Post UNIT 2 Seminar – Review

UNIT 2 Seminar – Activities / Evidence

1. **Create a table with qualitative and quantitative assessments used by Spears & Barki (2010). What benefits did each approach yield?**

Approach	How Spears & Barki (2010) used the approach	Benefits
Qualitative	Semi-structured interviews with 11 informants across 5 organisations to explore user participation activities, roles, and outcomes.	• Provided rich contextual insights that enabled theory-building. • Generated categories and constructs used to develop the survey instrument.
Quantitative	Survey of 228 ISACA members, with items developed from the qualitative findings, analysed using statistical methods.	• Produced measurable and generalisable evidence of relationships. • Enabled statistical testing and validation of the proposed model.
Mixed method	The qualitative results were used to build the survey instrument, and the subsequent quantitative survey tested and validated the model.	• Combining both phases allowed findings to be validated from multiple angles. • Strengthened the credibility and robustness of overall conclusions.

Pilcher (2024) notes that research methods textbooks, such as Punch (2005) and Bell and Waters (2014), often present quantitative research as objective, numerical, and structured, and qualitative research as subjective, exploratory, and interpretive — treating them as independent and binary. In practice, however, Pilcher argues these boundaries are blurred and interdependent. Spears and Barki (2010) illustrate this overlap clearly, since their “quantitative” survey was not independent but directly built on insights from the earlier “qualitative” interviews, showing how the two approaches can be mutually reinforcing rather than separate.

2. Create a table that analyses user participation in the Risk Management process based on Spears & Barki (2010).

User Participation in Security Risk Management Activities	Description based on Spears & Barki (2010)
A1: Business process workflow	Users documented and mapped their business processes to show how information flowed, providing the basis for identifying risks.
A2: Risk-control identification	Users identified risks in workflows and matched them with appropriate controls, flagging missing or weak controls.
A3: Control design	Users provided input on how controls should be structured so they were practical and workable in daily business operations.
A4: Control implementation	Users carried out security controls as part of their daily tasks, ensuring they were embedded in operations.
A5: Control testing	Users tested controls in practice to verify that they worked as intended before audits.
A6: Control remediation	Users created and applied remediation plans to fix failed controls and retested them after adjustments.
A7: Communication	Users communicated security policies and procedures to colleagues to ensure compliance and awareness.

User Participation in Security Controls	Description based on Spears & Barki (2010)
A8: Access control	Users reviewed and approved access rights for systems and applications.
A9: Segregation of duties	Users enforced separation of responsibilities to reduce fraud and error.
A10: Alerts and triggers	Users defined, reviewed, and responded to system alerts that signalled potential security issues.

A11: Exception reports	Users reviewed exception reports and investigated unusual or suspicious activities.
A12: End-user computing	Users protected spreadsheets and end-user applications with controls (e.g., passwords) and validated their accuracy.
A13: Training	Users participated in and sometimes delivered training to reinforce security practices.
A14: Risk tolerance	Users defined and approved acceptable levels of risk within their business areas.

User Participation via Accountability	**Description based on Spears & Barki (2010)**
A15: Roles and responsibilities documented	Users' security responsibilities were formally documented in policies and role descriptions.
A16: Roles and responsibilities assigned	Users were formally assigned responsibility for specific aspects of information security.
A17: Control owners designated	Individual users were made accountable for the effectiveness of specific security controls.
A18: Senior management review	Senior users and executives regularly reviewed security policies and practices.
A19: IS security policy committee	Users served on policy committees with IT staff to jointly decide security strategies.
A20: Executive business support demonstrated	Executives actively endorsed and supported security initiatives, reinforcing user accountability.
A21: IT-user committees used	Users participated in cross-functional committees with IT staff to oversee and guide security governance.

3. Create a list of risk management phases where user participation in the risk management process is difficult to maintain

A1: Business process workflow

Mapping workflows manually is time-consuming and costly, requiring detailed process knowledge from users.

