A · P · U

ASIA PACIFIC UNIVERSITY
OF TECHNOLOGY & INNOVATION

Security Audit and Assessment
Nuclear Facility Audit Checklist

Thomas MacKinnon TP066728
Intake Code: APDMF2204CYS(PR)
Module Code: CT114-3-M-SAA
Yogeswaran A/L Nathan
Date Assigned: 05/10/2022
Date Completed: 18/11/2022
Word Count: 3703

Abstract

This paper covers the development and use of a Security audit checklist in order to increase the safety and security in Nuclear Facilities, which as a prior literature review points out are a critical industry and prime target for Cyber attacks. The paper documents the steps of building an audit methodology through existing research, and what each stage should contain. This expanded upon in a further checklist where hypothetical answers have been added to show the state of security at a typical Nuclear Facility. These risks are thoroughly analysed and evaluated to find the best remediation plans possible, which are then presented and prioritised for efficiencies sake.

Contents

List of Figures

1 Introduction

Cybercrime has been rapidly rising over the last decade, with greater number of attacks everyday, each aiming to exploit a system for malicious gain. The Federal Bureau of Investigation's Internet crime report show that reported Cybercrime cases almost doubled between 2019 and 2020, as seen in Figure 1, with further increases during the Covid-19 Pandemic (FBI, 2020). Reports estimate that damages from Cybercrime will cost around $10.5 trillion annually by 2025, whilst currently being around $6 trillion, showing the rapid increase in this illegal field.

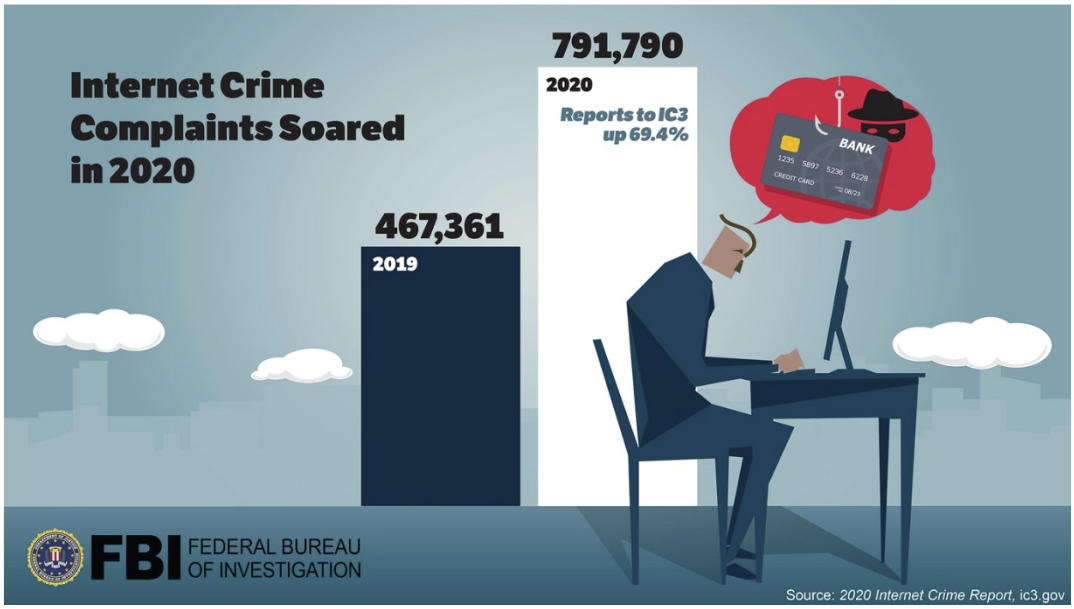

Figure 1: IC3 reported cases from 2020 compared to 2019 (FBI, 2021)

The danger of Cybercrime is not only monetary, but also can cause physical damages to machines, buildings, and innocent bystanders. Stuxnet is an excellent example of the chaotic damages that Cybercrime can cause to the industrial industry, as the USB based worm infected Iranian Uranium enrichment facilities in 2010 (Greenberg, 2019). The worm would raise pressure levels in machinery to dangerous levels, whilst reporting safe numbers to staff, causing enrichment centrifuges to become damaged, which led to an estimated nine hundred destroyed machines and many potentially endangered staff. The danger Cybercrime presents is clear to see, and in-fact as Litherland et al. (2016) highlights has been classified under the same level as International Terrorism and Serious Natural Disasters under the United Kingdom's Nation Security Concerns. The risk to Nuclear Facilities is particularly concerning, as the damages to citizens and the environment are potentially devastating. The Chernobyl disaster, which occurred over thirty five years ago, still leaves it's scar across Ukraine, with inhospitable irradiated areas, and was a key part in the fall of the Soviet Union.

