

Unit -3: Incident Handling

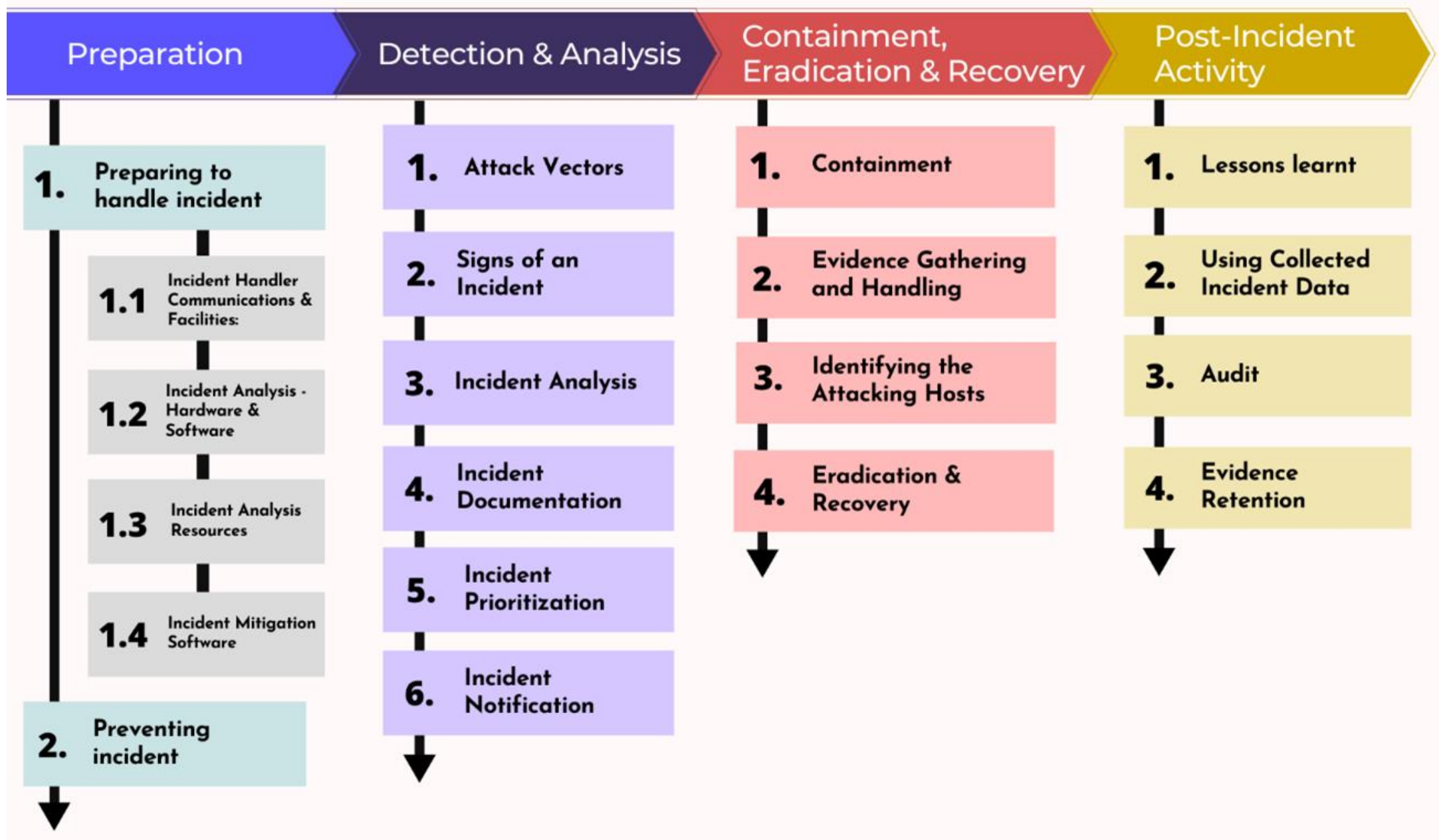
Incident

Cases of Financial Frauds/Bank Frauds in India 2020			
Nature of Frauds	F.Y 2018-19 (₹ in Crores)	F.Y 2019-20 (₹ in Crores)	Increase/ Decrease (₹ in Crores)
Advances	64,548	1,82,051	1,17,503
Off-balance sheet	5,538	2,445	-3,093
Forex Transactions	695	54	-641
Card/Internet	71	195	124
Deposits	148	616	468
Inter-branch accounts	0	0	0
Cash	56	63	7
Cheque/DDs	34	39	5
Clearing accounts	209	7	-202
Others	244	174	-70
Total (₹ in Crores)	71,543	1,85,644	1,14,101
		arthikdisha.com	

Incident handling Process

Incident handling process is a defined process for logging, recording, and resolving incidents. It aims at restoring services as quickly as possible, often through a work around or temporary fixes, rather than through trying to find a permanent solution immediately.

