CISSP-BEST-PRACTICES

ID	Priciple (# FROM 800-27 A FROM 800-160)
1	Establish a sound security policy as the “foundation” for design
2	Treat security as an integral part of the overall system design
3	Clearly delineate the physical and logical security boundaries governed by associated security policies
4	Ensure that developers are trained in how to develop secure software
5	Reduce risk to an acceptable level
6	Assume that external systems are insecure
7	Identify potential trade-offs between reducing risk and increased costs and decrease in other aspects of operational effectiveness.
8	Implement tailored system security measures to meet organizational security goals
9	Protect information while being processed, in transit, and in storage
10	Consider custom products to achieve adequate security
11	Protect against all likely classes of “attacks.”
12	Where possible, base security on open standards for portability and interoperability
13	Use common language in developing security requirement
14	Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process
15	Strive for operational ease of use.
16	Implement layered security
17	Design and operate an IT system to limit vulnerability and to be resilient in response
18	Provide assurance that the system is, and continues to be, resilient in the face of expected threat
19	Limit or contain vulnerabilities
20	Isolate public access systems from mission critical resources
21	Use boundary mechanisms to separate computing systems and network infrastructures.
22	Design and implement audit mechanisms to detect unauthorized use and to support incident investigations.
23	Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability.
24	Strive for simplicity.
25	Minimize the system elements to be trusted
26	Implement least privilege
27	Do not implement unnecessary security mechanisms
28	Ensure proper security in the shutdown or disposal of a system.
29	Identify and prevent common errors and vulnerabilities.
30	Implement security through a combination of measures distributed physically and logically
31	Formulate security measures to address multiple overlapping information domains

32	Authenticate users and processes to ensure appropriate access control decisions both within and across domains
33	Use unique identities to ensure accountability
A	Limit the need for trust.
B	Control visibility and use.
C	Contain and exclude behaviors
D	Layer defenses and partition resources.
E	Plan and manage diversity.
F	Maintain redundancy.
G	Make resources location versatile.
H	Leverage health and status data.
I	Maintain situational awareness.
J	Manage resources (risk) adaptively.
K	Determine ongoing trustworthiness.
L	Make the effects of deception and unpredictability user-transparent.