Chernobyl was caused by irresponsible testing, Cybercrime allows for many more ways to cause damage or disaster at Nuclear Facilities. It is therefore vital that these key areas of energy supply are properly protected and preserved to prevent a Malicious actor from causing chaotic destruction. Security Auditing and Assessment are necessary tools to make sure an organisation is maintaining

the proper security protocols and compliances, with the additional goal of finding and fixing flaws before they can be exploited by a Malicious Actor. Audits are key to avoiding preventable attacks, and should be performed regularly with a mix of internal auditors (experience security staff) and external (Penetration testers).

This report is split into two parts, the first being a review of literature related to Nuclear Facilities, the threats they face, the standards they abide by, and the possible solutions out there. This document contains the second half of the report, being the creation of a Security Audit Checklist to solve the issues identified in part 1. The report aims to present a thorough methodology for Security Auditing and Assessment, which will be converted into a detailed checklist for auditing a Nuclear facility, covering Physical and Digital defenses in order to give a full assessment. Then this report will make recommendations in order to fix issues in a Nuclear facility, using official and academic resources to justify the solutions presented.

2 Auditing Methodology for Nuclear Facilities

This section of the report aims to develop a Security audit methodology for a Nuclear Facility, aiming to properly audit Physical and Digital assets and security mechanisms through a thorough process. The methodology was constructed from existing research papers into Nuclear Facility security, articles published by Auditing companies, and official documentation on Nuclear security from existing facilities and Governmental standards, such as the one seen in Figure 2.

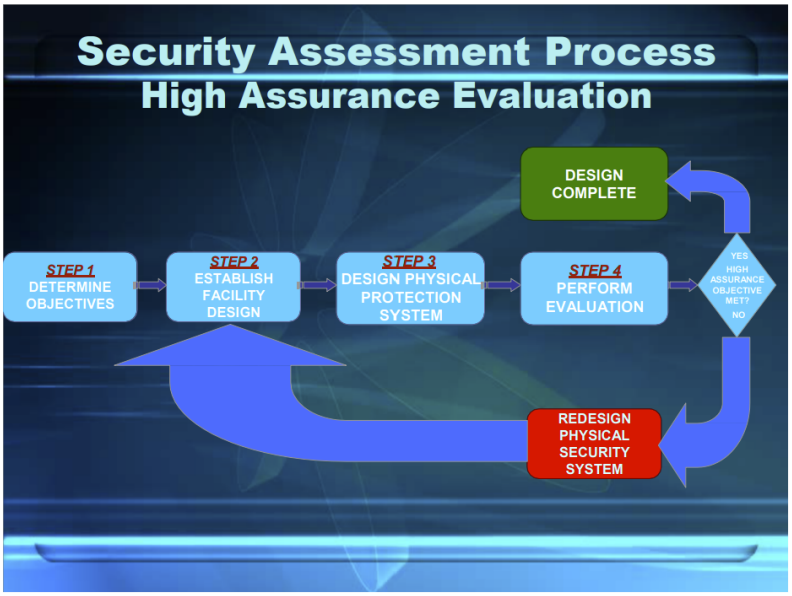

Figure 2: Method for Auditing Security in a Nuclear Facility (U.S.NRC, 2013)

1. **Determine Objectives -** This first stage of a Security Audit should involve determining the objectives of the audit. Goals of an Audit could include meeting standards for certifications or national security compliance's for a Nuclear facility. Audits can also be performed simply to make sure that the security of the facility is not at risk, as part of scheduled maintenance, or in response to a potential threat or recent breach that needs addressing to prevent future attacks (SecureFrame, 2022). To better define Objectives for the audit recent publications relating to Cybercrime, Physical and Digital Security mechanisms, and any other relevant papers should be researched and understood, to better understand the current security landscape, which could lead to additional checks in the Inspecting stages (U.S.NRC, 2013).

2. **Define Scope -** The scope should be everything that will be covered by the audit, such as all hardware, software, access controls, and security mechanisms (Glazer, 2021). The scope is not limited to the items mentioned, as each Nuclear Facility could have different needs for a Security Audit. The scope also does not need to be all encompassing, as that would simply delay the Security team from finding potential critical vulnerabilities, so some areas can be removed as redundant. As part of this stage Internal and External policies should also be reviewed, as to update or add to them due to new information gained since the previous review, documents like the privacy policy, backup policy, and remote access policy are applicable here

3. **Identify Threats -** This stage involves identifying threats to both the physical and digital assets of the Nuclear facility, and which ways they could potentially overcome the security in place. For Digital security this would include researching current Cyber threats that plague the modern technological landscape, how they can damage an organisation, and what prevention methods can be employed to prevent them. Physical threats follow a slightly different course, as malicious actors attempting to commit radiological sabotage will act very differently to a hacker. Number of adversaries, types of weapons or armaments used, and different scenarios of attack all must be discussed as part of security audit. This can be knowledge on attacker strategy through publications, news outlets, and primarily through experienced security staff with first hand experience. In both digital and physical threats the entry points to the Nuclear Facility must be mapped out, as that is where an adversary will attack from, as seen in Figure 3.

