

Health Information Compliance Alert

Reader Question: What Are Some Tips To Elicit More Support For Risk Management?

Question: How can I get support from management for my risk management program?

Answer: This is a very common question. **Bob Chaput, MA, CISSP, HCISPP, CRISC, CIPP/US**, provided the following suggestions in a recent blog posting for Clearwater Compliance LLC:

1. Get a friend on the executive team. If you don't already have an ally in the boardroom, align yourself with someone on the executive team. Try to secure a friend in the "C-suite" who understands risk management, such as your organization's legal counsel, CFO, Medical Officer, or COO, Chaput suggested.

2. Don't harp on "compliance." When you're talking with management about risk, talk about "patient safety" and "quality of care" instead of "compliance," Chaput recommended. "Talk about how the confidentiality, integrity and availability of health information is critical to patient safety and quality of care."

3. Set up a risk management oversight council or committee. According to Chaput, the council or committee should be responsible for:

- Providing strategic direction relative to risk philosophy;
- Establishing the authority, responsibility and accountability of the risk management program;
- Setting the organization's risk appetite;
- Understanding the level of risk in the organization and the impact of the consequences;
- Approving initiatives to reduce or mitigate that risk;
- Ensuring adequate resources to achieve initiatives;
- Providing high-level support for initiatives;
- Being aware of compliance issues and remediation; and
- Ensuring that risks are managed appropriately.

4. Establish a risk management working group. According to Chaput, this should be a cross-functional group that's responsible for:

- Implementing an effective coordinated risk management program, ensuring documented policies and procedures, training the workforce, determining sanctions for violations, establishing incident reporting procedures, and managing Business Associates.
- Mitigating gaps or weaknesses uncovered during compliance assessments and/or risk analyses.
- Keeping the oversight council informed on results and mitigation activities, as well as regulatory changes, trends in incidents and/or breaches, results of compliance audits, workforce training, and progress on remediation plans.

5. Align your recommendations with business strategy. Ensure your recommendations will improve the protection of health information but won't disrupt operations unnecessarily, Chaput recommended. "Focus your compliance and security recommendations on ensuring customer trust and creating a competitive advantage."