Part Two – Making Sure Your Compliance Armor is Strong!

Protecting your center mass; how much should your cuirass cover?

By Kassia Holt, CRCM, CBAP

Recently I introduced the concept of protecting your bank with a strong compliance management system with four layers of protection provided by a suit of armor. Between the 14th and 17th centuries, a suit of armor was typically worn when a soldier went into battle. This armor was designed to protect their body from harm. Just as a soldier would have dressed for battle hundreds of years ago, in the 21st century we, as banks and compliance officers, can "dress" ourselves to prepare for a different type of battle. It is a battle where we are working towards a process to avoid the pains associated with civil money penalties and enforcement actions.

The cuirass, which is forged with steel, is a piece used to protect a soldier's torso area. A compliance officer's cuirass is forged with their knowledge of their bank's business model and their understanding all of the risks involved with each of their products and services as well as which regulations pertain to those products and services.

Forging the compliance officer's knowledge starts with compliance officers understanding what type of bank we are trying to protect. What do our customers look like? Does our bank focus on retail or individual customers, commercial customers, or both areas equally? Once we understand the focus of our bank, we will have a better idea of what types of products and services we need to account for in our risk assessment. For example, if our bank focuses on individual customers, we should know that in addition to savings and checking accounts, does our bank offer other ancillary products like online banking, mobile deposit, or bill pay?

Now that we have an understanding of our bank and its products and services, we can continue to forge our compliance cuirass by supporting it with a compliance risk assessment. The goal of our compliance risk assessment is to understand the risks associated with our product offerings. We also need to know how our processes and procedures, in addition to federal regulations will either reduce those risks or clarify for us that a particular product offering will need a more frequent level of monitoring to ensure compliance with the regulations. Establishing our risk rating system, adds one more layer of protection as well as understanding to our risk assessment. There is no regulation requirement anywhere that directs a bank in how to create their rating system, just that they have one. It has been noted that using a numerical system like one through five, allows for more leniency when an area does not fall directly into a low, medium, or high category. In addition, when we create our risk rating system it is just as important to define and give meaning to each risk rating level. An example of what this could look like would be:

- Low Risk (1) –
    - No changes in regulation, regulation isn't complex, none or minimal growth within the area, (think Regulation CC – Funds Availability)
- Limited or Minimal Risk (2) –
    - A simple change to regulation, regulation has some idiosyncrasies, minimal growth within the area (think Regulation DD – Truth in Savings)
- Moderate/Medium Risk (3) –

    - Some changes to regulation, regulation is somewhat complex, some growth within the area (think Regulation E – Electronic Funds Transfer)
- Considerable Risk (4) –
    - Many changes to the regulation, regulation is fairly complex, more growth within the area (think Regulation B – Equal Credit Opportunity Act)
- High Risk (5) –
    - Consistent changes to regulation, regulation is really complex, consistent growth within the area (think Regulation Z – Truth in Lending or Regulation C – Home Mortgage Disclosure Act)

As we keep building, we take note that a soldier's cuirass structure is just as important as our structure of the compliance risk assessment. A compliance risk assessment should include four key areas of support:

1) Products and Services/Inherent Risks – when a risk assessment is complete, each one of the bank's products and services should be addressed within the assessment and the risks of them as stand-alone products without any controls in place should be rated.
2) Regulations – each regulation area that has been or could be a focal point for our examiners should be taken into consideration. We should ask questions like:
    a. Does this regulation pertain to our bank?
    b. Are the regulators putting a lot of attention to this particular regulation?
    c. Have there been or are there proposed changes to the regulation recently?
3) Mitigating Factors – With each area assessed, we should take into account what controls are in place to help mitigate our bank's exposure to civil money penalties or enforcement actions. In other words, what does our bank do to comply with federal regulations?
    a. Does our Bank have written policies and procedures in place?
    b. Is training for staff provided?
    c. Are audits performed in a particular area?
4) Residual Risks – Once the other three steps are performed, our Bank should look at what risks remain. The culmination of this process will lead to our overall risk rating for that area of the bank.

These four areas of support will complete our risk assessment, leaving us only to add comments regarding our decisions. If we are looking for a template, we can reach out to any UBB Compliance Services staff member.

Our compliance cuirass is now complete. Moreover, just as the soldier's cuirass is solid, so is our compliance cuirass. Let us continue our protection as we move into part three of creating our armor by adding gauntlets, vambraces, cuisses, and tassets, also known as policies, procedures, training, and consumer complaints.