Incident Handling Process



Real time Log capture & Analysis

Real-time log capture and analysis is a process of collecting and analyzing log data in real-time. It is used to monitor and analyze system logs, application logs, and network logs in real-time to detect and respond to security threats, system errors, and other issues.

Installation: **(try during practical's)**

https://www.youtube.com/watch?v=O83aKtv1ZJI&ab_channel=Graylog

<https://checkmk.com/download>

<https://www.loggly.com/>

common tools for real-time log capture and analysis

There are several tools available for real-time log capture and analysis. Some of the most commonly used tools include:

- Graylog: Graylog is a popular Elasticsearch-based open-source log management and analytics tool.
- ELK Stack: The ELK stack (or the Elastic Stack) is a combination of three commonly used open-source tools: Elasticsearch, Logstash, and Kibana.
- Octopussy: Octopussy is another free and open-source log analyzer popular among IT professionals.
- Checkmk: Checkmk is a comprehensive IT monitoring system that includes log analysis capabilities.
- Loggly: Loggly is a cloud-based log management and analysis tool that provides real-time log analysis and monitoring

BOTNET



gbhackers.com/hinatabot-botnet/

Sign-up For Cyber Security News Letter

Your email address..

Subscribe

HinataBot – A New Botnet Could Launch Massive 3.3 Tbps DDoS Attacks

By **BALAJI N** - March 20, 2023

Krebs on Security

In-depth security news and investigation



[HOME](#)

[ABOUT THE AUTHOR](#)

[ADVERTISING/SPEAKING](#)

Who's Behind the Botnet-Based Service BHPproxies?

February 24, 2023

15 Comments

Botnet identification and counteraction

What is botnet?

A botnet is a network of infected computers that are controlled by a remote attacker.

Botnet identification and counteraction is the process of detecting and mitigating botnets, which are networks of infected computers that are controlled by a remote attacker. Botnets are used for a variety of malicious purposes, such as spamming, phishing, and distributed denial-of-service (DDoS) attacks.

how to identify botnet

There are several ways to identify botnets. Some of the common ways are:

- Pattern of Speech: Bots run by an algorithm are programmed to use the same pattern of speech.
- Identical Posts: Another botnet indicator is identical posting.
- Handle Patterns: Another way to identify large botnets is to look at the handle patterns of the suspected accounts.
- Date and Time of Creation
- Identical Twitter Activity
- Location
- Monitor your network traffic for unusual activities
- Monitor failed login attempts
- Establish a baseline and watch out for spikes

common tools for botnet identification and counteraction

There are several tools used for botnet identification and counteraction. Some of the common tools are:

- Network Intrusion Detection Systems (NIDS)
- Rootkit detection packages
- Network sniffers for detection/prevention
- DNS traffic analysis
- Malware detection software and real-time monitoring solutions

Installation :

NIDS - <https://www.snort.org/>

Network sniffer: wire shark

How to Stay Safe from Botnet Attacks?

The best way to deal with cybersecurity attacks is to prevent them. Recovery from a botnet attack can be difficult and costly. Recent botnet attacks have shown that it's better to prevent than to cure. Here are some tips on how to keep your system safe:

- Training and education: educate all employees and partners on the risks posed by botnet attacks in general, and phishing in particular.
- New devices: Only add new devices to your network once you're sure they meet the security standards of your organization.
- Software updates: Make sure your system and device software are always up-to-date; regularly check for software updates.
- Credentials: Change login credentials for all your devices regularly.
- Limit access to your devices: make sure you monitor and restrict access to your organization's devices; only relevant members of your organization should have access to your system or devices.

