidence. Digital Investigation, 8, S3–S13.

Sinha, A. K., & Singh, V. (2016). Transformation of LOG file using LIPT technique. International Journal of Advanced Computer Research, 6(23), 58.

Soon, J. M., Davies, W. P., Chadd, S. A., & Baines, R. N. (2012). A Delphi-based approach to developing and validating a farm food safety risk assessment tool by experts. Expert Systems with Applications, 39(9), 8325–8336.

Tan, K., Baxter, G., Newell, S., Smye, S., Dear, P., Brownlee, K., & Darling, J. (2010). Knowledge elicitation for validation of a neonatal ventilation expert system utilising modified Delphi and focus group techniques. International journal of human-computer studies, 68(6), 344-354.

Thangaratinam, S., & Redman, C. W. (2005). The delphi technique. The Obstetrician & Gynaecologist, 7(2), 120–125.

Vega, C., Roquero, P., Leira, R., Gonzalez, I., & Aracil, J. (2017). Loginson: a transform and load system for very large-scale log analysis in large IT infrastructures. The Journal of Supercomputing, 73(9), 3879–3900.

Volchkov, A. (2013). How to measure security from a governance perspective. ISACA Journal, 5, 44–51.Wang, R., Ying, S., Sun, C., Wan, H., Zhang, H., & Jia, X. (2017). Model Construction and Data Management of Running Log in Supporting SaaS Software Performance Analysis. In SEKE (pp. 149–154).

Wang, R., Ying, S., Sun, C., Wan, H., Zhang, H., & Jia, X. (2017). Model Construction and Data Management of Running Log in Supporting SaaS Software Performance Analysis. In SEKE (pp. 149–154).

Wanko, C. E. T., Kamdjoug, J. R. K., & Wamba, S. F. (2019). Study of a Successful ERP Implementation Using an Extended Information Systems Success Model in Cameroon Universities: Case of CUCA. World Conference on Information Systems and Technologies, 727–737. Springer.

Weill, P., & Ross, J. W. (2004). IT governance: How top performers manage IT decision rights for superior results. Harvard Business Press.

Xu, W., Huang, L., Fox, A., Patterson, D., & Jordan, M. I. (2009). Detecting large-scale system problems by mining console logs. Proceedings of the ACM SIGOPS 22nd Symposium on Operating Systems Principles, 117–132. ACM.

Yakubu, M. N., & Dasuki, S. (2018). Assessing eLearning systems success in Nigeria: An application of the DeLone and McLean Information Systems Success Model. Journal of Information Technology Education: Research, 17, 183–203.

Yuan, D., Park, S., & Zhou, Y. (2012). Characterizing logging practices in open-source software. In Proceedings of the 34th International Conference on Software Engineering (pp. 102–112). IEEE Press.

Zartha, J. W., Montes, J. M., Vargas, E. E., Palacio, J. C., Hernández, R., & Hoyos, J. L. (2018). Methods and Techniques in Studies Related to the Delphi Method, Innovation Strategy, and Innovation Management Models. International Journal of Applied Engineering Research, 13(11), 9207–9214.

Zawoad, S., Dutta, A. K., & Hasan, R. (2013). SecLaaS: secure logging-as-a-service for cloud forensics. In Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security (pp. 219–230). ACM.

Zeng, L., Xiao, Y., Chen, H., Sun, B., & Han, W. (2016). Computer operating system logging and security issues: a survey. Security and Communication Networks, 9(17), 4804–4821.

Zhou, D., Yan, Z., Fu, Y., & Yao, Z. (2018). A survey on network data collection. Journal of Network and Computer Applications, 116, 9–23.

Zou, D., Qin, H., & Jin, H. (2016). UiLog: Improving Log-Based Fault Diagnosis by Log Analysis. Journal of Computer Science and Technology; Beijing, 31(5), 1038–1052. http://dx.doi.org.library.capella.edu/10.1007/s11390-016-1678-7

Appendix A – Coded topics

Round 1

- Log Management System Info
  - Q1-Log collection process
    - Automation
    - Centralized collection - 4
    - Defined process (specifics unspecified) - 2
    - Frequency - Daily
    - Keyword searching
    - Limited, manual process
    - Locally stored data

