



# How to Perform an IT Security Audit

---

NETWORK SECURITY BASICS

## TABLE OF CONTENTS

<b><u>INTRODUCTION</u></b> .....	<b>3</b>
<b><u>LITERATURE OVERVIEW</u></b> .....	<b>5</b>
<b>THE IMPORTANCE OF IT SECURITY AUDITING</b> .....	<b>5</b>
<b>ENTERPRISE RISK ASSESSMENT</b> .....	<b>8</b>
<b>IT SECURITY AUDITOR</b> .....	<b>10</b>
<b>IT SECURITY AUDIT TRAIL</b> .....	<b>11</b>
<b><u>SECURITY AUDIT PROCESS</u></b> .....	<b>13</b>
<b>PLANNING</b> .....	<b>14</b>
<b>SECURITY PROCESS SCOPING</b> .....	<b>15</b>
<b>FIELDWORK</b> .....	<b>17</b>
<b>DOCUMENTATION</b> .....	<b>20</b>
<b>REPORTING AND FOLLOW-UP</b> .....	<b>21</b>
<b><u>CASE STUDIES</u></b> .....	<b>22</b>

## INTRODUCTION

Cybercrime is an increasing threat that is faced by every organization and is becoming ever more prominent with the proliferation of cloud technology and complexity of devices. Each day new and sophisticated cybercrime cases are reported that causes significant trauma, financial loss and reputation damage.

There is no room for complacency. Recent trends and cybersecurity statistics reveal a huge increase in hacked and breached data from sources that are increasingly common in the workplace, like mobile and IoT devices. In 2018, 62% of businesses experienced phishing and social engineering attacks<sup>1</sup>. Further, 68% of business leaders feel their cybersecurity risks are increasing<sup>2</sup>.


In lieu of these alarming statistics, a heightened Information Security Plan is critical to protect an organization's IT infrastructure against cybercrime, fraud and data breach. It is imperative for every organization to ensure that their data is secure, confidential and accessible. The security of an organization's IT infrastructure stands on the foundations of user practices, software, and the company policies. These foundations are defined by IT Security Audit.

A Security Audit is a systematic evaluation of the security of a company's information system by measuring how well it conforms to a set of established criteria. A thorough audit typically assesses the security of the system's physical configuration and environment, software, information handling processes, and user practices.

---

<sup>1</sup> Source: <https://www.cybintnsolutions.com/cyber-security-facts-stats/>

<sup>2</sup> [https://www.accenture.com/\\_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50](https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50)



At its root, an IT Security Audit includes two different assessments. The manual assessment occurs when an internal or external IT security auditor interviews employees, reviews access controls, analyzes physical access to hardware, and performs vulnerability scans. These reviews are required to be done annually. For more complex organizations more frequent audit interval may be warranted. Automated assessments on the other hand involves the review of system generated reports. Automated assessments not only incorporate that data, but also respond to software monitoring reports and changes to server and file settings.

Information security auditing is a vital step in protecting organization's information system against Cybercrime, fraud and data breach. They should be carried out regularly, as a systematic examination by an independent expert to discover a weakness in the organization's IT security. Security audits are often used to determine regulatory compliance (such as HIPAA<sup>3</sup>, the Sarbanes Oxley Act<sup>4</sup>, and the California Security Breach Information Act<sup>5</sup>) that specifies how organizations must deal with information.

This research report will present the path and the procedure used to achieve a successful IT security audit, as well as examine if the procedure helps to improve the IT security. While it is clear that IT security commands significant resources in terms of time and money, it pales in comparison to the cost of cybercrime, fraud, and data breach. The worldwide spending on cybersecurity thus is forecast to reach \$133.7 billion in 2022<sup>6</sup>.


---

<sup>3</sup> Source: <https://searchhealthit.techtarget.com/definition/HIPAA>

<sup>4</sup> Source: <https://searchcio.techtarget.com/definition/Sarbanes-Oxley-Act>

<sup>5</sup> Source: <https://searchcio.techtarget.com/definition/California-Security-Breach-Information-Act>

