RACI Table – Task: Monthly System Patching

Subtask	R (Responsible)	A (Accountable)	C (Consulted)	I (Informed)
Schedule Maintenance Window	IT Scheduler	IT Supervisor	Department Heads	End Users
Test Patch in Staging Environment	System Admin	IT Supervisor	Security Analyst	QA Team
Apply Patch in Production	Tier 2 Engineer	IT Supervisor	DevOps Lead	Management Team
Validate System Performance	QA Lead	Supervisor	Tier 2 & Tier 3 Teams	Stakeholders
Document Patch Results & Rollback	Documentation Analyst	IT Supervisor	Security Team	All IT Staff

Patch management in a patching process is a high-impact and repetitive process in IT environments, where a RACI chart specifies strong ownership. Applying the concept of Responsible duties to technicians (e.g., Tier 2 Engineers), Accountability is delegated to the IT Supervisor to ensure deadlines are met and patching does not interfere with operations. DevOps and Security are among the stakeholders consulted regarding risk or testing (Buene & Fridtun, 2022). The Informed category maintains transparency among the teams and executives. This makes it clear and curtails misunderstandings as well as accelerates resolution in the event of failures or rollbacks. This disjuncture in ownership can inflate the

number of tickets and postpone fixes, as seen in your examples of the escalation matrix and ticketing. Such a RACI model, combined with key systems KPIs like Uptime% and Ticket Backlog, enables leaders to monitor not only the path but also the results of patch cycles (Iacob, 2023). It helps harmonize various functions and ensure continuity in service delivery, an important attribute of leaders in systems management.

References

Buene, K. F., & Fridtun, H. T. (2022). *Investigating trust relationships between software development teams and information security stakeholders* (Master's thesis, NTNU). https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/3023694

Iacob, A. (2023). Analysis of business processes for the detection of improvements. https://core.ac.uk/download/pdf/588553102.pdf