

COURSE: SECURITY+ SY0-401

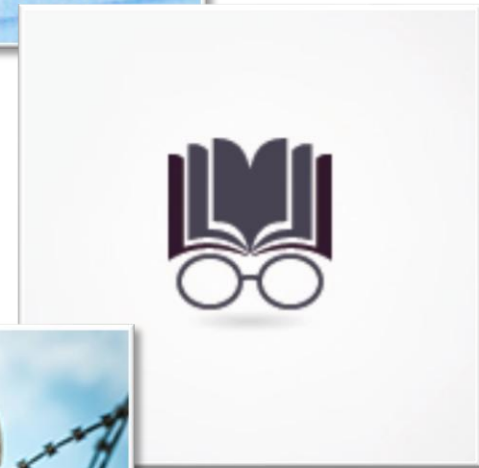
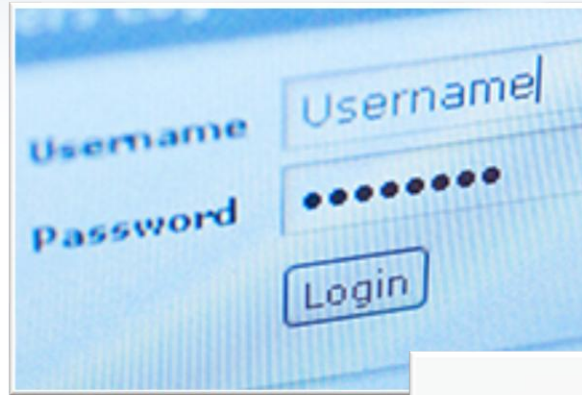
MODULE 2: COMPLIANCE AND OPERATION SECURITY

Part A

- **Explain the importance of risk related concepts**
- **Summarize the security implications of integrating systems and data with third parties**
- **Given a scenario, implement appropriate risk mitigation strategies**
- **Given a scenario, implement basic forensic procedures**
- **Summarize common incident response procedures**

Control Types

- Technical
- Management
- Operational



False Positives

A control that allows unauthorized access, falsely identifying the access as valid.



False Negatives

A control that refuses authorized access, falsely identifying the access as invalid.

Risk Reduction Policies

- Privacy policy
- Acceptable use
- Security policy
- Mandatory vacations
- Job rotation
- Separation of duties
- Least privilege



Calculation

- Likelihood
- ALE
- Impact
- SLE
- ARO
- MTTR
- MTTF
- MTBF

5					
4					
3					
2					
1					
	1	2	3	4	5

$$\text{Risk} = \text{Threat} \times \text{Vulnerability}$$

Quantitative Measures (numerical)

Allow for the clearest measure of relative risk and expected return on investment or risk reduction on investment.

Qualitative Measures (subjective/relative)

Assessment can involve brainstorming, focus groups, surveys, and other similar processes to determine asset worth and valuation to the organization.

Vulnerability: *A vulnerability is a weakness in hardware, software, process, or people that can be employed or engaged to affect enterprise security.*