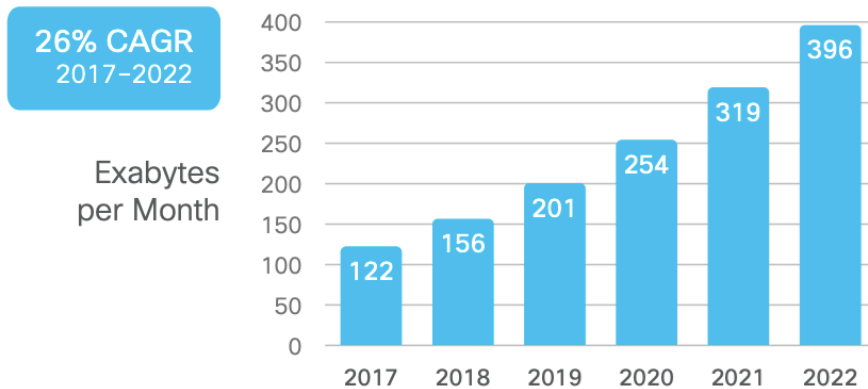
<sup>6</sup> Source: <https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019>



## LITERATURE OVERVIEW

### THE IMPORTANCE OF IT SECURITY AUDITING

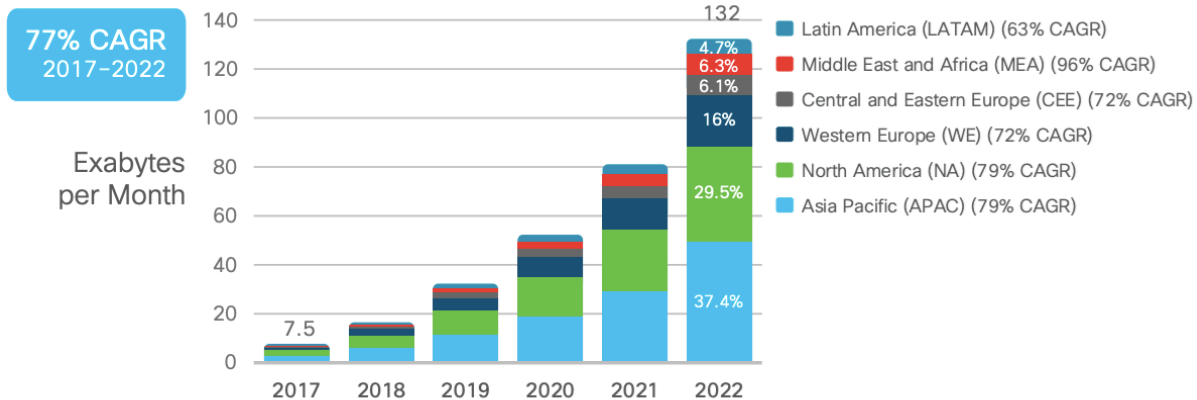
The explosive growth in the digital and interconnected world over the last decade has created tremendous opportunities and offered huge benefits to users, companies, and organizations around the world. This has also been the cause for the exponential and dramatic growth in data traffic which is estimated to reach 150,700 GB per second in 2022 (more than triple compared to 2017<sup>7</sup>), Americas accounting for nearly 30% of the total, second only to Asia Pacific



Source: Cisco VNI Global IP Traffic Forecast, 2017-2022

---

<sup>7</sup> Source: <https://cyrekdigital.com/pl/blog/content-marketing-trendy-na-rok-2019/white-paper-c11-741490.pdf>



Source: Cisco VNI Global IP Traffic Forecast, 2017-2022

Presently, an organization's value is determined by the amount and quality of data handled. Information security is formulated by taking into consideration the "CIA triad":

1. Confidentiality
2. Integrity
3. Availability of information.

The explosive growth in the digital world and the volume of data traffic generated gives rise to significant security risks such as cybercrime, fraud, and data breach.

The increasing amount of large-scale, well-publicized breaches suggests that not only are the number of security breaches going up — they're increasing in severity. Data breaches expose sensitive information that often leave exposed users at risk for identity theft, ruin companies' reputations. Almost always the breaches leave the company liable for compliance violations.

The statistics below sketch an alarming picture

- Security breaches have increased by 11% since 2018 and 67% since 2014<sup>8</sup>.
- Hackers attack every 39 seconds, on average 2,244 times a day<sup>9</sup>.
- The average time to identify a breach in 2019 was 206 days<sup>10</sup>.
- The average lifecycle of a breach was 314 days (from the breach to containment) <sup>11</sup>.
- 64% of Americans have never checked to see if they were affected by a data breach<sup>12</sup>.
- 56% of Americans don't know what steps to take in the event of a data breach<sup>13</sup>.
- The average cost of a data breach is \$3.92 million as of 2019<sup>14</sup>.