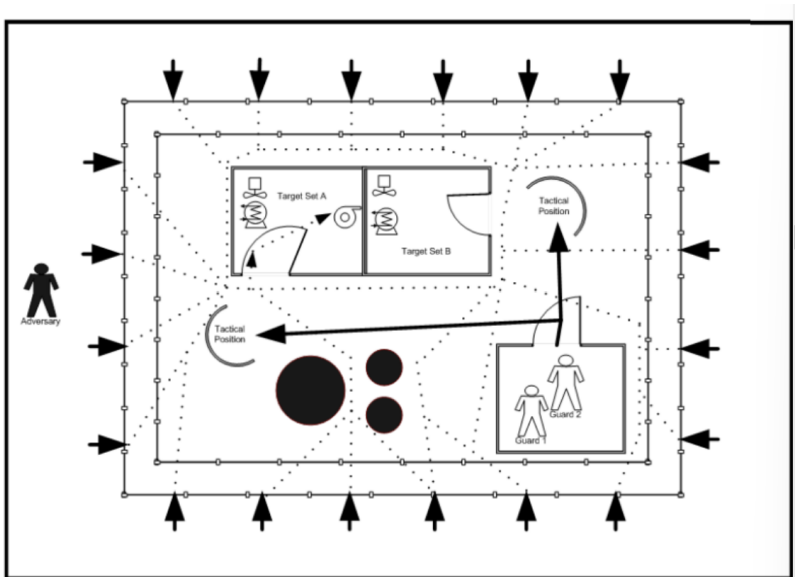

Figure 3: Entry points in a hypothetical Nuclear Facility (U.S.NRC, 2013)

4. **Inspect Digital Assets and Security -** This is were the actual auditing begins, by thoroughly assessing the security of all digital assets and security mechanisms defined in the scope. Checking the Servers, configuration files, DNS, static address assignment, up to date software, and proper access controls are in place are all key parts of Digital security (Corporate Vision, 2021). These are some ideas of what should be checked, however, a more in depth list can be found in the checklist created as part of this report. Logs are also an important aspect of the audit, as they provide valuable information and can be used to automate processes in the future.

5. **Inspect Physical Assets and Security -** Physical Assets should be protected by effective security mechanisms that should greatly deter any malicious actor from attack the Nuclear facility. This is achieved through three main factors, detection, delaying, and response to a threat. Detection methods like sensors, guards, alarms, intrusion detection systems should all be audited to make sure that they are working effectively to catch any unauthorised personnel

entering the facility (U.S.NRC, 2013). Delaying mechanisms are needed to give responders time to deal with a threat, use of turnstiles, locked doors, razor wire, deployable barriers should be in place to cause inconvenience to any potential attacker, and should be audited to make sure they are still functional (as some would not be used in day to day operation). The response elements would be security mechanisms like guards, using lethal or non-lethal weapons, dispensable materials (foam, oil, anything to halt attackers), remote operated weapon systems, each of these are crucial in defending the Nuclear Facility from attack, and deterring any potential threat from trying, and so must be audited thoroughly.

6. **Risks and Remediation -** After the Inspection has concluded the vulnerabilities present in the Nuclear Facility should be clear to the security team, so work towards fixing them can begin. A risk assessment should be completed to better understand the vulnerabilities, using a risk matrix to find which issues are most likely and present the biggest impact to the facility, an example of which can be seen in Figure 4. The matrix should highlight which risks present the biggest threat to the confidentiality, integrity, and availability of digital assets of the facility, and which physical problems are present. A Remediation plan should then be constructed, focusing on fixing the priority risks to the facility, closing any gaps in security through smart fixes and changes to procedures. This stage is critical in securing the Nuclear facility for the future, preventing future attacks and understanding the security ecosystem of the plant better. If the results of the inspection is not acceptable to Upper management (either because it did not reveal enough, or too many flaws) then the audit can be extended to external examiners, such as a Penetration testing team. This would provide a much better understanding of how a malicious adversary would attack the Nuclear facility, and should be conducted every year or so as part of regular auditing.