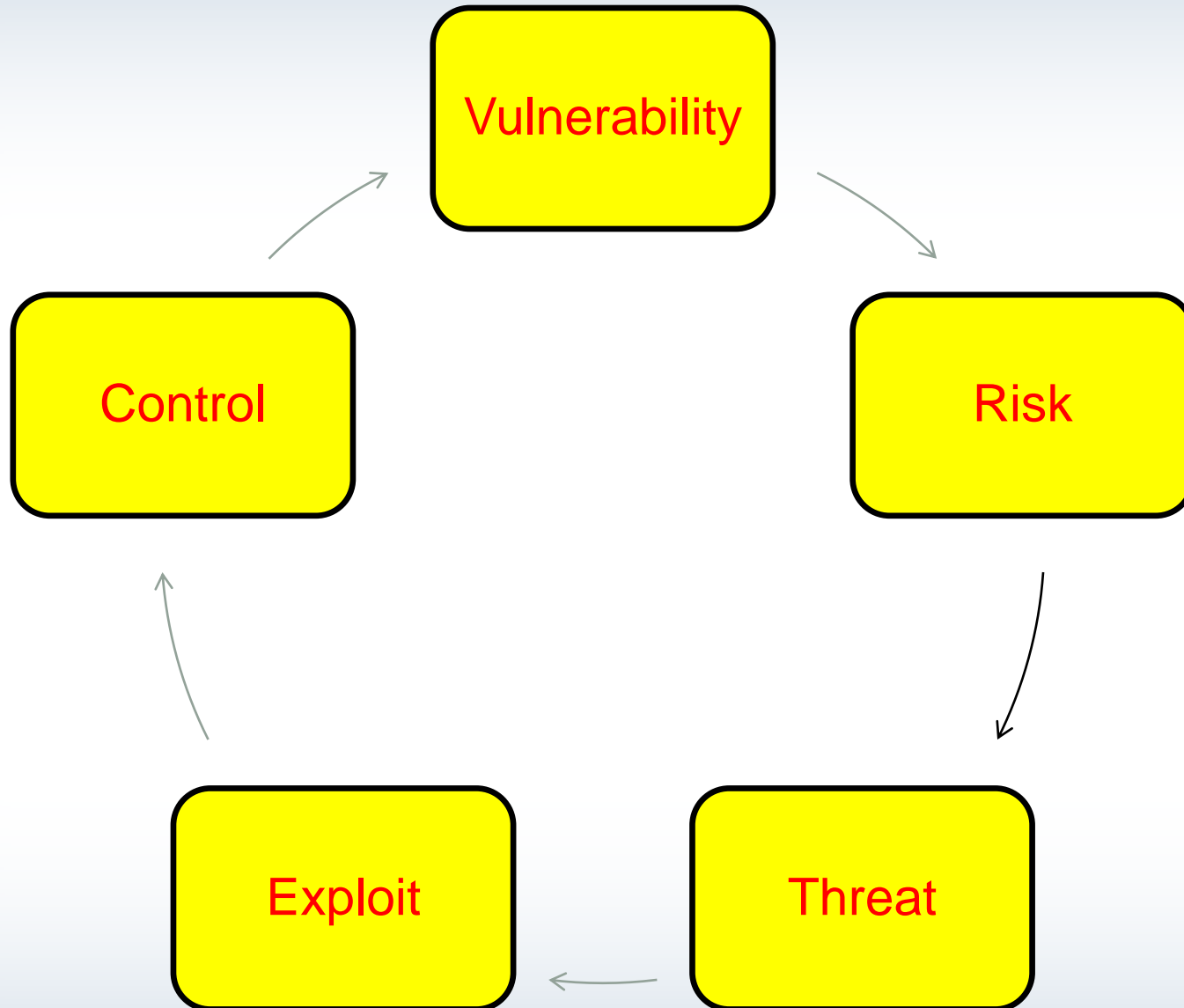
Risk: *A risk is the likelihood that a threat will occur and the measure of its effect.*

Threat: *A threat is the potential that a vulnerability will be identified and exploited.*

Exploit: *An exploit is a mechanism of taking advantage of an identified vulnerability.*

Control: *Controls act to close vulnerabilities, prevent exploitation, reduce threat potential, and/or reduce the likelihood of a risk or its impact.*

Risk Related Concepts



Probability / Threat Likelihood

Table 3-6. Risk-Level Matrix

Threat Likelihood	Impact		
	Low	Medium	High
High (1.0)	Low $10 \times 1.0 = 10$	Medium $50 \times 1.0 = 50$	High $100 \times 1.0 = 100$
Medium (0.5)	Low $10 \times 0.5 = 5$	Medium $50 \times 0.5 = 25$	Medium $100 \times 0.5 = 50$
Low (0.1)	Low $10 \times 0.1 = 1$	Low $50 \times 0.1 = 5$	Low $100 \times 0.1 = 10$

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)⁸

Risk Avoidance: *Elimination of the vulnerability that gives rise to a particular risk so that it is avoided altogether. This is the most effective solution, but often not possible due to organizational requirements*

Risk Transference: *A risk or the effect of its exposure may be transferred by moving to hosted providers who assume the responsibility for recovery and restoration or by acquiring insurance to cover the costs emerging from equipment theft or data exposure.*