Enterprise Solutions for Incident Response and Recovery

Eg:

<https://itsfoss.com/>

<https://cve.mitre.org/>

Company

Cynet

SecurityHQ

Security Joes

FireEye Mandiant

Secureworks

Sygnia

Harjavec Group

BAE Systems

Services

Incident Response, Managed Detection and Response, Endpoint Protection

Incident Response, Threat Intelligence, Managed Detection and Response

Incident Response, Digital Forensics, Penetration Testing

Incident Response, Threat Intelligence, Managed Detection and Response

Incident Response, Threat Intelligence, Managed Detection and Response

Incident Response, Digital Forensics, Penetration Testing

Incident Response, Digital Forensics, Penetration Testing

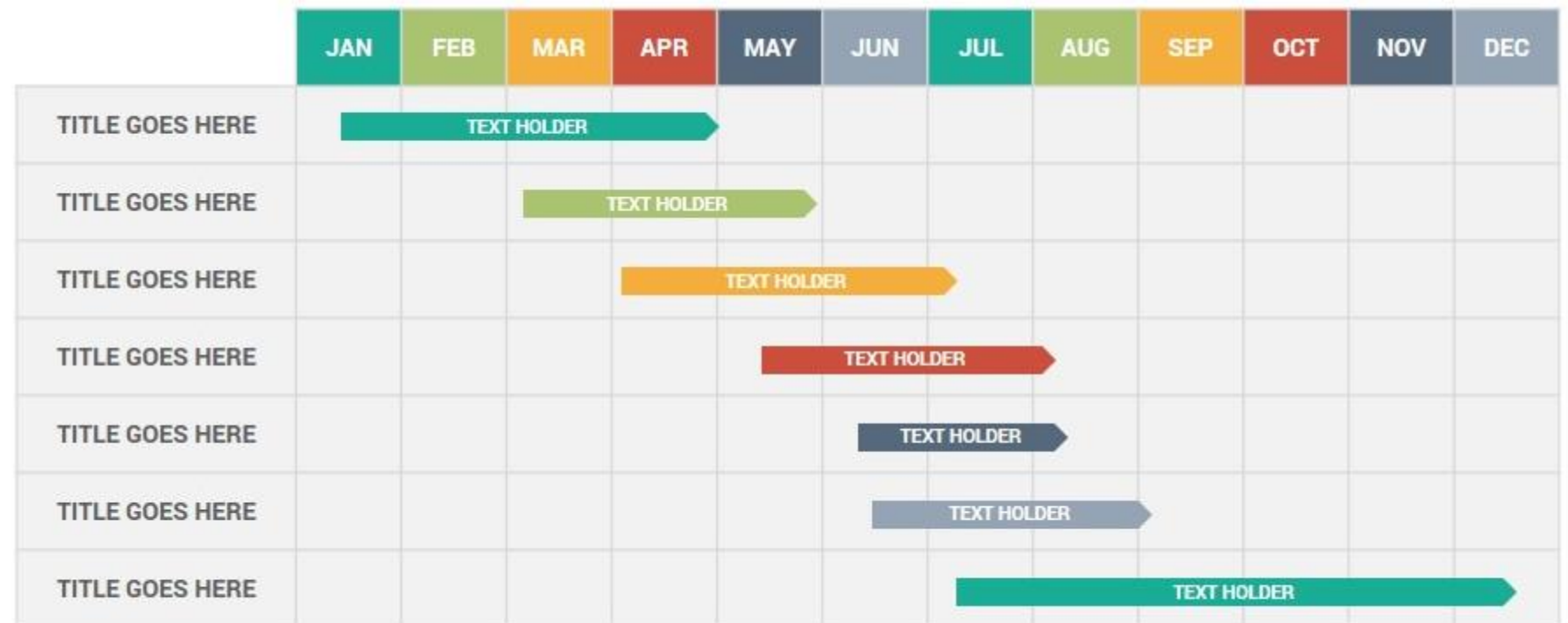
Incident Response, Threat Intelligence, Managed Detection and Response

Timeline Analysis

Timeline analysis is a process of collecting and analyzing event data to determine when and what has occurred on a system at a certain time. It is mainly used for various purposes in the investigation which involves collecting information within a particular time frame. It helps to make inferences very fast in an easy manner.

