**“Instructor Guidance for Evaluating Student Solutions to the Lifecycle and MM Exercise Study Case”**

***Contributed by Ken Sigler, CIS Faculty and Department Chair, Oakland Community College, Auburn Hills, MI***

In review of the Heavy Metal Technology (HMT) case, some specific details stand out. These points will assist in assessing the student’s justification in both the lifecycle and maturity model exercises.

1. The primary goal of the business is to target the best business opportunities, to win new business, and to deliver increased customer satisfaction.
2. The hosted model removes from the facility’s operations managers the burden of maintaining onsite data acquisition and management functions, while ensuring a secure and scalable worldwide environment. The embedded model allows each local facility to operate and maintain its own IT infrastructure, which is tailored around HMT’s enterprise systems to support that subsidiary’s specific line of business and business operation.
3. HMT targets component integration. Because parts of its products must be developed, the company relies on the RFP process up and down its supply chain. The business itself involves custom development, so the actual development process typically must accommodate large numbers of engineering change orders during the course of the process.
4. HMT knew that it couldn’t have each subsidiary on a separate governance system.
5. HMT wants to monitor the interface with the business process through quantitative data.
6. The problem is that the complexity of tracking an unknown number of business transactions across a large variation of industries would completely overwhelm the company’s relatively small central staff without considerable information technology (IT) support.
7. HMT wants to put strong process safeguards in place. Strategic security concerns, such as keeping all of the software engineering functions in the organization aligned with organizational goals, dealing with changing events in the technology environment, making sure that the right people are involved in the decision making process, keeping the architecture of the software engineering processes simple, and establishing a reliable response to market conditions, are all considerations.
8. Maintaining alignment between its software integration processes and the company’s overall vision is a central theme for HMT executive managers. The idea of coordination and communication as a way of thinking permeates the business operation.
9. HMT uses COTS software when possible, but it does not hesitate to build its own components when necessary or to mitigate risk.
10. HMT uses metrics as a key planning tool. Note: The metrics it uses will have an impact on which security model is selected.
11. The corporate CISO is responsible for providing quarterly status reports on the state of the governance system and any emerging concerns.
12. There is a strong focus on project planning and communication among the engineering disciplines.
13. Software estimates are used and backed up by estimation tools. Estimation improvement is done through retention of project data. A key point is that it is not used in a formal feedback sense.
14. Project metrics are used to evaluate project performance at the project level. The program manager and upper management never see the results of this extensive measurement process. Note: A missing component is that there is no mention as to how those project performance evaluations further influence change at the organizational level. The fact that upper management has no knowledge of the measurements is a strong indication as to why change is not taking place at the organizational level.
15. Software subcontracts are managed using a set of defined policies and procedures. Note: A question to be asked is, “Are they consistent across all subcontractors?”
16. There is no formal change management process. Note: Evidence of the lack of a defined process.
17. The state of software engineering and software improvement is more a rumor than fact based. Note: The facts that are missing will come from documentation provided through a well-defined software process.
18. There are no supporting or quality management services. Information Systems (IS) security is conducted as a separate function from the network and IT function. Note: Need for an integrated security model with a defined software process.
19. There are at least five communities of practice involved with HMT: Acquirers, Suppliers, Developers, Operators, and Maintainers. There is also a large and sophisticated network operation, which is conducted separate from the IT function. Note: This provides truth to the point in the first question that there is an approximate right answer here. Each of these communities is represented by the activities of the 12207:2008 standard. (See the response to the Lifecycle exercise.)

**Lifecycle Exercise**

It’s clear that HMT has some processes in place, but lacks, within those processes, consistency across projects and the ability to promote software improvement and change management across all levels of the organization. The best lifecycle model in this case is ISO/IEEE 12207:2008.

Within this top-down framework for decomposition, specific operational elements (from acquisition through maintenance) are tailored out by identifying the unique problems and criteria of the project environment, and then documenting the adjustments needed to modify (improve) the overall activity and task specifications for the specific project. If this decomposition procedure is followed correctly, the outcome is a unique representation of best practice within the organization for each element of the higher-order standard. When applied correctly, this standards-based decomposition approach allows an organization to ensure commonly recognized best practice while retaining its own distinctive characteristics and culture.