The need for information security thus, has never been more crucial as it is today. A systematic IT security audit process is one of the activities that enable organizations to proactively detect and prevent data breach, fraud and cybercrime.

---

<sup>8</sup> Source: <https://www.accenture.com/us-en/insights/security/cost-cybercrime-study>

<sup>9</sup> Source: <https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds>

<sup>10</sup> Source: <https://www.ibm.com/security/data-breach>

<sup>11</sup> Source: <https://www.ibm.com/security/data-breach>

<sup>12</sup> Source: <https://www.varonis.com/blog/data-breach-literacy-survey/>

<sup>13</sup> Source: <https://www.varonis.com/blog/data-breach-literacy-survey/>

<sup>14</sup> Source: <https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/>

## ENTERPRISE RISK ASSESSMENT

Some interesting statistics reveal that data breaches exposed 4.1 billion records in the first half of 2019<sup>15</sup>.

- 71% of breaches were financially motivated and
- 25% were motivated by espionage<sup>16</sup>.
- 52% of breaches featured hacking,
- 28% involved malware and
- 32–33% included phishing or social engineering, respectively<sup>17</sup>.
- The top malicious email attachment types are .doc and .dot which make up 37%, the next highest is .exe at 19.5%<sup>18</sup>.
- Only 5% of companies' folders are properly protected, on average<sup>19</sup>.

Therefore, prior to formulating procedures and controls around IT security, organizations are required to first assess their risk exposure. There are 4 primary reasons why organizations must establish an enterprise IT security audit capability:

---

<sup>15</sup> Source: <https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report>

<sup>16</sup> Source: <https://enterprise.verizon.com/en-gb/resources/reports/dbir/>

<sup>17</sup> Source: <https://enterprise.verizon.com/en-gb/resources/reports/dbir/>

<sup>18</sup>

Source: [http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D\\_ISTR23\\_Main-FINAL-APR10.pdf?aid=elq\\_](http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D_ISTR23_Main-FINAL-APR10.pdf?aid=elq_)

<sup>19</sup> Source: <https://www.varonis.com/2019-data-risk-report/>



### 1) Quantify the Cost/Risk

First among them is risk assessment can aid in justifying financial expenditures related to security protocols that are put in place to guard the organization. All information security comes at a cost, and many enterprises operate on a tight budget, which leaves little room for additional expenditure. An IT security risk assessment would inherently articulate critical risks and quantify threats to information assets. Risk assessment would not only provide internal stakeholders a clearer view of the exposure, but also the value of mitigating critical risks, thus justifying security investments.

### 2) IT Productivity

Second, risk assessment assists in streamlining IT productivity. By formalizing the structure and framework that aid ongoing monitoring, IT department can shift focus on proactively collecting and reviewing documentation rather than reactively respond to threats.

### 3) Self-Review

Enterprise security risk assessment also sets the foundations for self-review. While the IT staff is equipped with the knowledge of the technical system, network, and application information, implementation is dependent on the capabilities of staff of other business units. Risk assessment thus furnishes accessible reports prioritizing actionable information enabling all involved to take up appropriate level of responsibility. It is prudent to foster a culture of compliance as security cannot function in isolation.

#### 4) Increase Information Mobility

Lastly, security risk assessments disburse information across all business verticals. Individualized vendors and systems may not allow different departments within an organization access to the functions of others, assessments hands out necessary insights to facilitate meaningful discussions supporting IT security across the board.

### IT SECURITY AUDITOR

*"A security audit is essentially an assessment of how effectively the organization's security policy is being implemented." (Pupescu et.al, 2008 p.79)*

It is the IT security auditor that is tasked with carrying out the IT Security Assessment. While small organization may hire external security advisors to carry out this function, many large organizations have in-house audit department that systematically conduct assessment procedures to keep their security protocols updated and on track.

In addition to internal audit, a third-party audit by a certified external body is also warranted to comply with legal and regulatory parameters such as a financial SOX (Sarbanes–Oxley Act) auditing. The ISO (International Organization for Standardization) / IEC (International Electrotechnical Commission) standard number 17021 outlines the requirements for bodies providing audit and certification. ISO 19011, guidelines for auditing management systems, section 4 covers the six principles of the auditor(s);

- Integrity,
- Fair Presentation,
- Due Professional care,

- Confidentiality,
- Independence and Evidence-based Approach.