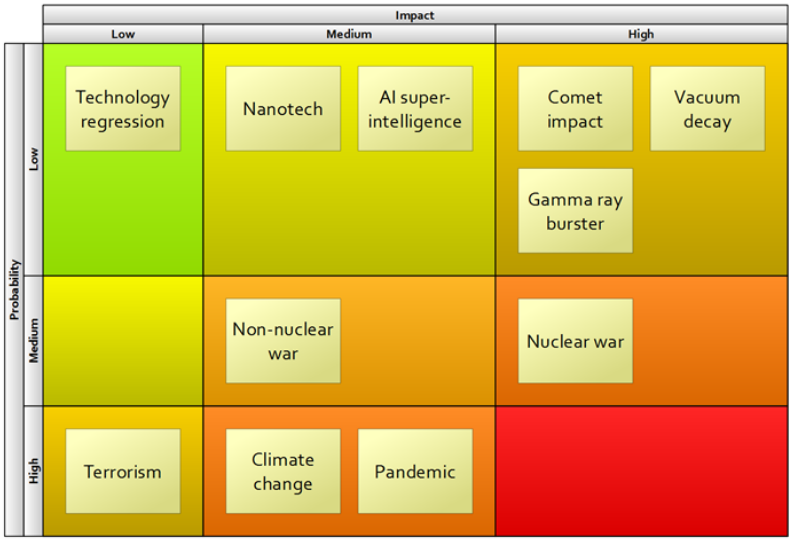

Figure 4: Risk Matrix Example (Hyper Plane, N.D.)

7. **Report Results -** The final part of the audit should be communicating all the results and important information to relevant staff, such as Board members, Security teams, and Upper management. Important changes from the audit should also be communicated in an effective

manner to all staff and stakeholders, so they are aware of the security progress made as a result of the audit, and any new procedures or policies that are now in place. Making the results readable could be in the form of graphs, posters like infographics, well written documents, and internal emails or memos, with many other options available. The results from the audit should also be documented and filed away for use in future audits or simply for reference.

3 Audit Checklist for Nuclear Facilities

Nuclear Facility auditing process presented is effective at ensuring the safety and security of a plant, but to better demonstrate this a hypothetical audit has been conducted. This aims to show how the checklist would be used in a real scenario, and how to use the results gathered from it to mitigate the risks a Nuclear Facility might face. The checklist was created from the stages presented in Section 3 of this report, with aid of several official publications to find the necessary items to check during the audit. The United State's Nuclear Regulatory Commission (U.s.NRC, 2013) document on physical security auditing of a Facility, as to follow official procedures, and IEEE's Standards for Security Systems in Nuclear Stations aided with much of the digital side of the checklist. The ISO/IEC 27001 (ISO, 2013) was used for checking security compliance requirements for Facility, with each Clause added to the associated checklist item (where applicable). The ISO/IEC 27001 2022 updates were also used to check for more recent threats that could effect a Nuclear Facility, such as remote working technology which saw a boom in use due to the Corona Virus Pandemic. Finally, the hypothetical test was conducted as an Internal audit to make it more applicable to general security testing seen in Nuclear Facilities.

Stage 1: Determine Objectives		
Item	Y/N	ISO Clause
Research papers and documents relating to Nuclear facilities and security	Y	A.5.1.1
Research papers on modern Cybercrime since previous Audit	Y	A.16.1.6
Research any other relevant papers or publications that could aid the Audit	Y	A.16.1.6
Determine Goals of Audit	Y	A.16.1.1

Stage 2: Define Scope		
Item	Y/N	ISO Clause
List all Hardware found in Facility	Y	A.8.1.1
List all Operating Systems found in Facility	Y	A.8.1.1
List all Software found in Facility	Y	A.8.1.1
List all Access Controls found in Facility	Y	A.9.1.1
List all Security Mechanisms found in Facility	Y	A.5.1.1
List any other relevant items for the scope	Y	A.8.1.1
Systematically remove any redundant items from the scope	Y	N/A
Find all Internal Policies and Procedure documents for review	Y	A.5.1.2

Stage 3: Identify Threats		
Item	Y/N	ISO Clause
List Digital Threats using research and news	Y	5.25
List Physical Threats from research and news	Y	7.4
Identify Entry points into the Facility	Y	A.11.1.2
Identify Entry points into the digital system of the Facility	Y	A.13.1.1