A2: Risk-control identification

This process is resource-heavy, requires specialised expertise, and is prone to inconsistency because it depends on subjective human judgment (Wang and Boukamp, 2011).

A4: Control implementation

Embedding and executing controls consistently in daily work is challenging due to staff turnover, compliance fatigue, and resource limits.

A5: Control testing

Manual testing is time-intensive and often skipped due to resource constraints, leading to weak assurance.

A6: Control remediation

Creating and coordinating remediation plans requires significant time and cross-team resources, slowing down response.

A8: Access control

Reviewing and approving access rights is repetitive and costly to maintain across large organisations..

A9: Segregation of duties

Monitoring SoD compliance across multiple systems is complex and resource-heavy.

A10: Alerts and triggers

High volumes of alerts overwhelm users, leading to “alert fatigue” and missed risks.

A11: Exception reports

Reviewing large volumes of exception reports is time-consuming and unsustainable for users.

A12: End-user computing

Manually protecting and validating spreadsheets is repetitive and error-prone, especially at scale.

4. Create a list of possible mitigations for each phase and the phase you cannot mitigate

Phase	Mitigations	Can AI mitigate?
A1: Business process workflow	Standardised workflow documentation templates; additional staff training in process mapping; periodic peer reviews.	**Partially** – AI can map workflows from digital systems, but tacit business knowledge and exceptions still require users.
A2: Risk-control identification	Cross-functional workshops to share expertise; use of checklists or control libraries; regular internal audits.	Partially - AI can suggest controls via pattern recognition, but user judgment is needed to align risks with business context
A4: Control implementation	Strengthen policies and accountability; increase staffing or role clarity; provide ongoing compliance training.	Not replaceable – requires contextual, organisational, and human-centred judgment to ensure controls are workable
A5: Control testing	Internal audit rotation schemes; standardised test procedures; allocate dedicated compliance staff.	Partially– AI can automate technical enforcement, but users must perform process-based and behavioural controls.
A6: Control remediation	Clear escalation pathways; remediation playbooks; stronger project management for fixes.	Partially – AI can automatically suggest corrective actions, or enforce policy resets, but human oversight is required to approve and coordinate fixes.
A8: Access control	Regular access review cycles; role-based access policies; enforcing segregation of duties through governance.	Partially– AI can automate access provisioning and anomaly detection, but user oversight is needed for exceptions
A9: Segregation of duties	Regular audits; clear job descriptions; staff rotation to minimise conflicts of interest.	Partially– AI can monitor SoD violations, but management decisions require users.
A10: Alerts and triggers	Tiered escalation processes; staff training to handle alerts; allocate more resources to monitoring teams.	Partially– AI can generate alerts, but users must interpret their business relevance.
A11: Exception reports	Risk-based prioritisation of reports; allocate additional staff to review; standardised reporting formats.	Partially– AI can filter anomalies, but human investigation remains essential.
A12: End-user computing	Establish strict policies for spreadsheets; provide training in secure spreadsheet use; implement peer review controls.	Partially– AI can enforce protections, but validation of business-specific content requires users.

5. **Create a table of RM phases where AI can be utilized in RM.**

Phase	AI Type	How AI can be utilised in RM
A1: Business process workflow	Machine Learning (process mining)	Spears & Barki (2010) observed that users manually documented workflows to identify risks. Caron, Vanthienen and Baesens (2013) show that process mining techniques can automatically extract and visualise workflows from event logs, making the process more efficient and accurate, while users still validate exceptions and tacit knowledge.
A2: Risk-control identification	Machine learning	Machine learning models can mitigate the resource-heavy and inconsistent nature of manual risk–control identification by learning from historical security assessment data and recommending appropriate security controls for new risks, thereby reducing workload and improving consistency while still requiring user validation (Bettaieb et al., (2020).
A5: Control testing	Generative AI, neural networks, and graph-based AI	Ramachandran (2024) shows that AI can enhance control testing by automating verification through anomaly detection, continuous monitoring, and intelligent audit procedures, thereby reducing manual effort while improving assurance.
A6: Control remediation	Case-Based Reasoning (CBR)	AI can support remediation by automatically suggesting corrective actions, or enforcing policy resets (e.g., restoring secure configurations)
A8: Access control	Behavioural Analytics	AI-driven systems automate access provisioning and detect anomalous user behaviour, requiring human oversight for exceptions.
A9: Segregation of duties	Machine Learning	Continuously monitors for segregation-of-duties violations across systems.
A10: Alerts and triggers	Predictive Analytics and Natural Language Processing (NLP)	Filter and prioritise security alerts to reduce alert fatigue, while users interpret business relevance.
A11: Exception reports	Machine Learning	Classifies exception reports and highlights anomalies for investigation, reducing user workload.
A12: End-user computing	Rule-Based AI	Enforces spreadsheet protections and detects anomalies, though business-specific validation stays human.