These principles should help make the audit effective and reliable.


The IT security auditors carry out a variety of functions to determine the effectiveness and efficiency of an organization's security policies. They are tasked with reviewing an organization's operations, financial reporting and compliance.

## IT SECURITY AUDIT TRAIL

The most resource intensive process of an audit is creating an audit trail. An audit trail is essentially documentation provided to the auditor that validates the processes that secure an organization's IT environment.


Organizing the documentation is an essential function of an organization when preparing for an IT security audit. These documents outline risk assessment procedures and policies, as well as artifacts of compliance with applicable regulatory statutes. Furthermore, an IT department would be required to collate information showing the:

- IT organizational structure,
- policies and procedures,
- standards,
- personnel list,
- the performance of employees and processes,
- internal control tests.



IT security audit thus demands vast amounts of documentation. SaaS tools can help speed up the aggregating process further streamlining the communication process between key stakeholders. When multiple areas of an organization have independent controls in place, aggregating data from various department can become unwieldy and time consuming.

SaaS tools would simplify the IT audit process, beginning with enterprise risk assessment modules that provide the required insight into vendor and company risks. SaaS tools can also be configured to store documentation and enable access moderation allowing organization to keep their record tamper proof. SaaS tools can also efficiently generate reports that meet diverse needs. It gives the c-suite the overview they need to understand the IT landscape, while simultaneously giving IT professionals a place to record the depth of information necessary during an IT security audit.



## SECURITY AUDIT PROCESS

ISACA (Information Systems Audit and Control Association) grouped the audit process into three major phases: planning, fieldwork and reporting as shown in the figure below



### Auditors must be independent

- **External Auditors** hired to present an independent vision and evaluation
- **Internal Auditors** integrating a separate line of reporting in order to preserve independence

### Common Audits

- **Risk Assessment**
- **Compliance Assessment**
- **Technical Assessment**
- **External Assessment (pen testing)**
- **Performance audit**

## PLANNING

Depending on the nature of their business and IT framework, planning and execution of audits vary between different enterprises. An important component of the planning phase of an IT security audit, that of developing an audit program, however, remains the same. The ISO 19011, Guidelines for auditing management system states:

*“An organization needing to conduct audits should establish an audit program that contributes to the determination of the effectiveness of the auditee’s management system. The audit program can include audits considering one or more management system standards, conducted either separately or in combination.”*

While there are certain planning and consensus building steps of the audit program that are recommended such as getting approvals and cooperation from the senior management, the following steps are essential to the audit itself:


1. **Define the physical scope of the audit** – The audit team should define the security perimeter within which the audit will take place. The perimeter may be physically organized around logical asset groups such as a datacenter or around business processes such as financial reporting. The physical scope of the audit allows the auditors to focus on assets, processes, and policies in a manageable fashion.
2. **Define the process scope of the audit** – This is a challenging feat as overly broad process scoping can stall audits, while, overly narrow scoping can result in an inconclusive assessment of security risks and controls. How to effectively scope security process have been detailed in the section that follows.

3. **Conduct historical due diligence** – An often-overlooked step in security audits is pre-audit due diligence. This due diligence should focus on historical events such as known vulnerabilities, damage-causing security incidents, and recent changes to the IT infrastructure and business processes. This would ideally include an assessment of past audits.
4. **Develop the audit plan** – An effective security audit is almost always guided by a detailed audit plan that provides the specific project plan for carrying out the audit. This should include descriptions of the audit scope, critical date milestones, participants and dependencies.

---

#### SECURITY PROCESS SCOPING

It is fairly easy to define the physical security perimeter that encloses the audit. However, more challenging and more valuable of the tasks is scoping the audit around security processes. To achieve this task effectively, it is imperative that businesses prioritize security processes by the amount of risk they pose to the organization. For instance, business continuity process may be a minimal risk process while the process of identity management may pose a severe risk. Under this sample scenario, the identity management process would form a part of the audit while business continuity would not.



The origins of security threats vary with industry and business environment. However, according to one of the world's leading research and advisory company<sup>20</sup>, businesses will be able to prevent 80% of all damaging security events by adopting effective policies in the following four key areas:

**Network Access Controls:** This process checks the security of a user or system that is attempting to connect to a network. It is the first security process that any user or system encounters when trying to connect to any IT asset within a business network. Network access controls should also track the security of users and systems that are already connected to the network. In some cases, this process will also look to correct or mitigate risk based on detected threats and user or system profiles.