  - Manual process
  - Retained for 30 days
  - Shared location
  - Team-based collection
  - Tools used across entire business
  - Training being done
- Q1-Log sources
  - Application - 4
  - Hardware
  - Multiple sources (unspecified types)
  - Network - 2
  - Server - 3
  - Storage devices
- Q1-Platform
  - Unix
  - Windows - 3
  - Linux
  - Cloud-based - 4
- Q1-Software and hardware
  - Future plans [in the works]
  - Software
    - Multiple tools - unspecified
    - Commercial
      - Microsoft tools - unspecified
      - QRADAR (for Windows security analysis) - 2
      - SIEM
      - Solarwinds for WMI and SNMP
      - Splunk - 4
      - VCM (vCenter Config Mgr)
      - WinCollect for Windows
    - Home grown
      - Home-grown analysis software
      - Syslogd and home-grown scripts
    - Open Source
      - ELK stack
      - log4net
  - Hardware
    - Linux VMs for collection
    - Microsoft Azure cloud solution
    - Private cloud infrastructure
    - Unix hardware
    - Linux servers
  - Cloud
    - AWS
    - Azure - 2
    - IBM

- Unspecified provider

- Q2-Software (really Q1)
  - Log analysis tools
  - New Relic

Quality measurement

- Q2-Information quality
  - Used at all stages of development
  - Best practices
  - Compile logs for readability
  - Current correlation is poor
  - Current quality is acceptable
  - Current quality is good
  - Current sharing is poor
  - ITIL compliance
  - Never have accuracy issues
  - No way to measure information quality
  - Quality is important
  - Single place for data is important
  - Active measurement
    - Actively analyze logs
    - Automated validation
    - Manual monitoring
    - Trying to improve quality
    - Actively measure information quality
  - Things to measure
    - Accuracy
    - Completeness
    - Consistency
    - Meets dimensions of timeliness, accuracy, and completeness
    - (Referring to the dimensions given in the block description)
    - Timeliness
    - Validity of data
  - Too much high-quality data
- Q3-Information quality measures
  - Accuracy
  - Completeness - 3
  - Do not measure
  - Drive by systems and applications (?)
  - Ongoing review - 2
  - Security
  - Timeliness
- Q4-Service quality measurement
  - 3rd party support contract
  - Alerts
  - Customer measurement - 2

- Dashboards - 3
- New Relic
- (Did not understand the question) - 6
- Do not measure - 2
- Quality standards are set - 3
- Active measurement
  - Questionnaires
    - Questionnaires (to measure service quality) - 3
    - Surveys
    - Interviews
  - Personnel measure quality - 3
  - Monitored
  - Manual
  - Process step for quality
  - In-house quality measurement systems developed
  - Provide performance info to users
- Things to measure
  - Uptime

Q5-Service quality measurement

- Challenging to assess
- Active measurement
  - Personnel measure quality
  - Questionnaire
- Information is up-to-date
- No impact on user satisfaction - 2
- Service quality is important
- They have problems
  - They have problems in performance
  - They have problems in proactive work
  - They have problems in troubleshooting
  - They have problems with service quality

Q6-System quality measurements

- Continuous improvement
- Logs are evaluated
- No measurement
- System QE testing
- They do not do proactive testing
- Active measurement
  - Manual - 2
  - Monitoring - 2
  - Automatic - 3
  - Auditing
  - Automatic reports with manual review - 2
  - Interviews
- Things to measure
  - Accuracy - 2

Data correlation across systems
Data integrity - 2
Happy users - 2
Incomplete data
Performance - 5
Long term log storage
Dashboards
Q7-System quality measurement
No impact on user satisfaction
System quality is important – 2

Log Management System Benefits
Q1-log uses
Insight into applications and data
Monitoring and Alerting - 10
Performance monitoring - 3
Reporting - 4
Resource prioritization and utilization - 2
Security management - 2
Troubleshooting - 7
Q2-Benefits (really Q3)
Code quality
Compliance
Easy-to-use
Efficiency
End-user benefit
Improve operations
Improve organizational visibility
Log management benefits described (?)
Resource management
Security
Supports software design cycle
Q3-Information quality benefits
Benefits software development process (helps detect "project delays, failures, resource alignment, and other considerations")
Benefits system end-user experience - 2
Bug fixing - 2
Compliance reporting
Customer morale
Faster problem resolution
Monitoring and Alerting - 3
Performance - 2
Proactively find problems with system - 2
Process efficiency
Reporting - 2
Resource management