Stage 4: Inspect Digital Assets and Security		
Item	Y/N	ISO Clause
Are all staff aware and trained in Digital Security and Safety	N, Staff did not know why certain security standards were in place	A.7.2.2
Are Access controls to Digital Assets effective	Y	A.9.1.1
Do users have the right access to restricted areas	Y	A.9.2.5
Are login systems secure	Y	A.9.4.2
Are former staff removed from the system	Y	A.9.2.1
Is the password policy in place effective	Y	A.9.4.3
Are firewalls in places and working as intended	Y	A.13.1.1
Is Anti-Malware working	Y	A.12.2.1
Are backups being made for the system regularly	Y	A.12.3.1
Are backups being stored securely and unchangeable	Y	A.12.4.2
Is there limits on software installation on machines	N, no limits in place	A.12.6.2
Is Auto-run disabled on machines	Y	A.12.6.1
Are internal messages confidential	Y	A.13.2.3
Are external messages confidential	N, as plant does not allow outside communication	A.13.2.3
Are software up to date	N, found some machines running without patches	A.14.2.3
Are any known vulnerabilities running on machines	N	A.14.2.8
Do security events get reported correctly	Y	A.16.1.2
Are security standards in compliance with laws and policies	Y	A.18.2.2
Are remote working portals secure	N, as none are in place	6.7
Are employee devices secure	Y, as none are allowed in the facility	A.8.3.1
Are security patches tested before deployment	N, no testing	A.14.2.6
Is all sensitive data encrypted	Y	A.18.1.5
Have anti-virus signatures files been updated with the latest information	Y	A.12.6.1
Do machines lock after a certain amount of inactivity	Y, after 5 minutes	A.11.2.8
Are unnecessary services disabled	Y	A.13.1.1
Are Intrusion Detection systems monitored 24/7	Y	5.7
Is there a Disaster Recovery plan in place	Y	A.16.1.5
Is the plan tested with latest security information	Y	A.16.1.5

Stage 5: Inspect Physical Assets and Security		
Item	Y/N	ISO Clause
Guards manning Physical Access points	Y	7.4
Are Entry point Guards following security procedure	N, Guards were not disciplined in security checks	7.2
Are the access controls found acceptable at entry	Y, if proper procedure is being followed	A.9.1.1
Is there a record of Staff and Visitors to the Facility	Y	5.33
Is the record properly maintained and filed	Y	5.33
Are Employees easily identifiable due to ID badges	Y	7.2
Are Access cards secure	Y	A.11.1.3
Are CCTV in operation and maintained	Y	A.11.1.1
Are Alarm systems working and maintained	Y	A.11.1.1
Are Guards trained for attacks/emergencies	Y	A.7.2.3
Are communication lines to authorities working and maintained	Y	A.6.1.3
Are Sensors working and maintained	Y	A.11.1.1
Are other Intrusion detection systems working and maintained	Y	A.11.1.1
Are door locks working as intended	Y	A.11.1.3
Can doors be locked/unlocked remotely	Y	A.11.1.3
Are deployable barriers working and maintained	Y	A.11.1.4
Are other delaying mechanisms fit for purpose	Y	A.11.1.4
Are all weapons maintained and operational	Y	A.11.1.4
Are Guards sufficiently trained in weapons and technology	Y	A.8.1.3
Are dispensable materials ready and fit for purpose	Y	A.11.1.4
Are remote operated weapons maintained and operational	Y	A.11.1.4
Are Metal detecting machines working as intended	Y	7.2
Are guards catching contraband entering facility	N, several USBs were able to bypass security	7.2

Stage 6: Risks and Remediation		
Item	Y/N	ISO Clause
Gather Vulnerabilities found in Audit	Y	A.16.1.3
Construct risk matrix	Y	A.17.1.3
Begin Remediation work on critical risks to less impactful risks	Y	A.17.1.1
Discuss whether further auditing is required at this time	Y	A.18.2.1
If yes, proceed to research and hire external professional Auditors	N, not needed at this time	A.18.2.3

Stage 7: Report Results		
Item	Y/N	ISO Clause
Gather all results from Audit and Remediation	Y	A.16.1.7
Transform Results into graphs and statistics, using old data from previous audits	Y	A.16.1.6
Write full report of Audit and Results	Y	A.16.1.2
Develop Information graphics to simplify results	Y	5.30
Present Report and Infographics to Higher Management and Board members	Y	A.16.1.6
Produce Internal announcement for the Auditing Results, changes to procedures and policy, using Infographics	Y	A.16.1.6
Get approval from board members and Higher Ups to distribute Internal announcement	Y	N/A
Distribute Announcement	Y	N/A
Produce marketing information from results of Audit	N, no marketable material gained from audit	N/A
Get approval from board and Higher Ups to release Marketing	N	N/A
Release Marketing	N	N/A
Document all of the Audit timeline	Y	5.33
File away full Audit documentation for future use	Y	5.33

4 Risks, and Remediation

Severe				
High			R2, R5	R4, R6
Medium		R1	R3	
Low				
	Not Likely	**Possible**	**Likely**	**Highly Likely**

Figure 5: Risk Matrix of found issues

This section of the paper focuses on detailing and evaluating the risks found in the Audit, which will then lead to a plan for remediating this issues. After the audit of the Nuclear Facility was completed the list of vulnerabilities and security flaws were gathered to better secure the plant. Each risk was categorised using a auditing ticket, an example of which can be seen in Figure 6, and then added to the risk matrix seen in Figure 5. Six risks where found throughout the Facility, each being of medium severity of higher, a particularly worrying statistic. Furthermore, the likelihood of these risk were all quite high, alerting security staff to fix these issues as soon as possible. Each risk will be addressed in detail within the following subsections.

