Matthew Roche

X00102929

Abstract

This report will focus on giving detailed insight into the State Claims Agency, it will particularly focus on the newly introduced IT System the National Incident Management System (NIMS) and the impact it has had on the organization.

IM Major CA

A Report on the State Claims Agency

**Table of Contents**

[**Introduction** 2](#_Toc438753427)

[What is the State Claims Agency? 2](#_Toc438753428)

[Why look at the State Claims Agency? 4](#_Toc438753429)

[What is the National Incident Management System? 4](#_Toc438753430)

[**SWOT Analysis – Implementing NIMS** 5](#_Toc438753431)

[Strengths 5](#_Toc438753432)

[Weaknesses 6](#_Toc438753433)

[Opportunities 6](#_Toc438753434)

[Threats 7](#_Toc438753435)

[**Stakeholder** **Analysis** 8](#_Toc438753436)

[**IT Risk Analysis** 10](#_Toc438753437)

[**Strategic Proposals** 14](#_Toc438753438)

[Proposal 1: Increase Training Initiative 14](#_Toc438753439)

[Proposal 2: Publish More Reports 14](#_Toc438753440)

[Proposal 3: Prioritise Rollout to Satellite Sites 15](#_Toc438753441)

[Elements to Monitor 15](#_Toc438753442)

[**Conclusion** 16](#_Toc438753443)

[**References** 17](#_Toc438753444)

[**Table of Figures** 17](#_Toc438753445)

# **Introduction**

## What is the State Claims Agency?

The State Claims Agency is a branch of the larger organization the National Treasury Management Agency (NTMA). The NTMA was established in 1990 with the purpose of managing the National Debt, it has since evolved to manage a much more complicated portfolio of public assets and liabilities. As well as the State Claims Agency and the National Debt, the NTMA manages newERA, the Irish Strategic Investment Fund and, the National Development Finance Agency. The organization also provides staff to the National Asset Management Agency (NAMA) and the Strategic Banking Corporation of Ireland.

Figure 1: Organizational Structure of the NTMA

Given the large and complicated nature of the NTMA as a whole, this report will seek to focus primarily on the State Claims Agency branch of the NTMA. The State Claims Agency was established in 2001 to provide claims and liability management services to the Irish Government, this means that any personal injury, property damage and clinical negligence claims brought against State Authorities are managed by this organization.

The State Claims Agency works with a variety of State Entities such as Government ministers, the Attorney General, healthcare enterprises, An Garda Síochána, prison governors, and community and comprehensive schools amongst others. Legal Claims brought against these Entities are managed by the State Claims Agency.

In all Claims against these State Entities the goal of the State Claims Agency is to ensure that the level of liability taken on by the State is kept to its lowest achievable level. In claims in which the State is determined to be liable, the State Claims Agency seeks to settle claims in a quick and timely manner, and seeks to keep the terms of such cases as reasonable as possible. On the other hand, if the state disputes that it is at fault in a claim the State Claims Agency’s goal is to provide all necessary resources required to defend the State. All Claims are handled by the State Claims Agency from the moment of notification until their resolution.

Currently the State Claims Agency has approximately 110 staff members divided into the following organizational structure:

Figure 2:SCA Organizational Chart

## Why look at the State Claims Agency?

There are a number of reasons I choose to examine the State Claims Agency, firstly as of the time of this writing I am currently employed as temporary staff at the organization, as a result I have a first-hand look at the day-to-day operations of the organization. I am currently working with the National Incident Management System (NIMS) and this proved to be an excellent opportunity to research and examine the workings of the system and gain a greater understanding through personal use and informal discussions with end users of NIMS.

As well as this, given my recent contact with the State Claims Agency there doesn’t seem to be much information about the Agency and the extremely important work that it carries out available to members of the public. All of the information available online is usually buried in large reports or on medical journals. I am personally curious about this agency and thus felt the need to investigate it further.

