**1. How did the authors use both Qualitative and Quantitative assessment approaches? What benefits did each approach yield?**

**Use of Qualitative Methods**

Spears and Barki (2010) began with a qualitative exploratory study by conducting semi-structured interviews with eleven informants across five organizations. These interviews helped the authors:

* Develop an in-depth understanding of how organizations approached Sarbanes-Oxley (SOX) compliance and, specifically, Information Systems (IS) Security Risk Management (SRM).
* Identify how, where, and to what extent “users” (i.e., non-IT business stakeholders) actually participated in security risk processes and how that participation influenced business processes and controls.
* Capture rich narratives of real-world practices in different industries and firm sizes, thereby grounding their subsequent model in empirical reality.

A core benefit of taking this initial qualitative approach was establishing *contextual richness*: the interviews revealed specific tasks (e.g., process documentation, user access reviews, segregation of duties) that helped inform the subsequent design of surveys regarding user participation in SRM. Such detail is often difficult to capture through purely survey-based or quantitative methods (Newman, 2007; Urquhart, 2001).

**Use of Quantitative Methods**

Spears and Barki (2010) conducted a confirmatory quantitative survey of 228 ISACA members involved in SOX compliance. This survey allowed them to:

* Test the model and hypotheses they had generated from the qualitative phase.
* Statistically validate the relationships among user participation, organizational awareness of security, alignment between security and the business, and control outcomes (e.g., improved control development, reduced deficiencies).

The benefits of the quantitative method include:

* **Triangulation**: By cross-referencing results from interviews with statistical findings, they increased confidence in their conclusions (Kaplan & Duchon, 1988; Mingers, 2001).
* **Measurable Evidence**: The survey showed how much variance in outcomes (such as control performance) could be explained by user participation.
* **Broader Applicability**: Large-sample, multi-industry data provided a stronger empirical foundation for concluding that user participation improves security controls and awareness in an SOX (and similar) context (Sawyer, 2001).

Combining qualitative and quantitative approaches (so-called *mixed methods*) provided Spears and Barki (2010) with evidence of how user participation impacts security risk management—both measurable *and* rooted in real-world context.

**2. What do the authors list as the advantages of involving users in the risk management process?**

Spears and Barki (2010) found multiple advantages of user participation, including:

1. **Raised Organizational Awareness of Security Risks and Controls**  
   Users who participated in documenting business processes, testing controls, or approving access requests exhibited greater awareness of threats and safeguards (Furnell, 2008; Siponen, 2000). This understanding often led to proactive behaviors—such as questioning suspicious access requests or highlighting anomalies.
2. **Alignment of Security Measures with Business Objectives**  
   Users bring contextual business knowledge about how, where, and why sensitive data are processed (Halliday et al., 1996). This “business-aligned SRM” ensures that security controls are both feasible to implement and tailored to specific workflows.
3. **Accountability and Role Clarity**  
   Participation often goes hand in hand with establishing formal accountability (e.g., designating “control owners,” “data stewards”). These new roles shift security from an IT-only function to a shared organizational responsibility (ITGI, 2005).

In essence, involving users in SRM engages them both cognitively and practically, thereby strengthening the security posture overall (D’Arcy, Hovav, & Galletta, 2009).

**3a. How will the lack of user access affect the risk assessment I will carry out?**

Because Pampered Pets is entirely fictitious, I can’t draw on real staff experiences. This forces me to rely on *assumed* workflows and security habits, which might not fully reflect a real-world setting.

* **Skewed Risk Prioritization**  
  Specific details—like the warehouse computer’s software status or how staff actually handle emailed orders—are unknown. Consequently, some risks may be overstated, while others remain unaccounted for.
* **Incomplete Realism**  
  While I can map typical threats for small retail stores, the absence of genuine input means the assessment is theoretical and may not capture the nuance of a real world operation.

**3b. Will it affect my choice of Qualitative vs. Quantitative methods?**

Yes, it will absolutely affect my approach to the assignment. Without real interviews or data logs, I have to rely largely on secondary sources such as industry research into SME cybersecurity and risks, standard risk frameworks (e.g. NIST SP 800-30) and academic papers regarding supply chain risks. Rather than using primary data, my assessment will be based on the best practises, common vulnerabilities and effective mitigation strategies that I encounter via these secondary sources.

**3c. How might I mitigate any issues encountered?**

1. **Use Representative Industry Examples**
   * Examine case studies of comparable small businesses transitioning to partial digital operations.
2. **Apply a Structured Framework**
   * Follow recognized approaches to identify and classify threats, even if the specifics are hypothetical.
3. **Clearly State Assumptions**
   * Each conclusion should note which details are inferred or general, emphasizing this is a theoretical scenario without actual user participation.

Given the inherent limitations to the assignment, my assessment will be strictly academic in nature and will lack the depth you’d expect from a real world report. However, I’m confident I can still produce a high quality and well supported risk assessment within these constraints.

**References**  
Alberts, C., & Dorofee, A. (2003). *Managing Information Security Risks: The OCTAVE Approach.* Addison-Wesley.

D’Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79–98.

Furnell, S. (2008). End-user security culture: A lesson that will never be learnt? *Computer Fraud & Security, 2008*(4), 6–9.

Halliday, S., Badenhorst, K., & von Solms, R. (1996). A business approach to effective information technology risk analysis and management. *Information Management & Computer Security, 4*(1), 19–31.

ITGI. (2005). *COBIT 4.0.* IT Governance Institute.

Kaplan, B., & Duchon, D. (1988). Combining qualitative and quantitative methods in information systems research: A case study. *MIS Quarterly, 12*(4), 571–586.

Mingers, J. (2001). Combining IS research methods: Towards a pluralist methodology. *Information Systems Research, 12*(3), 240–259.

Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and Organization, 17*(1), 2–26.

Sawyer, S. (2001). Analysis by long walk: Some approaches to the synthesis of multiple sources of evidence. In E. M. Trauth (Ed.), *Qualitative Research in IS: Issues and Trends* (pp. 163–189). Idea Group.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31–41.

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly, 34*(3), 503–522.

Urquhart, C. (2001). An encounter with grounded theory: Tackling the practical and philosophical issues. In E. M. Trauth (Ed.), *Qualitative Research in IS: Issues and Trends* (pp. 104–140). Idea Group.