Create you timeline
for:

1. Education
2. Data creation
3. Computer knowledge
4. Gaming
5. Minor Project



Timeline analysis - types

Suggest at list 3 examples for each timeline
Also suggest 1 tool for each.

1. Horizontal timeline

One of the most common types of timelines is a horizontal timeline, which tracks events from left to right. Usually these present information in sequential order, with the oldest event on the left and the most recent one on the right. The chronological timeline is one type of horizontal timeline.

2. Vertical timeline

Vertical timelines track information from bottom to top. You can use this type of timeline to measure time and amounts, such as money raised for an organization's fundraiser. Usually, these start at the bottom and go up to show the progress or growth toward a goal. The upward motion provides a visual representation of gains or losses for an organization.

3. Roadmap timeline

Roadmap timelines represent a company's business life cycle with the steps to take to reach an end goal. Businesses use roadmaps to track their achievements for their marketing strategy, product development and business sales. They also use them to communicate how long they estimate a project to take and when to expect completion. This type of timeline takes many shapes, often winding around corners, with a starting point and ending point.

Timeline analysis - types

4. Biographical timeline

To showcase the events of a person's life, you can use a biographical timeline. Typically, these represent famous or historical figures, such as celebrities or former presidents. Here, you can select some of their top accomplishments or major life moments and put them in order of occurrence.

5. Historical timeline

A historical timeline presents a sequence of historical events in chronological order of their occurrence. Often these focus on a specific concept, such as the rise and fall of the Roman Empire. This type of timeline is helpful for students to use as study material when trying to learn multiple important dates and occurrences.

6. Gantt chart timeline

Gantt chart timelines use a spreadsheet-like template to organize project components, such as the project schedule, workflow and progress report. Similar to a bar graph, the Gantt chart uses an X-axis and a Y-axis. The X-axis represents the duration of each task, and the Y-axis represents the task.

7. Interactive timeline

An interactive timeline is an online, dynamic tool where you can scroll and zoom in or out to see real-time data. This is helpful for organizations with large amounts of information since it condenses it. Interactive timelines allow individuals to learn more about a point in time by clicking on that section. Sometimes these include additional blocks of text or videos explaining the event in more detail.

Timeline analysis - types

8. Biological timeline

Biological timelines help outline a biological sequence, such as photosynthesis. Here you can outline the various steps throughout the process, sometimes adding images, to help individuals understand it more clearly. This also shows the connections between certain actions and how they lead to other reactions.

9. Company background timeline

Some businesses incorporate a company background timeline on their "About Us" page on their website or in their company profile. Using an infographic, they share how their company came into existence, leading up to the present day. Company background timelines also include major milestones, such as when they earned a specific award or completed certain projects. These can be helpful for consumers to skim and learn about key moments for the company.

10. Project timeline

A project timeline lays out the various stages of a specific project to keep team members on schedule. This type of timeline is future-oriented, setting deadlines for others to work toward. Project managers use these as a way to visualize their operations. Project timelines list tasks in chronological order so team members know what needs to be done and can anticipate future activities.

11. Event timeline

Event timelines focus on components for a specific occasion, such as a wedding. Here you can outline different parts of the event, such as the ceremony and reception, to show guests the order of activities happening.

Malware Handling: Safety; Documentation; Distribution

What is malware?

Malware is a term for any software that is designed to harm or disrupt computers, servers, networks, or devices. Malware can include viruses, worms, trojans, spyware, adware, ransomware, and more. Malware can steal data, damage files, lock devices, or interfere with security and privacy.

Safety: How can I protect my device from malware?

- Use a reliable antivirus or antimalware software and keep it updated.
- Update your operating system, programs, and applications regularly.
- Avoid clicking on suspicious links or attachments in emails or messages.
- Don't download any software or apps from unknown sources.
- Use strong passwords and change them frequently.
- Use a firewall and a VPN when connecting to public Wi-Fi networks

Malware Handling: Safety; Documentation; Distribution

malware Documentation

Malware documentation refers to the technical information that manufacturers or developers provide about their devices or software. Malware creators can use this documentation to exploit vulnerabilities or create cyber threats that target specific systems

[Guide to Malware Incident Prevention and Handling for Desktops and Laptops \(nist.gov\)](#)

[What Is Malware? - Definition and Examples - Cisco](#)