## What is the National Incident Management System?



Figure 3:NIMS Logo

The State Claims Agency recently implemented a new ICT Database System called the National Incident Management Agency (NIMS) the purpose of this database is to record any adverse incidents including ‘near-misses’ on the premises of over 2,500 locations. These locations are state-run or under the prevue of state entities such as An Garda Siochana, the HSE, the Irish Prison System among others.

This System is extremely useful as it allows a more unified approach to incident reporting and claims investigation. Rather than each state entity having a different approach to incident reporting and disparate repositories in which these incidents are recorded, NIMS allows a unified model for every participating organization.

It also allows much greater analysis capabilities with which to gather statistics regarding incidents, this enables a more responsive approach to responding to issues which have the potential to cause incidents.

# **SWOT Analysis – Implementing NIMS**

For the purposes of this report I have chosen to carry a SWOT Analysis as an alternative to the STEEPLE approach as it is more suitable for this area review. The Case Study being analysed is the task of implementing the NIMS System in the State Claims Agency.

## Strengths

Currently NIMS has been enabled in around 2,500 locations, according an article published in the Irish Medical Times Pat Kirwan, Deputy Director of the SCA stated the following regarding the NIMS rollout:

“The feedback was extremely positive and it was universally acknowledged that in respect of speed, ease of data entry, risk management functionality and data analytics tools significant improvements had been made to the system”

This feedback highlights some of the primary strengths the NIMS system has provided the SCA and its stakeholder’s since it’s depute. The system allows for a greater speed as a result of it being a single commonly used recording system, procedures do not need to be relearned when recording different types of incidents or recording incidents in a separate location.

NIMS also provides much improved risk management functionality. When assessing a case against the government, the SCA has easy access to all relevant information regarding the case in one system. This is an improvement over previous systems which would require a much greater level of work to achieve the same result. Given this greater functionality, decisions can be made with a greater level of knowledge and with a better turnaround time.

Among the State Claims Agency’s stated goals is the effort to “implement targeted personal injury and property damage risk work programmes to mitigate litigation risk” (State Claims Agency, 2015). A critical component to risk mitigation is data analytics, for instance, in 2010 the SCA agency published a report stating that there were over 117,000 reported “slips, trips and falls” in hospitals from the period of January 2004 to December 2009.

This is an example of how data analytics can be utilized to highlight trends which can lead to injury, NIMS provides greater ease of access to these statistics and has been used to reduce state liability.

## Weaknesses

The weaknesses involved in the NIMS rollout are primarily associated with the initial overheads involved in the rollout of any large scale Information System. The Staff members used to the operation of the old System will need to be retrained, this takes time and is generally an unpopular change to the workflow of existing users. The process of transitioning staff is a slow, ongoing process which has caused a short term loss in efficiency. According to staff at the SCA the IT Support line received a significant increase in the number of calls during the rollout process, this is indicative of a high-level of end user issues.

One of the benefits of NIMS is that it provides a greater level of detail in incident reporting, however, this requires a greater input from the Staff members generating the incident. The greater amount of input means generating these reports is more demanding on staff members at NIMS enabled sites.

Another downside to the increased level of detail is a greater incidence of human error present in the reports. Since NIMS relies entirely on human input this can lead to an unreliable assessment of the incident in question.

A System as significant as NIMS is very costly to deploy and maintain. It has a dedicated staff assigned to ensure the rollout continues smoothly. Since NIMS is distributed across over 2,500 sites, the overhead associated with performing security checks on each of these sites is massive. The previously mentioned support helpline also needed to be scaled up to meet the larger number of support requests further adding to the costs.

## Opportunities

The implementation NIMS provides many opportunities to build upon the functions of previous incident reporting solutions. It is built to be able to provide better Data Analytics tools, these tools allow for automatic reporting, are capable of highlighting trends among other features. These improved analytical features can be used to inform health and safety policy to help mitigate risk.