The ISO 12207 model alone does not provide sufficiently detailed guidance to make an organization manageable. Further, it is not suggested that HMT does not have mechanisms in place to help manage the process. However, the processes within the framework still have to be tailored to fit each given situation. In other words, an optimum approach can be engineered top-down for the AH64D Longbow project using the 12207 framework because the model embraces all possible forms of activity.

The implementation strategy is always top-down, meaning that an explicit process model can always be constructed for any given project at any level of definition from the reference framework. This hierarchical approach creates a practical, top-down management process from policies formulated at the enterprise level through practical management procedures at the operational level.

In general, ISO 12207 can provide HMT with the basis for defining the systematic activities, roles, and tasks of the lifecycles employed by all of its subsidiaries. Because those elements are defined in concrete terms, they can be easily evaluated by all levels of management. The 12207 lifecycle model is particularly useful in the case of complex systems (such as the case with HMT) when the requirement for integration places exceptional demands on coordination of the process. These systems and demands include situations such as multi-tiered vendor arrangements and interoperable product lines. By defining the best practices for each lifecycle element, interruptions of the practical outcomes are minimized at all levels of work. Definition also helps ensure early risk detection and true product-in-process visibility, both of which were noted as current weaknesses the current processes employed by HMT.

Important to note is that ISO 12207 does not put focus on the security aspect of development of ITC systems software. As such, HMT would need to adopt an appropriate security lifecycle model. At first understanding of TouchPoints (as discussed in the Software Assurance Lifecycle Models lecture), the student will have a tendency to associate them only to activities that are associated with the Software Development Process Group of the ISO 12207 standard. However, the contrary is true. The activities defined through Touchpoints play a significant role and can be easily integrated into many activities across several processes of the standard. HMT will develop requirements and use cases, perform architecture design, develop and implement test plans, and gain feedback in numerous places throughout the lifecycle (as defined by 12207). It is clear that, using the ISO12207 standard in combination with the Touchpoints considered in all relevant activities across all standard processes, HMT will have taken appropriate steps toward a defined AND secure lifecycle model.

**Maturity Model Exercise**

In attempting to answer this question, the student is likely to go up to the Business Architecture section of the case. In that section, key security metrics that HMT employs are outlined. The student will attempt to match those metrics already gathered to the requirements of the specific models. That’s a mistake. If you notice, all but one of the metrics identified are reactive as compared to proactive in nature. The point of security models is to follow a core set of security processes that are intended to integrate security activities into an existing lifecycle process. Given that, the question becomes, “Which is the best security model for an organization that has a centralized management structure and numerous subsidiaries?”

Another insight that some students will make is that if you compare each model side by side, they all tend to address all of the relevant activities needed for secure software systems (give or take) one or two activities, depending upon the model. However, what the student should realize is that HMT is already performing some of the activities addressed in several of the models. It follows then, that a clear set of measurements and matrices are needed to determine the degree to which existing activities are being performed and what activities are missing. Thus, most students will likely choose BSIMM as the preferred model.

The BSIMM is said to be a measuring stick for software security. The best way to use the BSIMM is to compare and contrast HMT’s own initiatives with the data about what other organizations are doing, which is contained in the model. HMT can then identify goals and objectives of its own and look to the BSIMM to determine which further activities make sense.

Since BSIMM is based on what organizations are actually doing, it can be seen as a de facto standard. The BSIMM does not provide any real insight into which activities are commonly practiced in organizations and which are not. Also, unlike many official standards, the BSIMM accepts the notion that not all organizations need to achieve the same security goals. As such, HMT does not need to carry out all 111 activities and can apply specific activities to individual projects (such as the AH64D Longbow project). However, the model does provide a potential benchmark against which all organizations can be measured and demonstrate progress. This benchmark has made the BSIMM quite appealing over the past several years and should be equally appealing to HMT at this point in time.