CVP Certification Exam Domains

1. Physical Security (11%)

A. Understand the different module types and different embodiments for modules (2-4%)
B. Understand requirements for physical security for modules specific to levels 1-3 (4-6%)
C. Understand requirements for physical security for modules specific to level 4 (1-3%)

2. Authentication, Roles, Services, SW/FW Security and Operational Environment (20%)

A. Understand authentication requirements and concepts (3-6%)
B. Define the requirements for roles (1-3%)
C. Understand the concepts of services using approved and non-approved functions, and bypass (2-5%)
D. Understand the self-Initiated cryptographic output capability, SW/FW security including loading requirements and their applicability. (5-9%)
E. Describe the operational environment requirements/concepts and how to test them (2-4%)

3. Algorithms & Self-tests (20%)

A. Understand the concepts of the approved and allowed algorithms (2-4%)
B. Identify which algorithms are approved or allowed (5-6%)
C. Identify testing for components of the algorithms (2-4%)
D. Identify the tester's responsibilities when reviewing an algorithm's implementation (2-3%)
E. Identify the pre-operational self-tests (e.g. integrity, bypass) and know the associated requirements (4-6%)
F. Understand the requirements for conditional and cryptographic self-tests (4-5%)

4. SSP Establishment (20%)

A. Understand the requirements for SSP generation, SSP agreement, SSP transport and SSP derivation and applicable standards and guidance (5-8%)
B. Understand and identify the approved random bit generators (3-5%)
C. Understand the notion of entropy and methods of entropy estimation (4-5%)
D. Possess general knowledge of the SSP establishment protocols and standards in the IT industry (2-5%)

5. SSP Management (13%)

A. Understand the requirements for SSP entry and output and trusted channels (6-8%)

B. Understand the requirements for SSP storage (3-4%)

C. Understand the various types of SSPs and their zeroization requirements (2-3%)

6. Security Assurances (16%)

A. Understand the requirements of module specification including degraded operation, approved and non-approved modes (4-7%)
B. Understand the programmatic guidance and associated documentation requirements (5- 10%)
C. Understand the requirements for ports & interfaces, finite state model, development, mitigation of non-invasive and other attacks, and design assurance (3-5%)