4.1 R1: Staff Security Knowledge

Certificate Standard	ISO/IEC 27O01: 2013	**Clause**	A.7.2.2
Risk Category	Medium to High		
Stage	4: Inspect Digital Assets and Security		
Item	Are all staff aware and trained in Digital Security and Safety		
Details	Staff were aware of the security standards in place, but did not know the reason why this procedures were in place. A general perception of the Security being "overkill", with complaints about not being allowed personal devices into the workplace		
Remediation	Free educational seminars organised with guest speakers to inform staff on the dangers to nuclear facilities, and how the security mechanisms protect them and the station.		

Figure 6: R1: Staff Security Knowledge ticket

Auditors were happy to find that non-guard staff in the Facility knew and followed Security and Safety procedures put in place. However, it was revealed that staff had no understanding about why they had to follow these rules, which they deemed as "Strict and Overkill". Staff were aware of a the threat of Cyber attacks, but thought specific rules like "No personal devices or storage devices onsite" were ridiculous.

This is a worrying thing to learn, as the resentment towards security standards could lead to future trouble and noncompliance with procedures. One member of staff claimed they had petitioned several time to allow mobile devices onsite to management (claiming he needed his phone to communicate with his pregnant wife), showing the rising tension in the workforce. The entire site is disconnected from the internet to limit potential entry points for attacks, as per Nuclear standards (U.S.NRC, 2013). This does still allow for personal devices to tract malicious software in, if permitted, which could lead to attacks like Stuxnet, which entered Iranian Nuclear Facilities through USBs.

The remediation plan for this is simple, as once the staff are educated on the matter of why each security procedure is in place the likelihood of noncompliance will reduce significantly. Auditors recommend a series of education seminars which staff are incentivised to attend, with guest speakers to make it more interesting and engaging. Furthermore, informative emails can be spread internally to educate staff in a easy to read manner.

4.2 R2: Software Installation Limitation

Certificate Standard	ISO/IEC 27001: 2013	**Clause**	A.12.6.2
Risk Category	High		
Stage	4: Inspect Digital Assets and Security		
Item	Is there a limit on software installation on machines		
Details	Auditors found that staff machines were able to install any software, without restrictions.		
Remediation	Immiedietly deploy an Application Whitelist on all machines in the Facility to allow only approved software to run.		

Figure 7: R2: Software Installation Limitation ticket

Auditors checked whether machines found in the Nuclear Facility were able to have non-approved software installed upon them, through the use of USBs (which will be discussed in section 5.6). The test showed that Windows Auto-run, a commonly used tool for installing malware onto a victim machine, was disabled on the facility workstations, however, no limit was in place. Auditors were able to install several programs onto machines throughout the facility, each being a proof of concept for a potential piece of malware.

The lack of limitations means that any malware that enters the facility has nothing stopping it from acting out the attack, making it a priority to solve this issue. This issue can be easily remediated

through the use of an Application Whitelist, which is a piece of software that only allows approved software to run on machines (Posey, 2019). This is particularly effective for Nuclear Facilities, as workstations run repetitive commands and use the same service everyday, without need for installation of new software. An Application Whitelist would also aid in halting hasty additions to the network, as security teams would have to consult before including any new items to the whitelist.

4.3 R3: Security Patch Deployment

Certificate Standard	ISO/IEC 27O01: 2013	**Clause**	A.14.2.6
Risk Category	Medium to High		
Stage	4: Inspect Digital Assets and Security		
Item	Are Security patches tested before deployment		
Details	IT staff informed auditors that updates are done overnight to avoid loss of work hours, but are not tested before hand.		
Remediation	Update procedure to include testing updates and patches on an isolated virtual machine before deployment.		

Figure 8: R3: Security Patch deployment ticket

When consulting and interviewing the security team it became apparent that there was no procedure to test patches and updates before addition to the network. IT staff claim that updates are done overnight to avoid disrupting key work hours, and claim that if any issue does arise the team can simply solve it by morning, which in their minds was an effective solution. Madnick & Nourian (2018) claim otherwise, stating that updates can also create new problems, citing that a Nuclear Facility was shut down after install an update. This could be a critical issue, causing loss in work hours (or even days), lack of control over vital systems, and potentially a meltdown in the worst case scenario.

The auditors suggest a separated testing environment, containing a virtualised version of the Nuclear Facilities system. This environment would provide the perfect testing bed for new updates and patches to ensure they will not cause damage to the Facility or open up new potential vulnerabilities. Furthermore, this testing environment can be used by IT staff to test new software before addition to the Application Whitelist, making it a particularly effective way to remediate both issues.