NIMS currently has the opportunity to expand to a greater number of locations such as the Education & Skills sector of the public service. It is also not enabled in every site of each of the major stakeholders, there are still a number of minor satellite sites that NIMS has not expanded into. This expansion would help alleviate risk in a greater number of areas allowing for increased savings in the area of risk.

## Threats

The public sector is very highly subject to the political climate of the country; the National Treasury Management Agency is heavily involved in the management of finance in Ireland, an area subject to a large amount of public scrutiny in recent years. Given the large cost of the NIMS deployment, it is at very real risk of being scaled back as a short term cost saving measure. This would severely cut back the usefulness of the System as it removes the benefit of having all incident reporting targeted to a single repository.

Another point of weakness in NIMS security are the users themselves, the System is subject to falsified reporting which would severely weaken any Incident investigation. This falsified reporting could simply be human error, or it could be the result of a determined effort to undermine an incident’s investigation. This threat would be very difficult to detect given the scale of the System in place.

As well as this, the Staff Members with access to NIMS have the ability to find a large number of personal information regarding anyone involved in an incident. This information could be used against the person involved in the claim. Another risk is the abuse of privileged statistics, for instance, a pregnant staff member could use NIMS to determine which maternity hospital has the lowest level of incidents.

During the initial rollout of the NIMS system there were several outages reported. These outages undermine the integrity of incident reporting as it can lead to a backlog of reports which need to be processed, this leads to an increased incidence of human error. Another Threat to the system is how relatively new it is, any new piece of software is subject to bugs which could potentially be exploited to undermine the System.

Figure 4: SWOT Matrix

# **Stakeholder** **Analysis**

There are a number of stakeholders involved with NIMS, the primary group are the state entities which have implemented NIMS. These groups include the HSE, An Garda Siochana, the Prison Service among others. These groups benefit greatly from the rollout of NIMS to their sites as it allows them to handle incident reporting in an efficient standardised way, it removes the pressure to create and manage their own incident reporting system.

These groups also benefit from Risk Mitigation advice derived from NIMS statistics. An example of this in action was the 2010 report issued by the State Claims Agency related to the large number of “Slips, trips and fall” incidents at HSE locations throughout the country, given this information the HSE can undertake risk mitigation efforts such as procedures to monitor patients, provide non-slip mats in shower areas, and provide better signage around wet floors etc.

Statistics generated by NIMS have also been used by An Garda Siochana to determine areas high-risk areas in terms of collisions between Garda Cars and members of the public. This information has been put to use to inform Garda Patrols.

The other large stakeholder is the NTMA and particularly the State Claims Agency itself. The rollout of NIMS has greatly increased the efficiency of the organization and expanded its ability to advice the various NIMS enabled state entities.

Another Stakeholder is the Department of Finance, and the Taxpayer a whole. Ultimately NIMS is a cost saving measure, by mitigating risk factors in the public service the number of legal claims brought against the state is reduced. This reduction in legal cases brought against the state reduces costs in the area of legal costs for defence and the number of settlements.

A lesser stakeholder is the Court Services of Ireland. The more improved accuracy of incident reporting has allowed for better assessment of the facts in court cases.

