**Student Name:** Ahmed Almass **Weight: 3%**

**Student ID:** **Marks: /**

# Introduction

Security operations encompasses many areas, including incident response, security controls, security events analysis, monitoring, change management, backup strategy, BCP and DR. An operation plan must be developed for each of these areas to address the operational tasks associated with them.

# Instructions

Develop an operation plan to handle the collection of evidence in an investigation of a corporate user’s Internet access through the corporate Internet firewall. The HR department can also request an Internet usage profile on an individual if the necessity arises (e.g., for a performance evaluation).

Provide one answer to each of the questions in the chain of custody below.

1. Who is the appropriate person to collect the evidence from the Internet firewall?

Security administrator

1. What kind of information from the firewall can serve as evidence?

* Authentication allowed
* traffic dropped
* firewall stop/start/restart
* firewall configuration changed
* interface up/down status changed
* administrator access granted
* connection was torn down
* authentication failed
* administrator session ended

1. When should the evidence be collected from the firewall?

During the breach or when discovered

1. Where should the evidence be collected (from which security device)?

* IDS and IPS

1. How should the evidence be collected to ensure its confidentiality and integrity?

* Use file integrity checking tools
* Record the date and time of the breach, the personnel who discovered the breach, the nature of the breach, the kinds of data stolen/lost, when the response efforts began and all of the employees who had access to the affected systems. Document all data and/or devices and hardware lost in the breach.