Risk Acceptance: *Recognizing a risk, identifying it, and then accepting that it is sufficiently unlikely or of such limited impact that corrective controls are not warranted. Risk acceptance must be a conscious choice, documented, approved by senior administration, and regularly reviewed.*

Risk Mitigation/Deterrence: *Risk mitigation involves the reduction in likelihood or impact of a risk's exposure. Risk deterrence involves putting into place systems and policies to mitigate a risk by protecting against the exploitation of vulnerabilities that cannot be eliminated.*

Cloud Computing and Virtualization Risk

Secure data transfer: *Because data must travel over public Internet connections for both hosted and hybrid clouds, data must be encrypted and authenticated between endpoints.*

Secure APIs: *Application interfaces must be protected against unauthorized access as well as flood attacks intended to deny legitimate access to remote resources.*

Secure data storage: *Data must be encrypted at rest and in backup media to protect against unauthorized access even with physical server access.*

Recovery Time Objective (system)

A measure of the time in which a service should be restored during disaster recovery operations.

Recovery Point Objective (backup)

The latest backup that can be restored to return to normal operation.

- **On-boarding/off-boarding business partners**
- **Social media networks and/or applications**

Interoperability Agreements

Service Level Agreements: One of the best ways to ensure the availability of replacement parts is through service level agreements (SLAs). These are signed contracts between the organization and the vendors with which they commonly deal.

BPA

MOU

ISA

Privacy Considerations

Privacy-sensitive information is referred to as personally identifiable information (PII). This is any information that identifies or can be used to identify, contact, or locate the person to whom such information pertains. Examples of PII are name, address, phone number, fax number, email address, financial profiles, Social Security number, and credit card information

- Unauthorized data sharing
- Data ownership
- Data backups
- Follow security policy and procedures
- Review agreement requirements to verify compliance and performance standards

Change Management

You should document all configuration changes. Many companies are lacking in this area. We are often in a hurry to make changes and say we will do the documentation later most of the time, that doesn't happen.

Incident Management

Incidents do happen from time to time in most organizations no matter how strict security policies and procedures are. It is important to realize that proper incident handling is just as vital as the planning stage, and its presence may make the difference between being able to recover quickly and ruining a business and damaging customer relations. Customers need to see that the company has enough expertise to deal with the problem.

- User rights and permissions reviews
- Perform routine audits
- Enforce policies and procedures to prevent data loss or theft
- Enforce technology controls

Data Loss Prevention (DLP)

Security services that identify, monitor, and protect data during use, storage, or transfer between devices. DLP software relies on deep inspection of data and transactional details for unauthorized access operations.

Chain of Custody

Forensics analysis involves establishing a clear chain of custody over the evidence, which is the documentation of all transfers of evidence from one person to another, showing the date, time, and reason for transfer and the signatures of both parties involved in the transfer.

Order of Volatility

Data of potential evidentiary value can be stored in many different forms within a subject system. Some of these storage locations preserve the data even when a system is powered off, whereas others might only hold data for a very brief interval before it is lost or overwritten. Even the process of evaluation can modify or over-write these volatile storage areas, whereas shutting off a running system might completely wipe all data stored in active memory.

Order of Volatility

1. **Registers and Caches:** Data stored within the CPU's registers and cache levels might remain only nanoseconds before being overwritten by normal system operations.
2. **Routing and Process Tables:** Data stored within networking and other active devices can be modified externally by ongoing operations.
3. **Kernel Statistics:** Data regarding current kernel operations can be in constant transit between cache and main memory.
4. **Main Memory:** Data stored within the System's RAM storage.

