2. RACI Chart – System Patching Process

Task	IT Supervisor	System Admin	Security Analyst	Support Team
Identify systems to patch	A	R	C	I
Sandbox patch testing	I	R	C	I
Approve release	A	C	R	I
Schedule downtime	R	A	C	I
Notify impacted users	A	I	I	R
Monitor patch results	I	R	A	C
Log outcomes & resolution	R	C	I	A

The above RACI chart identifies the areas of division in tasks and the responsibilities of the system patching lifecycle. It promotes proper teamwork by removing doubts and duplication of functions. The IT Supervisor ensures that all actions taken are within the law and adhere to operational policies. It is the System Administrator who installs and tests the patches, ensuring that each patch meets the security requirements identified by the Security Analyst (Dissanayake et al., 2022). The no-direct-funding Support Team helps with notifying the users and verifying the system. This allows for the patch rollout and does not affect uptimes or compliances. Security-related input is also generated through a well-outlined consultation, without compromising efficiency in implementation. Such a structure is crucial for maintaining SLA performance and minimizing disruptions to businesses (Gupta & Anika, 2023). It also enables auditability and policy compliance, which are important characteristics of good leadership and effective governance.

References

Dissanayake, N., Zahedi, M., Jayatilaka, A., & Babar, M. A. (2022). Why, how and where of delays in software security patch management: An empirical investigation in the healthcare sector. *Proceedings of the ACM on Human-computer Interaction*, *6*(CSCW2), 1-29. https://dl.acm.org/doi/abs/10.1145/3555087

Gupta, S., & Anika, M. N. A. I. (2023). Digital security monitoring of cloud services-SLA Analyser-Availability Monitoring tool for DB Cloud Services. https://www.diva-portal.org/smash/record.jsf?pid=diva2:1791438