**Intrusion Prevention:** As a process, intrusion prevention covers more than traditional intrusion detection. It is closely in line with access control as it is the first security layer that blocks users and systems from attempting to exploit known vulnerabilities. This process should also enforce policies and controls to minimize the scope of an attack across the business network. While intrusion detection systems are an obvious, non-negotiable component of this process so are other technologies such as firewalls.

**Identity and Access Management:** This process controls who can access what and when. While, authentication and authorization are two key pillars of this process, robust policy management and storage also form critical components.

---

<sup>20</sup> Source: <https://www.gartner.com/en>

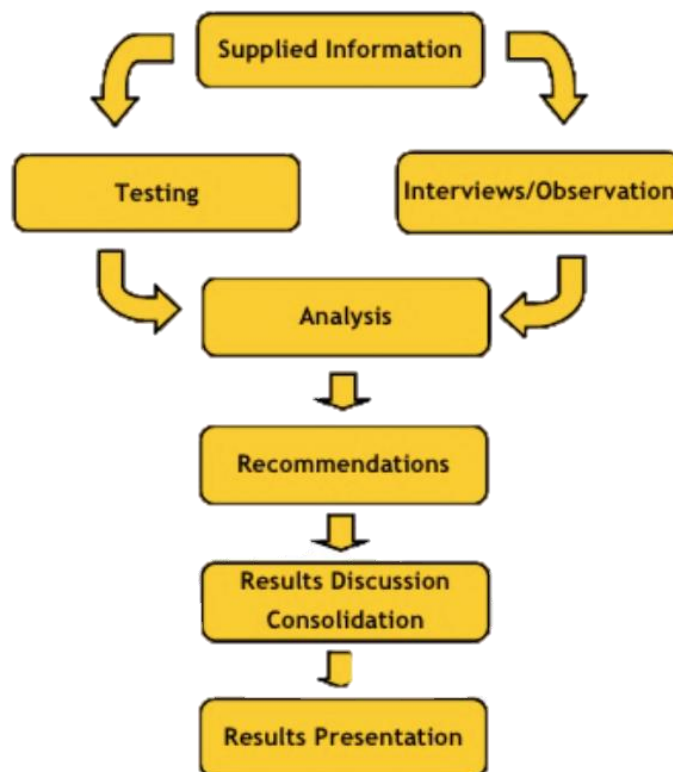





**Vulnerability Management:** The vulnerability management process manages the baseline security configurations across full range of asset classes. It also identifies and mitigates risks by performing root cause analysis and taking corrective measures against specific risks.