Figure 5:Stakeholder Chart

# **IT Risk Analysis**

| **Template Risk Register Entry** | | | | | | | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Part I—Summary Data** | | | | | | | | | | | | | | | | |
| **Risk statement** | ***National Incident Management System Data Breach*** | | | | | | | | | | | | | | | |
| **Risk owner** | ***SCA IT Security*** | | | | | | | | | | | | | | | |
| **Date of last risk assessment** | ***2015/01/12*** | | | | | | | | | | | | | | | |
| **Due date for update of risk assessment** | ***2016/01/12*** | | | | | | | | | | | | | | | |
| **Risk category** | **🞏 Strategic**  **(IT benefit/value**  **enablement)** | | | | | **🞏 Project Delivery**  **(IT program and**  **project delivery)** | | | | | **☑ Operational**  **(IT operations and**  **service delivery)** | | | | | |
| **Risk classification (copied from risk analysis results)** | **🞏 Low** | | | **☑ Medium** | | | | | **🞏 High** | | | | | **🞏 Very high** | | |
| **Risk response** | **🞏 Accept** | | | **🞏 Transfer** | | | | | **☑ Mitigate** | | | | | **🞏 Avoid** | | |
| **Part II—Risk Description** | | | | | | | | | | | | | | | | |
| **Title** | ***Data Breach of the National Incident Management System*** | | | | | | | | | | | | | | | |
| **High-level scenario (from list of sample high level scenarios)** | ***An Unauthorized Third Party gains access to the National Incident Management System gaining access to confidential information such as Health Records, Claim Details etc.*** | | | | | | | | | | | | | | | |
| **Detailed scenario description—scenario components** | Actor | ***Unauthorized Third Party*** | | | | | | | | | | | | | | |
| Threat type | ***Malicious*** | | | | | | | | | | | | | | |
| Event | **Malicious Third Party gains access to NIMS, gains access to a large amount of confidential information, a massive information leak occurs** | | | | | | | | | | | | | | |
| Asset/  resource | **NIMS enabled terminal** | | | | | | | | | | | | | | |
| **Part III—Risk Analysis Results** | | | | | | | | | | | | | | | | |
| **Frequency of scenario (# times per year)** | **0** | | **1** | | **2** | | | **3** | | | | **4** | | | | **5** |
| **N≤0.01**  **☑** | | **0.01<N≤0.1**  **🞏** | | **0.1<N≤1**  **🞏** | | | **1<N≤10**  **🞏** | | | | **10<N≤100**  **🞏** | | | | **100<N**  **🞏** |
| **Comments on frequency** | ***This scenario is very unlikely due to the security steps taken, however the consequences would be severe*** | | | | | | | | | | | | | | | |
| **Impact of scenario on business** | **0** | | **1** | | **2** | | | **3** | | | | **4** | | | | **5** |
| 1. **Productivity** | **Revenue loss over one year** | | | | | | | | | | | | | | | |
| **Impact rating** | **I≤0.1%**  **N/A** | | **0.1%<I≤1%**  **N/A** | | **1%<I≤3%**  **N/A** | | | **3%<I≤5%**  **N/A** | | | | **5%<I≤10%**  **N/A** | | | | **10%<I**  **N/A** |
| **Detailed description of impact** | ***N/A because this is a Public Organization it is funded by the Government, hence, revenue loss is not an issue*** | | | | | | | | | | | | | | | |
| 1. **Cost of response** | **Expenses associated with managing the loss event (US $)** | | | | | | | | | | | | | | | |
| **Impact rating** | **I≤10k$**  **🞏** | | **10k$<I≤100k$**  **🞏** | | **100k$<I≤1M$**  **🞏** | | | **1M$%<I≤10M$**  **🞏** | | | | **10m$<I≤100M$**  **☑** | | | | **100M$<I**  **🞏** |
| **Detailed description of impact** | ***Depending on the severity of the leak, the personal details of several thousand members of the public could be at risk. This would open the state up to severe legal liability.*** | | | | | | | | | | | | | | | |
| 1. **Competitive advantage** | **Drop in customer satisfaction ratings** | | | | | | | | | | | | | | | |
| **Impact rating** | **I≤0.5**  **🞏** | | **0.5<I≤1**  **🞏** | | **1<I≤1,5**  **🞏** | | | **1,57<I≤2**  **🞏** | | | | **2<I≤2,5**  **🞏** | | | | **2,5<I**  **☑** |
| **Detailed description of impact** | **A leak of this nature would have a large impact on the political reputation of the NTMA and the Government as a whole** | | | | | | | | | | | | | | | |
| 1. **Legal** | **Regulatory compliance—Fines (US $)** | | | | | | | | | | | | | | | |
| **Impact rating** | **None**  **🞏** | | **< 1m$**  **🞏** | | **<10m$**  **☑** | | | **<100M$**  **🞏** | | | | **<1B$**  **🞏** | | | | **>1B$**  **🞏** |
| **Detailed description of impact** | ***Given the large Data Breach it is likely that there would be a relatively large legal cost*** | | | | | | | | | | | | | | | |
| **Overall Impact rating** | **4** | | | | | | | | | | | | | | | |
| **Overall rating of risk** | **🞏 Low** | | | **☑ Medium** | | | **🞏 High** | | | | | | **🞏 Very high** | | | |
| **Part IV—Risk Response** | | | | | | | | | | | | | | | | |
| **Risk response for this risk** | **🞏 Accept** | | | **🞏 Transfer** | | | | | **🞏 Mitigate** | | | | | | **X Avoid** | |
| **Justification** | **Given the consequences of this kind data breach, the best course of action would be to take action to avoid it occurring in the first place.** | | | | | | | | | | | | | | | |
| **Detailed description of response (not in case of ‘accept’)** | **Response Action** | | | | | | | | | **Completed** | | | | | **Action Plan** | |
| 1. **Establish proper security protocols to access NIMS** | | | | | | | | | **☑** | | | | | **🞏** | |
| 1. **Monitor unauthorized access requests** | | | | | | | | | **☑** | | | | | **🞏** | |
| 1. **Provide sensitive information on a need-to-know basis** | | | | | | | | | **☑** | | | | | **🞏** | |
| 1. **Educate Staff Members on proper Security Protocols** | | | | | | | | | **🞏** | | | | | **☑** | |
| **Overall status of risk action plan** | ***Currently a great many measures have been taken to secure NIMS against a data leak, however, a better effort could be made to educate members of Staff about these security measures*** | | | | | | | | | | | | | | | |
| **Major issues with risk action plan** | ***The biggest issue with the Risk action plan is the lack of education of staff members about existing security protocols.*** | | | | | | | | | | | | | | | |
| **Overall status of completed responses** | ***Response actions 1-3 have been in place and operational since before the deployment of NIMS*** | | | | | | | | | | | | | | | |
| **Major issues with completed responses** | ***The current responses are not sensitive to malicious actions by authorized employees.*** | | | | | | | | | | | | | | | |
| **Part V—Risk Indicators** | | | | | | | | | | | | | | | | |
| **Key risk indicators for this risk** | **1. A large number of unauthorized access attempts**  ***2. Unusual login activity*** | | | | | | | | | | | | | | | |