4.4 R4: Entry Point Guard Procedure

The gates to the Facility allow for cars to be parked inside, but have a Guard station to stop cars and check Employee ID cards before being allowed past. Subsequent doors are not as heavily manned as the perimeter guard house, making a key part of the Facilities security. Auditors had personal IDs, but decided to use other employees' cards to see if the guards would let them past. Shockingly

several guard allowed entrance into the Facility grounds after seeing the card, failing to check if it matched the person presenting it. Furthermore, on several occasions guards failed to check passenger IDs, only checking the driver of the vehicle.

This is a serious offense to the security standards in place at the Nuclear Facility, as Malicious Attackers could use this to gain unauthorised access to restricted areas. The variety of attacks possible or information an attacker could gather is large, and could lead to future problems for the Facility. Social Engineering techniques could further be employed to gain valuable data about the plant, making it imperative to fix this issue.

Educational Seminars is the recommended remediation plan for this vulnerability, much like the first risk discussed in section 5.1, as educating guards on why standards are in place will greatly help them understand the significance of their role. Guest speakers could give past examples of successful tailgating attacks, and how damaging they can be. Routine tests could also be used to keep guards on their toes, as to not let any intruders into the Facility. It is also recommended that punishments, such as verbal warnings or dock of pay, be used to keep guards diligent at security checks.

Certificate Standard	ISO/IEC 27O01: 2022	**Clause**	7.2
Risk Category	High		
Stage	5: Inspect Physical Assets and Security		
Item	Are Entry point Guards following security procedures		
Details	Guards did not check whether IDs matched the person attempting to gain access, they only cared if there was an employee ID.		
Remediation	Serious seminar restating security procedures to guards, with regular random tests to make sure standards do not slip, and punishment if a guard fails.		

Figure 9: R4: Entry point guard procedure ticket

4.5 R5: Contraband Entering Facility

The Facility operates a metal detecting machine to walk through and X-Ray, which employees put there possessions in before going to work, as to check for contraband such as storage devices or phones. The guards use a metal detection wand to do more thorough checks on any staff who set the primary machine off. The auditors tested this by putting USBs into their bags, and on their person in places like pockets, under hats, and even in socks. Guards caught contraband only when it was obvious, however, any attempt to conceal the device led it to getting through the primary security layers. Guards seemed reluctant to use the metal detection wand, preferring to just wave the auditors through rather than check again. When the wand was used it was never in an effective manner, allowing hidden USBs to pass into the Facility unnoticed.

It has already be emphasised on the importance of preventing outside devices from entering the Facility, and potentially infecting workstations. The lack of care shows the inherent risk to the Facility, so the same Educational steps should be taken so that guards are aware of the security risks that allowing even one USB would present to their place of work. The use of regular tests and punishing failures to catch contraband would also be effective at keeping guards attentive, and thus mitigating this risk.

Certificate Standard	ISO/IEC 27O01: 2022	**Clause**	7.2
Risk Category	High		
Stage	5: Inspect Physical Assets and Security		
Item	Are Guard catching contraband entering facility		
Details	Guards manning the metal detection station did not catch several USB devices in bags as well as on the auditors person.		
Remediation	Education Seminar on why security procedures are in place, regular tests to keep guards up to standard, and punishment if any more contraband enters the Facility.		

Figure 10: R5: Contraband entering facility ticket

4.6 R6: Unpatched Software

Checking the workstations found in the Facility revealed that a majority of them were running unpatched software, thus creating vulnerabilities that could be exploited. Several large scale attacks in the past have been as a result of unpatched systems, such as "WannaCry", which shutdown much of the United Kingdom's national health service back in 2017 (Darzi et al, 2019). WannaCry caused chaos and thousands in losses, it is just as likely that an attack like this could occur in another critical industry, like Nuclear power. Therefore it is key to solve this problem

Auditors recommend a dedicated update day for IT teams, where all systems are checked for the latest security patches. Patches would first be verified in the testing environment as mentioned earlier to assure they would not cause any disruption. It is recommended that updates are scheduled weekly as to maintain on top of the latest patches.

Certificate Standard	ISO/IEC 27O01: 2022	**Clause**	A.14.2.3
Risk Category	High		
Stage	4: Inspect Digital Assets and Security		
Item	Is Software up to date		
Details	Machines were found to be running without security patches		
Remediation	Regular update procedure put in place, once a week, and tested in virtualised enviroment		

Figure 11: R6: Unpatched Software ticket

4.7 Priority of Patches

All the risks found during the audit now have been thoroughly analysed and the proper remediation plans have been created, however, there should be an order to which fixes occur first. Certain risks are more of a priority, or can be conducted quickly, so an ordered list has been created to ensure that important changes to the Facility are done in the most effective and efficiently way.