  - Security benefits - 2
  - Six sigma reporting
  - Troubleshooting - 6
  - User satisfaction is critical
  - Impact of Info Quality
    - Significant impact - 2
- Q4-Service quality benefits
  - Application understanding
  - Better decision making
  - Customer Trust - 2
  - Issues addressed quickly
  - Issues impact other systems
  - Monitor user behavior
  - Monitor web applications
  - Performance - 4
  - Proactive problem solving - 2
  - Reliability
  - Service improvement
  - Troubleshooting - 6
  - Understanding impacts of issues
  - Customer satisfaction
    - Assess client satisfaction
    - Better customer interactions
    - Customer satisfaction with help desk - 2
    - End-user confidence in platform
    - SLA measurement
- Q7-System quality benefits
  - Allows automation
  - Customer satisfaction
  - Improved compliance
  - Improved operations
  - Improved uptime
  - Improved decision-making
  - Long-term system stability
  - Measured against design goals
  - Proactive notification
  - Provides Service level agreement values
  - Reduced risk
- Q8-Net benefits
  - Easier troubleshooting
  - Faster problem resolution
  - Find configuration issues
  - Find performance issues
  - Identify security issues
  - Improved monitoring
  - Improved software quality

- Inconvenient
- Increased efficiency of systems
- Lack of system does not provide benefits
- Logs enhance customer experience
- Monitoring
- Net benefits make effort worthwhile
- No impact
- Prevent downtime
- Prove regulatory compliance
- Provide SLA measurements
- Provide high level of service
- Provide SLAs to customers
- Success of system depends on consideration during design process
- Troubleshooting
- User satisfaction provides feedback to improve systems

Round 2

- Choice considerations
  - Future
    - Company-specific needs - 2
    - Daily work usefulness - 2
    - Ease of implementation - 2
    - Empower to gain insights
    - Growth
    - Improve work efficiency
    - Multi-team needs - 2
    - Product evaluations
    - Resolve issues quickly
  - Past
    - Chosen by team leaders
    - Cost - 3
    - Dashboarding
    - Ease of use - 4
    - Evaluated by upper management
    - Features - 4
    - Vendor support
- Fully utilized
  - Middle ground
    - Room for improvement - 4
    - Still being determined
    - Yes because there is no other option
    - Yes in some areas, no in others
  - No - 10
  - Not sure
  - Yes - 14

- LMS success measure
  - Business results
    - Ability to identify problems - 2
    - Good results - 5
    - Meets organization needs
    - Troubleshooting effectiveness
    - User satisfaction
  - Data-related
    - Data access - 4
    - Data accuracy - 2
    - Data timeliness
      - Following the progress
      - Up-to-date?
  - Do not know - 2
  - Financial
    - Low TCO
    - ROI
  - System-related
    - Able to filter non-relevant values
    - Configurable
    - Easy to maintain
    - Log centralization
    - Reliability - 2
    - System performance - 3
  - Usability
    - Efficiency of use
    - Ease of use - 4
- System choice
  - How
    - Community decision
    - Government best value selection process
    - Home grown
    - Multi-organization group decision
  - In place a log time - 2
  - Who
    - Chosen by dedicated team - 2
    - Chosen by parent company
    - IT committee - 3
- What would you change?
  - Do not know
  - Implementation
    - Customize for organization needs - 0
    - Process
      - Consolidate to single system
      - Improve security
      - More accessible

- More rights to users
- Reduce processes
- Stricter controls
- Lower TCO
- No changes - 5
- Product
  - Add AI features
  - Add security alerting
  - Easier maintenance
  - Enhance for notifications - 2
  - Improve data validity
  - Improve performance - 5
  - Improve reliability
  - Make it easier to use - 5
  - More automation
- Training

Round 3

Q1. What would they change in current LMS?

- Business outcomes
  - Business processes most important
  - Increased efficiency
  - Product increases security
  - Product minimizes risk
- Continuing improvement of system
- Current implementation is poor
- Priorities
  - Features are most important - 2
  - Product implementation is most important - 5
- Product features
  - Access to logs
  - Additional alerting
  - Analysis tools
  - Data accuracy - 2
  - Data timeliness
  - Documentation is important
  - Easier reporting
  - Improve disparate systems information
  - Improved documentation
    - Good documentation
    - Quick guide
  - Product features
  - Security of logs and log systems (CIA)
  - Usability - 2