Initial Findings

- Secure all contracts with third party vendors immediately
- Develop a strong understanding of the 'Flow of PHI' within and outside of the hospital (if you don't know where it goes, you cannot maintain its privacy and provide adequate security)
- Establish better communications amongst all HIPAA Team Members and throughout the hospital.
- Create physical and information security policies and procedures. Educate all staff. Institutionalize this training (HR).
- Remove 'Discards' from the hallway in the old building. The discards contain PHI and are accessible from both inside and out.
- Medical Records room (dictation) needs to be secured at all times since PHI is fully accessible and there is no one to prevent entry.
- Secure all non-essential hospital external access doors at all times.
- Establish patch management program for server and maintain proper patch levels.

Initial Findings

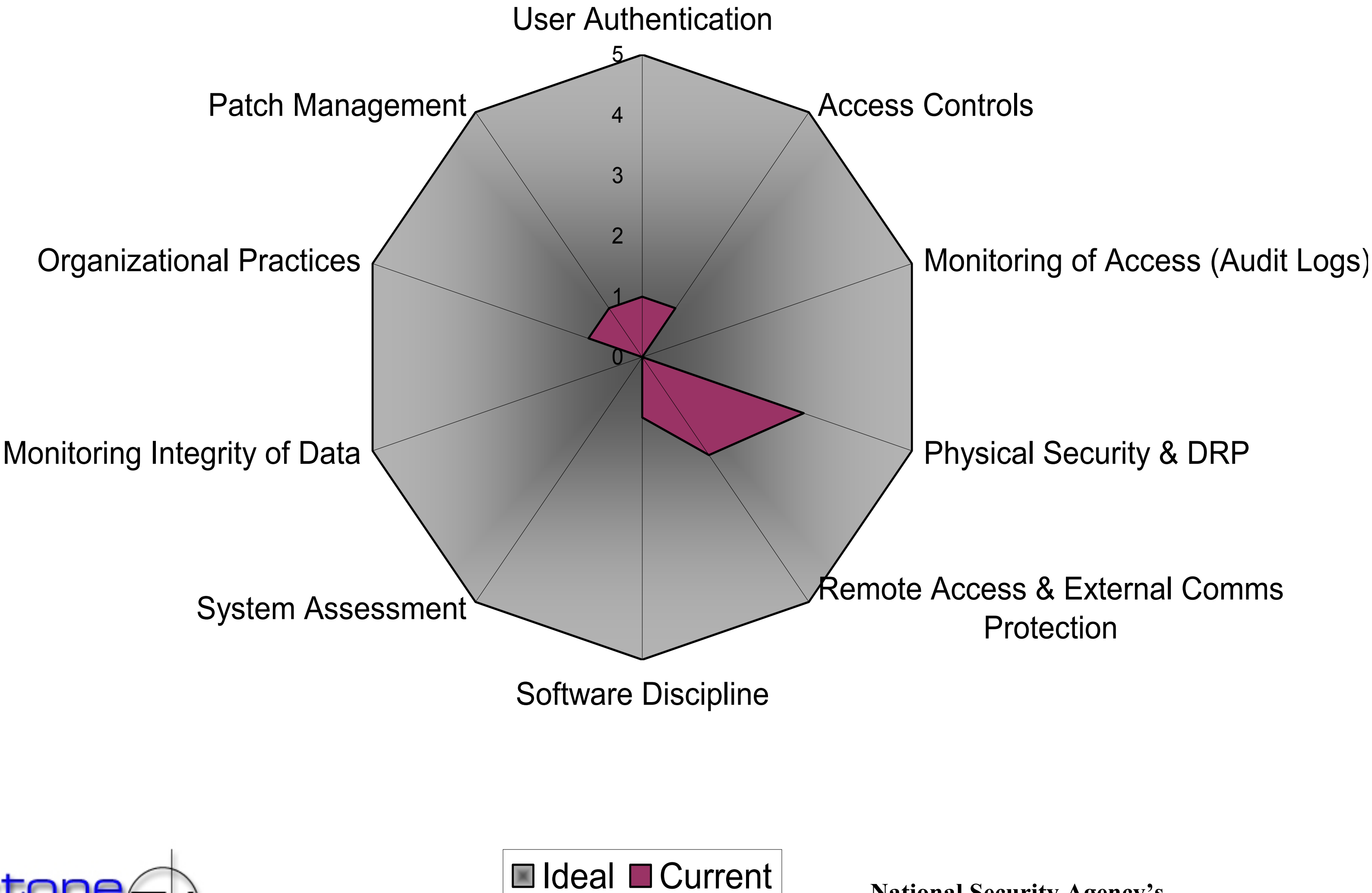
- Heliport needs to be cleared of vehicles at all times versus an after-the-fact removal of vehicles.
- Take backups offsite for storage on all critical systems.
- Asset management inventory of all IT hardware and software (if you don’t know what it is, you cannot secure it).
- Stop the practice of faxing lab information to non-securely located fax machines and to non-essential personnel. Principle of least privilege applies.
- Create and maintain network diagrams.
- Establish a password management program with strong passwords and 60 day changes.
- Provide external storage to critical systems

Initial Findings

- Ensure anti-virus software is on all critical servers.
- Establish electronic audit logs and event monitoring.
- Review the use of modems to critical systems as a vendor method for updating and maintenance as an appropriate method of access. Identify capability of audit logs for the modems.
- Create a video surveillance policy and educate staff on the uses of this security solution.
- Principle of Least Privilege needs to be applied online and in physical security situations.