6. List additional tools that you could utilise in each phase

- **Celonis**: Process mining software for mapping and analysing workflows automatically.
- **Power BI**: Analytics and visualisation tool for assessing control performance and risk indicators.
- **Splunk**: Security Information and Event Management (SIEM) tool that aggregates and analyses security alerts.
- **Okta**: Identity and Access Management (IAM) system that automates user provisioning and enforces access controls.
- **Jira**: Workflow and issue-tracking tool for managing remediation and audit follow-ups.
- **Cyber Kill Chain Tools** (e.g. Metasploit, Maltego): Used to simulate attack phases and support intelligent-driven risk assessment.

7. Create a slide deck presentation with up to 4 slides that discuss your solution

Refer to PPTX.

8. Create a list of additional references you have reviewed.

Bell, J. and Waters, S. (2014) *Doing your research project: a guide for first-time researchers*. 6th edn. Maidenhead: Open University Press.

Bettaieb, S., Shin, S. Y., Sabetzadeh, M., Briand, L. C., Garceau, M. and Meyers, A. (2020) 'Using machine learning to assist with the selection of security controls during security assessment', *Empirical Software Engineering*, 25(4), pp. 2550–2582. Available at: https://doi.org/10.1007/s10664-020-09814-x (Accessed: 05 September 2025).

Caron, F., Vanthienen, J. and Baesens, B. (2013) 'A comprehensive investigation of the applicability of process mining techniques for enterprise risk management', *Computers in Industry*, 64(4), pp. 464–475. Available at: https://doi.org/10.1016/j.compind.2013.02.001 (Accessed: 05 September 2025).

Pilcher, N. and Cortazzi, M. (2023) '"Qualitative" and "quantitative" methods and approaches across subject fields: implications for research values, assumptions, and practices', *Quality & Quantity*, 58, pp. 2357–2387. Available at: https://doi.org/10.1007/s11135-023-01734-4 (Accessed: 13 August 2025).

Punch, K.F. (2005) *Introduction to social research: quantitative and qualitative approaches*. 2nd edn. London: SAGE.

Ramachandran, A. (2024) *The transformative impact of artificial intelligence on controls audit procedures and testing: A comprehensive analysis of risks, methodologies, and emerging best practices in the AI era*. Available at: https://www.researchgate.net/publication/382465491_The_Transformative_Impact_of

_Artificial_Intelligence_on_Controls_Audit_Procedures_and_Testing_A_Comprehensive_Analysis_of_Risks_Methodologies_and_Emerging_Best_Practices_in_the_AI_Era (Accessed: 05 September 2025).

Spears, J.L. and Barki, H. (2010) 'User participation in information systems security risk management', *MIS Quarterly*, 34(3), pp. 503–522. Available at: https://www.jstor.org/stable/25750689 (Accessed: 03 August 2025).

Wang, H. and Boukamp, F. (2011) 'Ontology-based representation and reasoning framework for supporting job hazard analysis', *Journal of Computing in Civil Engineering*, 25(6), pp. 442–456. Available at: https://doi.org/10.1061/(ASCE)CP.1943-5487.0000125 (Accessed: 05 September 2025).