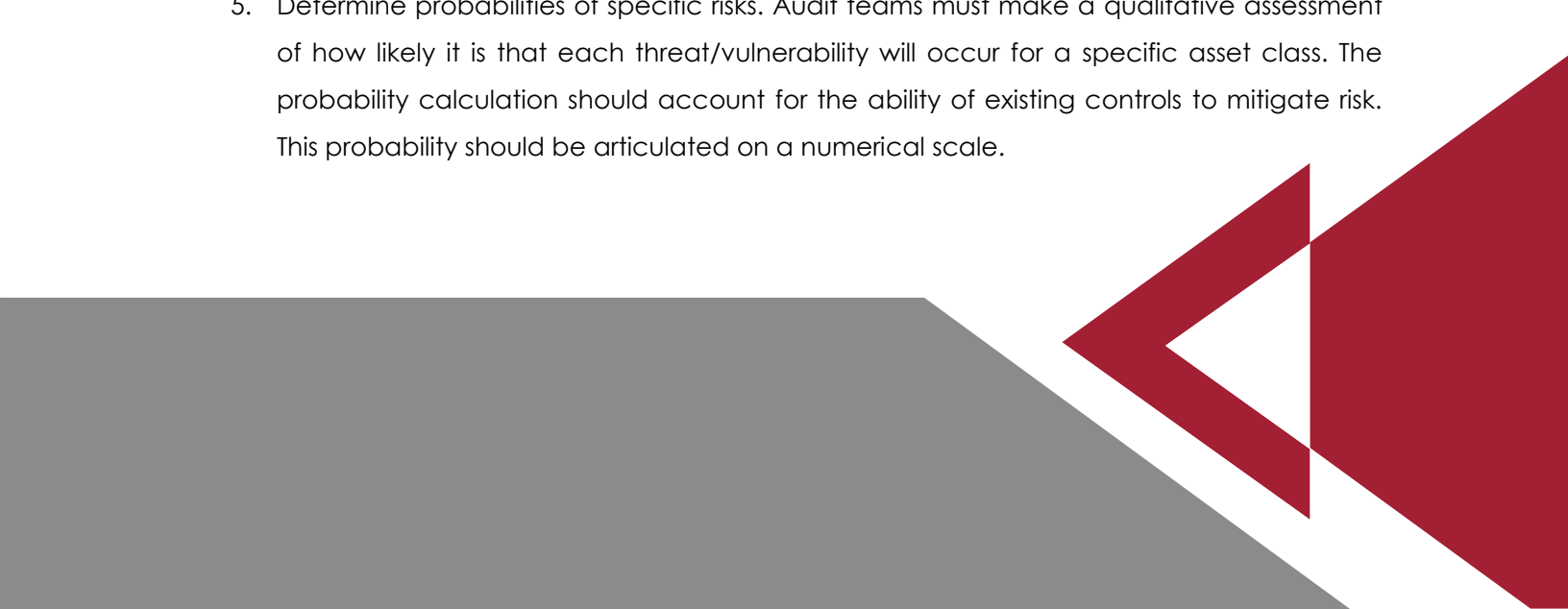
## FIELDWORK

In this phase, the audit functions are carried out by the audit team. The audit team walks through the audit program collecting evidence, performing a technology check by accessing the systems, reviewing logs, using tools, scripts, etc. Gathering information to support the audit functions and to analyze the prevalent risks and exposures.

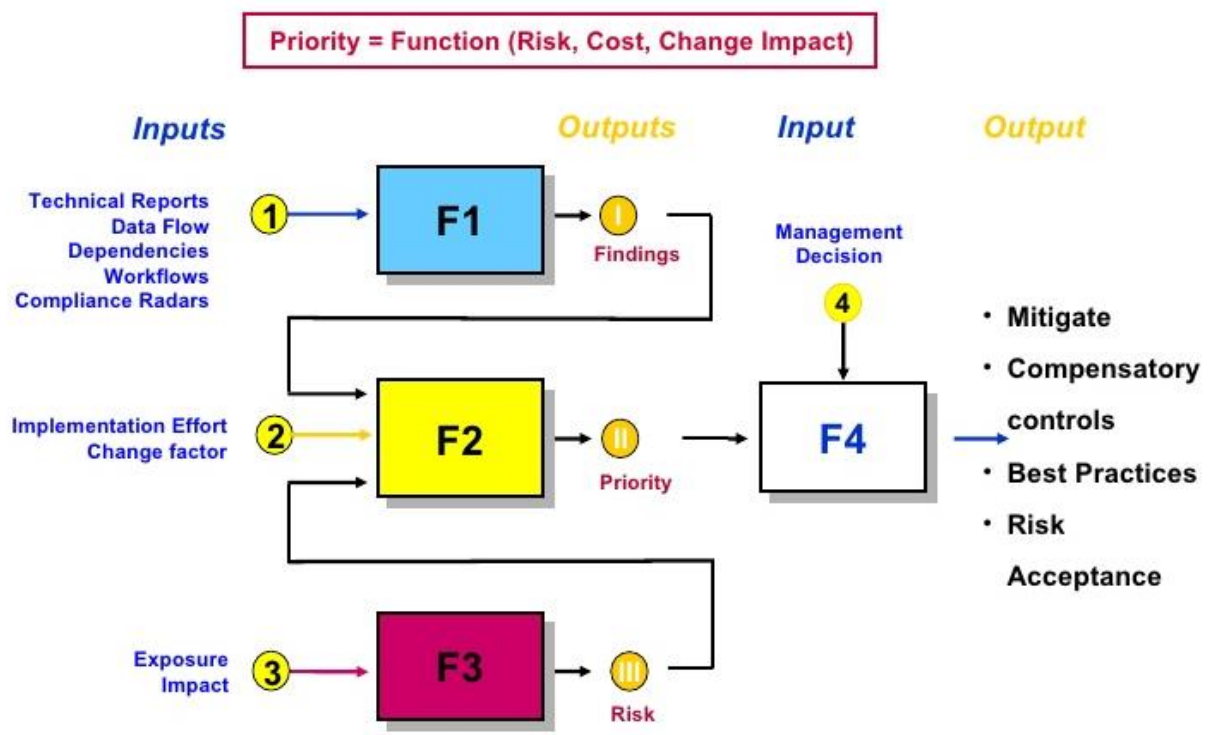




Once the audit team has an actionable plan in place, they can begin the core audit processes – risk assessment. This process covers the following steps:

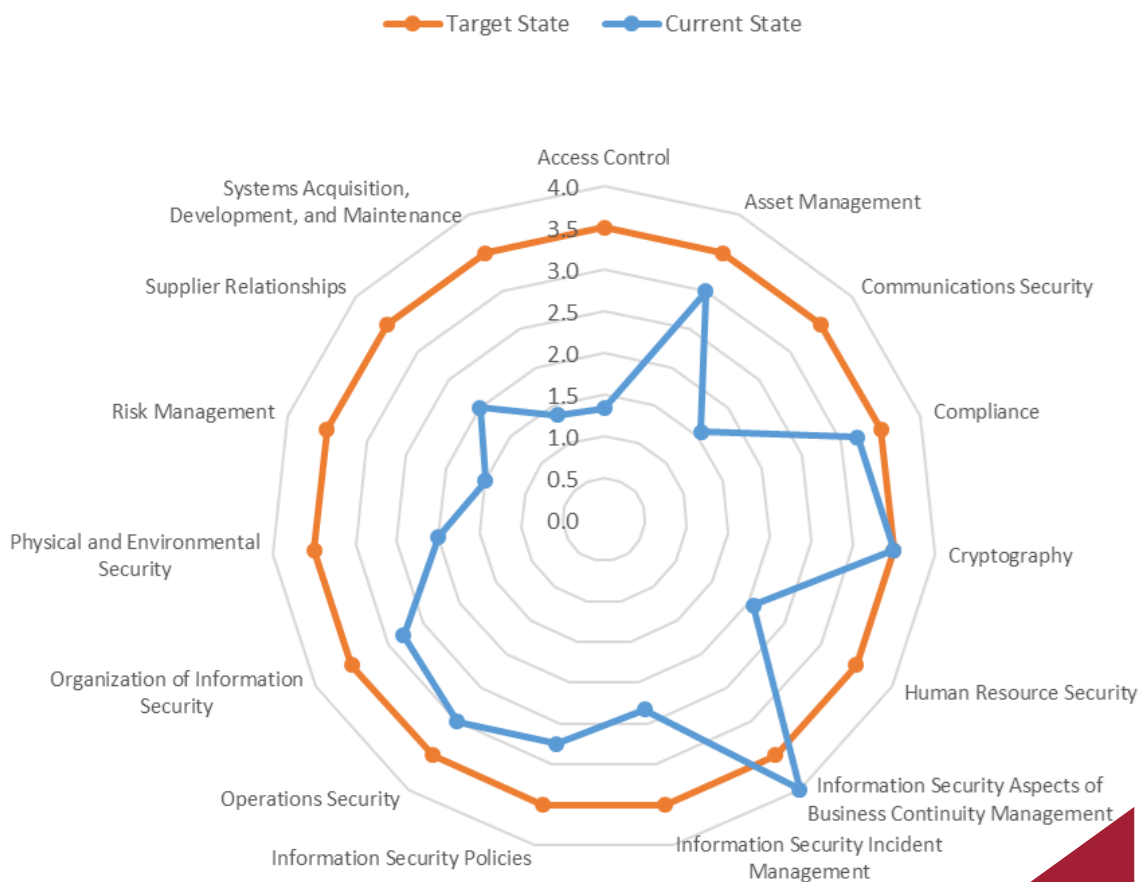
1. Identify and locate the assets within the security perimeter and prioritize those assets based on value to the business. For instance, a cluster of web servers supporting the order entry application is more important than a web server supporting the IT department's internal blog.
  2. Identify potential threats against the assets covered by the audit. The definition of a threat is something that has the potential to exploit a vulnerability in an asset.
  3. Catalog vulnerabilities or deficiencies for each asset class or type. Vulnerabilities exist for specific types of assets and present opportunities for threats to create risk.
  4. Identify the security controls currently in place for each asset class. These controls must exist and be used on a regular basis. Anything short of this should be noted and not counted towards existing controls. Controls include technologies such as firewalls, processes such as data backup procedures, and personnel such as the systems administrator that manages the relevant assets.
  5. Determine probabilities of specific risks. Audit teams must make a qualitative assessment of how likely it is that each threat/vulnerability will occur for a specific asset class. The probability calculation should account for the ability of existing controls to mitigate risk. This probability should be articulated on a numerical scale.
- 