How To Recognize, Remove, and Avoid Malware

1. Popup Ads Pop Up Everywhere
2. Your Browser Keeps Getting Redirected
3. An Unknown App Sends Scary Warnings
4. Mysterious Posts Appear on Your Social Media
5. You Get Ransom Demands
6. Your System Tools Are Disabled
7. Everything Seems Perfectly Normal

Malware removal tools

- Kaspersky Internet Security
- Malwarebytes
- Bitdefender Total Security
- Norton Antivirus Plus
- AVG Antivirus Free
- Avast One Essential
- Avira Free Security
- Norton Power Eraser
- HitmanPro
- Malware Hunter

Which is best tool ?

What are other alternatives ?



How To Avoid Malware or How malware is distributed ?

- **Read each screen when you install new software.** If you don't recognize a program, or are prompted to install bundled software, decline the additional program or exit the installation process.
- **Get well-known software directly from the source.** Sites offering lots of different browsers, PDF readers, and other popular software for free are more likely to include malware.
- **Pay attention to your browser's security warnings.** Many browsers come with built-in security scanners that warn you before you visit an infected webpage or download a malicious file.
- **Instead of clicking on a link in an email or text message, type the URL of a trusted site directly into your browser.** Criminals send phishing emails that trick you into clicking on a link or opening an attachment that could download malware.
- **Don't click on pop-ups or ads about your computer's performance.** Scammers insert unwanted software into pop-up messages or ads that warn that your computer's security or performance is poor. Avoid clicking on these ads if you don't know the source.
- **Scan USB drives and other external devices before using them.** These devices can be infected with malware, especially if you use them in high traffic places, like photo printing stations or public computers.

Report Writing: Reporting Standards; Report Style and formatting; Report Content, Quality Assurance.

General Report writing format

- **Title:** A clear and concise report title.
- **Table of Contents:** A page dedicated to the contents of your report.
- **Summary:** An overview of your entire report — you'll need to wait you've completed the full report to write this section.
- **Introduction:** Introduce your report topic and what readers will find throughout the pages.
- **Body:** The longest section of your report — compile all of your information and use data visualization to help present it.
- **Conclusion:** Different from the summary, this concludes the report body and summarizes all of your findings.
- **Recommendations:** A set of recommended goals or steps to complete with the information provided in this report.
- **Appendices:** A list of your sources used to compile the information in your report.

Academic Report

Title Page
Author Declaration
Abstract or Executive Summary
Table of Contents
Introduction
Literature Review
Methodology or Research Design
Results or Findings
Discussion of Results or Analysis or Interpretation
Conclusions and Recommendations
References

Research Report

Title page
Abstract
Table of contents
Introduction
Literature review
Methodology
Results
Discussion
Conclusion
References
Appendices

Sales/Marketing Reports

[Company name]
[Department]
Monthly report from [start date] to [end date]

Team performance data

Lead conversion rates
[Sales rep one]: [percent]
[Sales rep two]: [percent]
[Sales rep three]: [percent]

Touch points
[Sales rep one]: [number of touch points]
[Sales rep two]: [number of touch points]
[Sales rep three]: [number of touch points]

Lead response time
[Sales rep one]: [number of minutes]
[Sales rep two]: [number of minutes]
[Sales rep three]: [number of minutes]

Revenue closed
[Sales rep one]: [dollars of revenue from closed deals]
[Sales rep two]: [dollars of revenue from closed deals]
[Sales rep three]: [dollars of revenue from closed deals]

Performance improvement over last month
[Sales rep one]: [percent change]
[Sales rep two]: [percent change]
[Sales rep three]: [percent change]

Project Reports

Template for the Project Reports

1 INTRODUCTION

- Scope of project
- Goals of project
- Structure of the report

2 BACKGROUND

- Short descriptions of methodologies, techniques, and tools that are used in the project. Don't define the trivial testing concepts in your reports, e.g., unit testing. But explain the choices and decisions.
- Summary of relevant published works
- If apparently relevant techniques were left out of the project, explain why

3 DESIGN OF THE CASE STUDY

- Description of material used, e.g., system under test, fault data – provide enough information (e.g., you should not include the system's user manual)
- Provide the sources of the material.
- How will the techniques be evaluated and compared?, e.g., fault seeding, mutation testing, model accuracy

4 ANALYSIS OF THE RESULTS

- How are the results analyzed in this section, e.g., measures, quantitative analysis
- Detailed presentation of analysis results, e.g., tables, graphs
- Summary of important results

Weekly Reports

Know the Purpose of the Weekly Report

Know Who Will Read the Weekly Report

Present the Data and Information According to Its Importance

Deliver the Report in a Compelling

[**Title:** Include the title of the project or task.]