ScoreCards

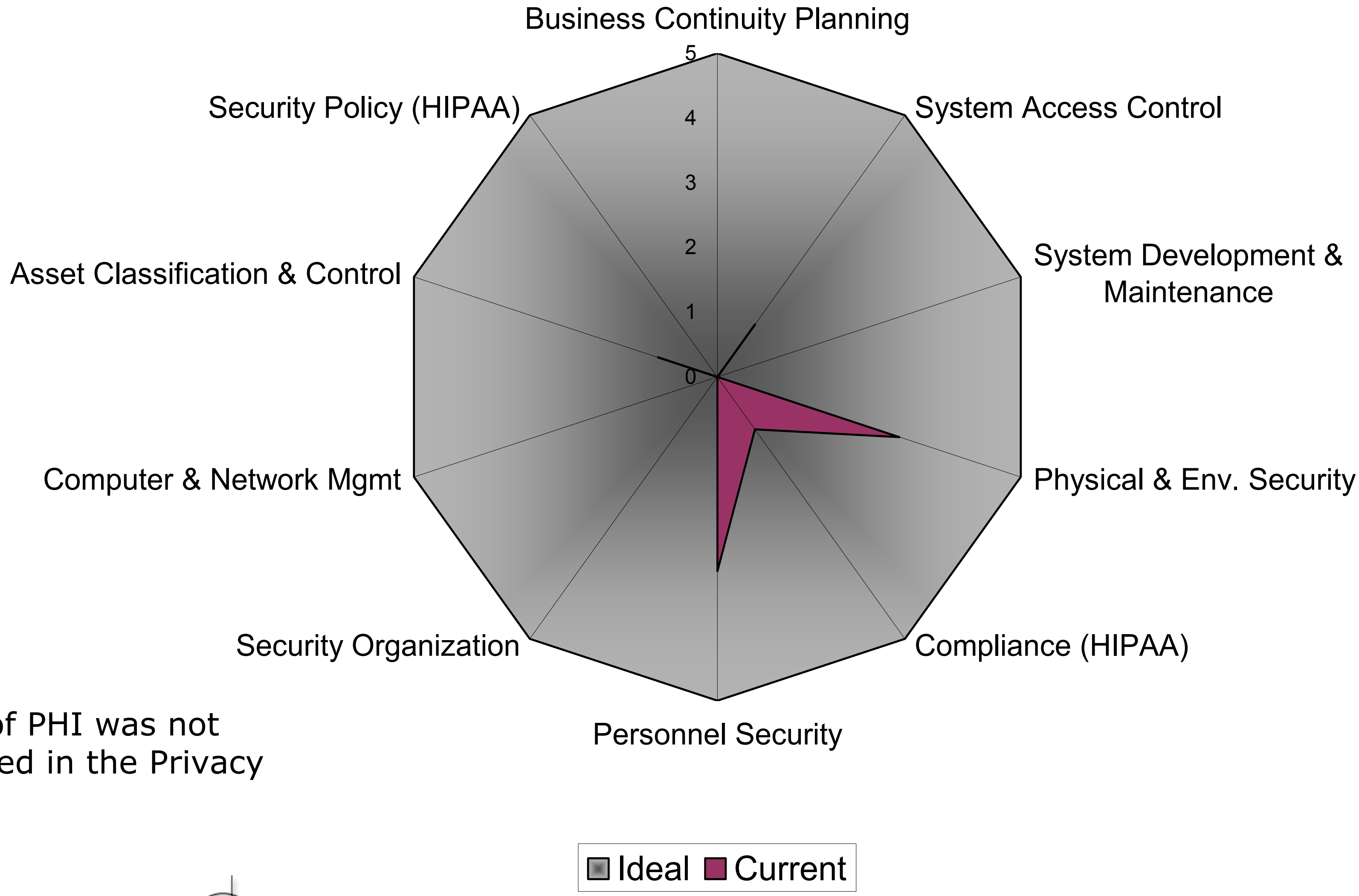
0 **Non-Existent** — Management processes are not applied at all
1 **Initial** — Processes are ad hoc and disorganized
2 **Repeatable** — Processes follow a regular pattern
3 **Defined** — Processes are documented and communicated
4 **Managed** — Processes are monitored and measured
5 **Optimized** — Best practices are followed and automated



National Security Agency's

ScoreCards

0 **Non-Existent** — Management processes are not applied at all
1 **Initial** — Processes are ad hoc and disorganized
2 **Repeatable** — Processes follow a regular pattern
3 **Defined** — Processes are documented and communicated
4 **Managed** — Processes are monitored and measured
5 **Optimized** — Best practices are followed and automated



Flow of PHI was not included in the Privacy effort