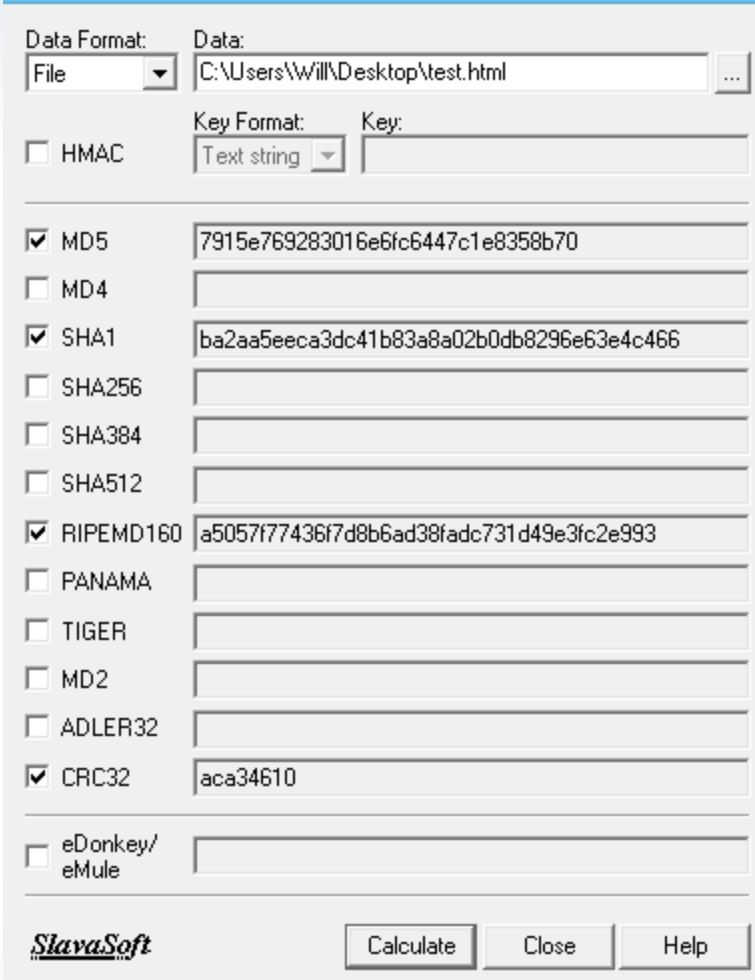
Order of Volatility

7. Temporary File Systems: Data stored within elements of system memory allocated as temporary file stores, such as a RAM disk, or within virtual system drives.
8. Secondary Memory: Data stored in non-volatile storage such as a hard drive or other form of media that retains data values after a system shutdown.
9. Removable Media: Non-volatile removable media such as backup tape storage media.
10. Write-once Storage: Non-volatile media not subject to later overwrite or modification, such as CD-ROMs and printouts.

Capture of running systems is a specialized practice and should not be attempted by untrained responders.

Capture System Image

Take Hashes



The screenshot shows the SlavaSoft HashCalc application window. The 'Data Format' is set to 'File' and the 'Data' field contains the path 'C:\Users\Will\Desktop\test.html'. The 'Key Format' is set to 'Text string' and the 'Key' field is empty. The following table lists the checked hash algorithms and their corresponding values:

Algorithm	Value
<input checked="" type="checkbox"/> MD5	7915e769283016e6fc6447c1e8358b70
<input type="checkbox"/> MD4	
<input checked="" type="checkbox"/> SHA1	ba2aa5eeca3dc41b83a8a02b0db8296e63e4c466
<input type="checkbox"/> SHA256	
<input type="checkbox"/> SHA384	
<input type="checkbox"/> SHA512	
<input checked="" type="checkbox"/> RIPEMD160	a5057f77436f7d8b6ad38fadc731d49e3fc2e993
<input type="checkbox"/> PANAMA	
<input type="checkbox"/> TIGER	
<input type="checkbox"/> MD2	
<input type="checkbox"/> ADLER32	
<input checked="" type="checkbox"/> CRC32	aca34610
<input type="checkbox"/> eDonkey/ eMule	

At the bottom of the window, the 'SlavaSoft' logo is on the left, and three buttons labeled 'Calculate', 'Close', and 'Help' are on the right.

- Network traffic and logs
- Capture video
- Record time offset
- Screenshots
- Witnesses
- Track man hours and expense
- Big Data analysis



Demonstration FTK Imager & Hachcalc

- Preparation
- Incident identification
- Escalation and notification
- Mitigation steps
- Lessons learned
- Reporting

- Recovery/reconstitution procedures
- First responder
- Incident isolation
 - Quarantine
 - Device removal
- Data breach
- Damage and loss control



THANK YOU