[**Date:** List the start date and completion date for the work.]

[**Names:** Include your name and the names of the team members who support the workflow.]

[**Roles:** Give details about your role in the project and your team members' roles.]

[**Summary:** Include a brief summary outlining project tasks, specifications and objectives.]

[**Completed:** Separate completed and in-progress tasks.]

- [Task]

- [Task]

- [Task]

[**In progress**]

- [Task]

- [Task]

- [Task]

[**Outcomes:** Describe the outcomes of completed work.]

- [Outcome]

- [Outcome]

- [Outcome]

[Briefly describe any challenges to the workflow.]

[Implemented solutions]

[Include a section with the main objectives for the following week's workflow.]

Annual Reports

- Adjusted earnings per share* in line with expectations, up 2.7% to 26.7 pence (2014: 26.0 pence)
- Dividend per share up 10.5% to 10.5 pence (2014: 9.5 pence)
- New Virgin Trains East Coast rail franchise to 2023
- Bid submitted for TransPennine Express rail franchise
- Joint venture shortlisted to bid for East Anglia rail franchise
- Continued organic growth in UK Bus
- Significant investment in new vehicles, digital technology and customer service across bus and rail
- Growing network of inter-city coach services in Europe and North America

* See definition in Note 35 to the consolidated financial statements.

Group revenue (by division)

- UK Bus regions
- UK Bus London
- UK Rail
- North America



Group operating profit (by division)

- UK Bus regions
- UK Bus London
- UK Rail
- North America
- Other



Adjusted earnings per share (Year ended 30 April)



Dividend per ordinary share (Year ended 30 April)



Total shareholder return (Five year comparative performance to 30 April 2015)





Notes

- Group revenue:** Revenue is for the year ended 30 April 2015, excluding joint ventures. See Note 2 to the consolidated financial statements.
- Operating profit:** The chart shows the breakdown of total operating profit for the year ended 30 April 2015, excluding intangible asset expenses and exceptional items. See Note 2 to the consolidated financial statements.
- Adjusted earnings per share:** See Note 9 to the consolidated financial statements.
- Dividend per ordinary share:** See Note 8 to the consolidated financial statements.
- Total shareholder return:** The graph compares the performance of the Stagecoach Group Total Shareholder Return (TSR) (share value movement plus reinvested dividends) over the 5 years to 30 April 2015 compared with that of First Group, Go-Ahead Group, National Express Group, the FTSE 350 Travel and Leisure All-Share Index, and the FTSE 250 Index.


Why QA and QC ?





Menu


Search



Community


Learning Portal


Calendar


Marketplace

FDA cites Sun Pharma with litany of GMP violations, including poor aseptic practices

 Regulatory News | 11 January 2023 | By [Joanne S. Eglovitch](#)

1986 Challenger Space Shuttle explosion

On January 28, 1986, the **NASA Shuttle Challenger** exploded minutes after take-off, resulting in the tragic death of all seven astronauts on board. The hardware failure of a **solid rocket booster** (SRB) 'O' ring was cited as the immediate, mechanical cause, but human culpability lay with the decision-making process behind the launch.

In an [extensive report](#), Jeff Forest from the Metropolitan State College points to a flawed **Group Decision Support System** (GDSS), which misrepresented risk and failed to communicate concerns surrounding quality assurance.

2010 BP Deepwater Horizon explosion and oil spill

The explosion of BP's Deepwater Horizon rig on April 20th, 2010 ranks as the biggest manmade environmental disaster in US history. The explosion killed 11 on-board workers, and discharged 4 million barrels of oil into the Gulf of Mexico, before the leak was sealed on July 15th 2010. On top of widespread damage to Gulf marine wildlife and tourism industries, BP faced a slew of lawsuits and forked out over **\$4.5 bn in fines and payments**.