6. Determine the potential harm or impact of a threat. Auditors must again make a qualitative assessment of the likely extent of the harm for a specific asset class. This qualitative assessment should also be represented on a numerical scale.
7. Perform risk calculation. Risk can be quantified by multiplying the two values determined above (probability\*harm). These calculations must be performed for each asset class, which will yield the priority list for risk mitigation efforts and highlight the specific security controls that need to be implemented.



## DOCUMENTATION

The conformity and nonconformity of audit evidence, logs, results and observations are documented, and each finding is classified. The results capture should be documented in detail and proactively communicated with the company decision makers. The documents should include and executive summary, audit determinations, suggested updates/corrections, and supporting data in the form of exhibits.






The audit documentation is crucial for the approval of the audit process to the organization and to the regulation authorities. In addition, the records are tools used to correct the nonconformity objectives and for future reference.

## REPORTING AND FOLLOW-UP

Once the documentation and the necessary conformity tests are carried out a report is drafted to provide the auditor's conclusions, opinions, recommendations and improvements to mitigate the potential risks. The core of the report is a list of issues and actions needed to be taken as an audit follow-up to correct, preventive or improve the weakness in the audited area.

It is important to note that there are a several audit frameworks and methodologies to perform an audit. However, it is essential to ensure, at the beginning of each audit, that the auditors, both internal and external, have a deep understanding of the business they are reviewing, and they should be familiar with the organization's information systems. The auditors have the responsibility to build an audit program, execute it and issue a result report that describes the accurate status of the IT systems being audited.



## CASE STUDIES

In his book, *Network Security Auditing*, Chris Jackson<sup>21</sup>, Technical Solutions Architect in the Cisco Architectures, states that auditing is one of the most important phases to protect the vulnerabilities of information systems. This section will provide case studies that further cements the need of an IT security audit as effective process in improving the organization's information security.

- In 2016, 3 billion Yahoo accounts were hacked in one of the biggest breaches of all time<sup>22</sup>.
- In 2016, Uber reported that hackers stole the information of over 57 million riders and drivers<sup>23</sup>.
- Uber tried to pay off hackers to delete the stolen data of 57 million users and keep the breach quiet<sup>24</sup>.
- In 2017, 412 million user accounts were stolen from Friendfinder's sites<sup>25</sup>.

---

<sup>21</sup> Source: Jackson C., (2010). *Network Security Auditing*, Cisco Press

<sup>22</sup> Source: <https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html>

<sup>23</sup> Source: <https://www.uber.com/newsroom/2016-data-incident/>

<sup>24</sup> Source: <https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data>

<sup>25</sup> Source: <https://www.wsj.com/articles/friendfinder-investigates-report-of-breached-accounts-1479160660>

- In 2017, 147.9 million consumers were affected by the Equifax Breach<sup>26</sup>.
- The Equifax breach cost the company over \$4 billion in total<sup>27</sup>.
- In 2018, Under Armor reported that its "My Fitness Pal" was hacked, affecting 150 million users<sup>28</sup>.
- 18 Russians, 19 Chinese individuals, 11 Iranians and one North Korean were involved in indictments for their alleged state-sponsored espionage against the United States<sup>29</sup>.
- 100,000 groups in at least 150 countries and more than 400,000 machines were infected by the Wannacry virus in 2017, at a total cost of around \$4 billion<sup>30</sup>.

---

<sup>26</sup> Source: <https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628>

<sup>27</sup> Source: <http://time.com/money/4936732/equifax-massive-data-breach-has-cost-the-company-4-billion-so-far>

<sup>28</sup> Source: <http://www.uabiz.com/news-releases/news-release-details/under-armor-notifies-myfitnesspal-users-data-security-issue>

<sup>29</sup> Source: <https://www.symantec.com/security-center/threat-report>

<sup>30</sup> Source: <http://technology.inquirer.net/62619/least-100000-groups-150-countries-hit-ransomware>