Chapter 7
Life Cycle Management

Life-Cycle Management

Life-Cycle Management (LCM) is applied to programs, projects, and activities concerned with the design, development, deployment, and operation computing and telecommunications resources. Formal LCM is a control process applied by DoD directive[1] to expenditures on new information systems, and to expenditures on the modernization of existing systems. Control decisions for all expenditure are based on the total anticipated benefits that will be derived over the life of the new system, or, that will be derived over the life of a modified and improved information system.

LCM Phases

Phase 0. Need Justification

Phase 1. Concepts Development

Phase 2. Design

Phase 3. Development

Phase 4. Deployment

Phase 5. Operations

LCM is used to control expenditures on new or upgraded systems to ensure that the benefits derived cost effectively satisfy mission needs to the greatest extent possible. For information security, LCM is intended to safeguard information resources using prescribed protective measures and controls to meet the specified security requirements. Information policy and procedures, functional requirements, information flows, information technology, telecommunications, security requirements, and other elements are integrated into the planning and evaluation of each alternative program concept.

Technology Life-Cycle

Technology life-cycle (TLC) describes the value gain of a product through the expense of research and development phase, and the financial return during its "vital life". Information technologies have a relatively short lifespan requiring constant re-evaluation an improvement to keep abreast of industry enhancements or threat increases.

Within the commercial world, technology life cycle is concerned with the time and cost of developing the technology, the timeline of recovering cost, and modes of making the technology yield a profit proportionate to the costs and risks involved. In the information security world, particularly in DoD, life-cycle is concerned with continued protection of mission assets through reliability, availability and maintainability, the “RAM” process. Figure 1 depicts the traditional TLC process.

Software Life-Cycle

Unfortunately, software is only as secure as the ability of the developers to make it secure. Historically, applications are developed in a way that doesn’t always ensure that all vulnerabilities are mitigated prior to its release, particularly in the world of commercial-off-the-

[1] ***NUAIBER 7920.1, Life-Cycle Management of Automated Information Systems (AlSs);NUIBER 7740.1, DoD Information Resources Management Program; DoDD 5000.1, Major and Non-Major Defense Programs Acquisitions***

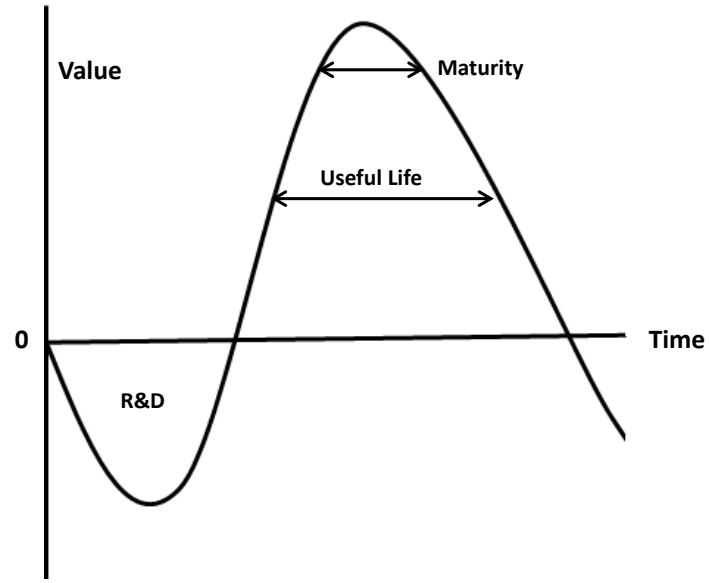

Figure 1 – Technology Life-Cycle

shelf (COTS) solutions. For this reason, many applications require continuous improvements (called patch management) to enhance their secure operational characteristics. Additionally, a host of external protection mechanisms have evolved to help further protect these applications from internal and external threats.

Continuing Life-Cycle and Decommissioning

Once the product has been delivered and deployed, continuing dialog with the customer is necessary to solicit feedback and identify software bugs or vulnerabilities that are identified, plus learn of new capabilities that may be useful to implement. This dialog may also identify capabilities that other products can provide.

As with all lifecycles, the stages of TLC consist of requirements gathering, design and development, quality assurance testing, distribution, software change and configuration, and maintenance are all part of the application lifecycle, as is decommissioning.