The overarching cause was a quality management failure. Contractors did not test the weak cement around the oil well, which failed to contain hydrocarbons within the reservoir and allowed flammable gas and liquids to flow up the production casing. Technicians misinterpreted fluid pressure tests, and gas passed through the ventilation system into the engine room, paving the way for ignition. After the explosion, the oilrig's blow-out preventer located on the sea-bed failed to activate and seal the well.

Quality Assurance

What Is Quality Assurance?

The quality assurance process helps a business ensure its products meet the quality standards set by the company or its industry. Another way to understand quality assurance (QA) is as a company's process for improving the quality of its products.

Many businesses view their QA program as a promise to internal stakeholders and customers that the company will deliver high-quality products that provide a positive user experience.

QA VS QC

Quality Assurance (QA)

- Proactive
- Broad process
- Goal is to prevent quality failures
- Takes place throughout the development process

VS

Quality Control (QC)

- Reactive
- Narrow process
- Goal is to detect mistakes or errors in a product
- Takes place after development

What Do Quality Assurance Engineers Do?

The roles of quality assurance engineers will vary by company and industry. Using software as an example, a QA engineer's job description might include the following responsibilities:

- Usability testing

- Feature testing

- System testing

- Integration testing

- Creating test plans built on automated scripts to test the product

- Developing standards to ensure quality software code

Importance of Quality Assurance

The quality of the product is the only thing that matters in today's software world. It helps companies to create products and services that fulfill the customer's expectations. Also, it yields high-quality product offerings that build trust and loyalty with customers. Implementing a few standard software quality assurance practices will take Quality Assurance a long way:

Make quality assurance an inherent part of the technical team.

Create a robust testing environment

Predefined quality standards

Select the release criteria carefully.

Measure quality metrics

Create a performance testing and dedicated security team.

Allocate appropriate time for each process

Prioritize the bug fixes based on software usage

Leverage automation tools whenever needed.

Maintain continuous communication, collaboration, and optimization across all departments.

QA process: What does it involve?

The quality assurance process involves four key phases:

Developing a quality assurance plan

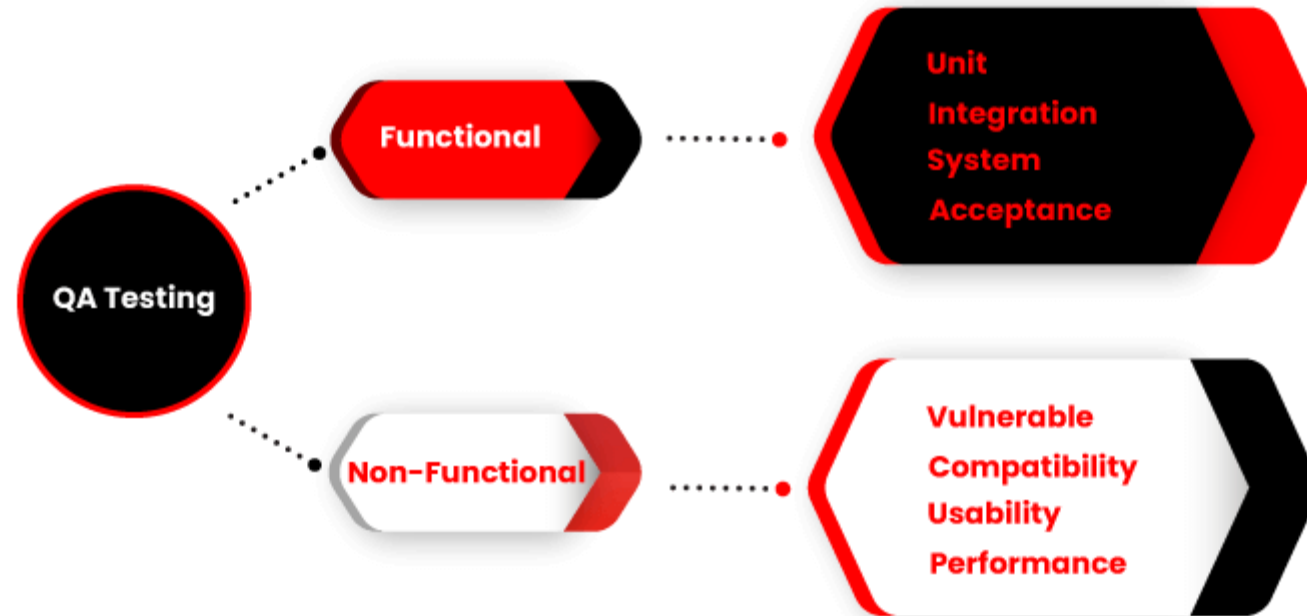
Audit project quality

Analyze

Review project



Quality Assurance (QA) Methods



Quality Assurance (QA)	Quality Control (QC)	Testing
Quality assurance checks the processes and adds changes to the processes which led to the end-product.	Quality control reviews a product or service and checks for the result.	Testing includes activities that ensure the identification of defects/errors/bugs in software.
Focuses on processes and procedures rather than carrying out the actual testing on the product.	Focuses on the actual quality of the product, by implementing various processes and procedures, including testing.	Testing is one of the techniques of quality control to identify defects and bugs for improving quality.
It's a subset of the STLC (Software Test Life Cycle).	It's a subset of QA (Quality Assurance).	It's a subset of QC (Quality Control).
Process-oriented activities	Product-oriented activities	Product-oriented activities
Responsible for the entire Software Development Life Cycle.	Responsible for the software testing life cycle.	Accountable for the bug/defect-free product.
It's a failure prevention system.	QC is a corrective measure.	Testing is a failure detection system.

Advantages of Quality Assurance

- QA saves money - It leads to cost reductions stemming from the prevention of product defects.
- Prevents from unforeseen emergencies - With corporate software, the stakes are even higher, and the bugs can lead to system blackouts, missing data, and communication breakdowns. With QA, there is no margin for errors.
- Promotes the Organization's productivity and efficiency - While development and testing performed in parallel can fix defects in the early stages.
- Boosts customer satisfaction - Regular client involvement in software development and testing increases the customer satisfaction that software quality developed as per the requirements.
- Improves Client Confidence - Proper quality checks at various levels of software like a review, inspection, and more with the involvement of both internal and external stakeholders will increase the client's confidence in the submission of weekly reports of the defect. Requirement metrics also help in assuring the client's work gets done on time.

Disadvantages of Quality Assurance

- Time-consuming - Executing each action in QA will be time-consuming and leads to wastage of time in documentation and meetings rather than working on actual software development and testing sometimes.
- High cost - Through QA, though the cost of fixing bugs in later stages of the software will be reduced, for the small projects with the low budget, it's difficult to quality assurance as the number of resources increases in the project so does the cost of a project. For small projects, hiring the whole team of QA and implementing SQA causes a drastic increase in the price of a project.
- Challenging to implement sometimes - As quality assurance defines all the activities and actions that should be taken at each step of software development in a very detailed manner, sometimes it becomes difficult to implement every single process in development.

Typical Skills of a Quality Assurance Manager

The following skills may be found helpful in this position:

- **Communication:** The ability to communicate effectively both orally and in writing.
- **Organization:** A good sense of orderliness and time management.
- **Problem-solving** – An aptitude for analyzing situations and formulating solutions.
- **Teamwork** – Ability to get along well with others.
- **Leadership** – Leadership qualities such as initiative, self-confidence, assertiveness, decisiveness, and diplomacy.
- **Creativity** – Creative thinking abilities including imagination, originality, resourcefulness, flexibility, adaptability, and inventiveness.
- **Judgment** – Judgmental capabilities include discrimination, discernment, foresight, objectivity, and sound judgment.
- **Analytical Thinking** – The ability to think logically and critically about issues and solve problems.
- **Inquiry** – Curiosity and interest in learning new things.
- **Decision-Making** – Decision-making skills that involve choosing alternatives and evaluating their relative merits.
- **Planning** – Planning skills that enable one to anticipate future needs and devise appropriate courses of action.
- **Time Management** – Time management skills that allow you to organize your activities efficiently and keep on schedule.
- **Self Control** – Self-control refers to the capacity to delay gratification and resist impulses.
- **Adaptability** – Adaptability involves the ability to adjust behaviour to suit changing circumstances.
- **Attention To Detail** – Attention to detail can mean paying close attention to small details while performing routine tasks.
- **Technical Skills** - Technical skills and experience related to the industry.