**Team: Kompliance Krew**

GLBA In Class Exercise:

1. Does your WISP entail the security of NPI, regular risk assessments, at least annual updation and regular maintenance, training of employees for GLBA compliance, have a DR and BCR plan enclosed?
2. What is SMSB's process for responding to data breaches or security incidents? How are incidents documented and reported, both internally and to regulators, if necessary?
3. Does SMSB maintain an up-to-date inventory of all systems and their life cycles, including planned end-of-life dates and How does SMSB ensure that decommissioned systems are securely disposed of, and what documentation or evidence is maintained?
4. How does SMSB ensure the security and confidentiality of all Personally Identifiable Information (PII) and it retains, including measures to protect PII against anticipated threats or hazards, and prevent unauthorized access or use that could result in identity theft, fraud, or other harmful outcomes in application nearing end-of-life or sunset?
5. What measures does SMSB have in place to protect customer information as per GLBA requirements after an application’s end of life?
6. How does SMSB assess the compliance of third-party vendors handling customer information?
7. Does the GLBA annual report contain

* The status of the information security program
* Risk assessment summary and any material issues discovered
* Risk management and control decisions
* Service provider arrangements
* Any security violations and actions taken in response

(What if the organization changed the system midway through the year, do they report the statuses of the older and newer systems ?)