1. **R4: Entry Point Guard Procedure**
2. **R5: Contraband Entering Facility**
3. **R1: Staff Security Knowledge**
4. **R3: Security Patch Deployment**
5. **R6: Unpatched Software**
6. **R2: Software Installation Limitation**

This list aims to get the pressing matters out of the way first, being the guards manning the entry points and X-Ray machines, as they are the first line of defense. The educational programs for these two risks will be easy to setup and have the most immediate effect on the safety and security of the Facility, thus the reason why they appear first on the priority. As R1 is also solved through education it has been moved up to the third position, as staff education can be done in conjuncture with the guards.

Although the Security Patch Deployment is fourth on the list it can actually be done at the same time as the educational seminars, as it involves the technical rather than Human Resources. Getting the virtualised environment setup for testing patches is key to the remaining items on the list, so takes priority over them. Naturally the Patching procedure can be implemented, which leaves only the Application whitelist which is the least pressing of the vulnerabilities found.

5 Conclusion

In Conclusion, this report thoroughly documents each stage of Security auditing and assessment through a seven step methodology that was shown its use through a realistic audit upon a hypothetical Nuclear Facility. The stages where developed from several examples presented in existing literature, and streamlined to better fit the needs of modern day Nuclear Facilities, which were researched throughout the literature review from part 1 of this report. Each stage was then expanded upon in the constructed checklist, which aimed to walk an auditor through the entire process whilst following standard compliance guidelines of official documents, like the United States Nuclear Regulatory Commission and the ISO/IEC 27001.

The checklist was filled with realistic data, which was then expanded upon in the Risks and Remediation section to evaluate and solve the vulnerabilities found in standard auditing procedure. The results where transformed into a risk matrix and priority list so that Management at a Nuclear Facility would have as easy a time as possible in fixing the issues found. Overall, this report would aid any auditor wishing to understand the nuances of Nuclear Security and Safety in the modern age, and provide a detailed methodology for auditing. The threat of Nuclear meltdown, Radiological Sabotage, terrorism, Cyber attacks, and equipment failure is great towards Nuclear Facilities, but through diligent auditing and assessment security professionals can greatly mitigate these risks for the good of all.

6 References

Corporate Vision. 2021. 12 Must-Include Items In Your Cyber Security Audit Checklist. [online] Corporate Vision News. Available at:
https:
//www.corporatevision-news.com/12-must-include-items-in-your-cyber-security-audit-checklist/
[Accessed 31/10/2022]

Darzi, A., Ghafur, S., Grass, E., Jennings, N.R. 2019. The challenges of cybersecurity in health care: the UK National Health Service as a case study. *The Lancet, Digital Health, Volume 1, Issue 1.* pp. 10-12.

FBI. 2020. Internet Crime Report 2020. Pennsylvania, United States of America. Available at: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf [Accessed 31/10/2022]

Glazer, Y. 2021. Your network security audit checklist. [online] Vulcan. Available at: https://vulcan.io/blog/your-network-security-audit-checklist/ [Accessed 31/10/2022]

Greenberg, A. 2019. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. New York, Anchor Books.

Hyper Plan. N.D. How To Create A Risk Assessment matrix. [online] Hyper Plan. Available at: https://www.hyperplan.com/how-to-create-a-risk-assessment-matrix.html [Accessed 31/10/2022]

Kim, S., Kim, S., Kim, S., Kwon, K.H., Nam, K.H. 2019. Cyber Security Strategy for Nuclear Power Plant through Vital Digital Assets. *2019 International Conference on Computational Science and Computational Intelligence (CSCI)*. pp. 224-226.

Kisi. N.D. Why does your business need a workplace security audit checklist?. [online] Get Kisi. Available at:
https://www.getkisi.com/guides/workplace-security-audit-checklist [Accessed 31/10/2022]

Litherland, P., Piggin, R., Orr, R. 2016. Cyber security of operational technology: understanding differences and achieving balance between nuclear safety and nuclear security. *11th International Conference on System Safety and Cyber-Security (SSCS 2016)*. pp. 1-6.

Madnick, S. & Nourian, A. 2018. A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet. *IEEE Transactions on Dependable and Secure Computing.* pp. 2-13.

Posey, B. 2019. Application whitelisting. [online] Tech Target. Available at:
https://www.techtarget.com/searchsecurity/definition/application-whitelisting [Accessed 15/11/2022]

PurpleSec. 2022. Cyber Security Statistics The Ultimate List Of Stats Data, & Trends For 2022. [online] PurpleSec. Available at:

https://purplesec.us/resources/cyber-security-statistics/ [Accessed 31/10/2022]

SecureFrame. 2022. How to Do an Internal Audit + Security Audit Checklist. [online] SecureFrame. Available at: https://secureframe.com/blog/security-audit-checklist [Accessed 31/10/2022]

United States Nuclear Regulatory Commission (U.S.NRC). 2013. *Nuclear Power Plant Security Assessment Guide*. Rockville, Office of Nuclear Security and Incident Response.