# **Strategic Proposals**

## Proposal 1: Increase Training Initiative

Currently the largest issue facing the rollout of NIMS is the general lack of understanding among the users of the System. There is still an abnormal number of support calls being placed to the dedicated NIMS helpline.

An increase in NIMS expertise would dramatically improve efficiency and overall satisfaction with users of the system. A better training program would also reduce human error in the creation of incident reports. This is extremely valuable as NIMS is only useful if the information stored is accurate.

## Proposal 2: Publish More Reports

During my research of this System I noticed a distinct lack of public reports derived from NIMS. The few that I found I thought to be quite interesting, an initiative to publish reports derived from NIMS could raise public awareness of common safety issues, as well as raise awareness about NIMS and the benefit it has for the Irish taxpayer.

An increased public awareness of common risk issues would be valuable as it could allow people to be more proactive and cognisant of common scenarios which could cause an incident, this would improve the standard of risk mitigation.

Raising awareness about NIMS could be of benefit as it could have the effect of improving public support for the initiative, thus putting it on better political ground.

## Proposal 3: Prioritise Rollout to Satellite Sites

Currently NIMS has yet to be rolled out to a number of smaller, more remote sites. This somewhat undermines the usefulness of NIMS as it cannot be fully relied upon to as a universal incident investigation and cataloguing tool.

Currently these sites have their own methodology for recording incidents, this can be incompatible with the new standards and are therefore not as reliable.

## Elements to Monitor

For NIMS to continue to be a success it is important to monitor the continuing rollout of NIMS, paying close attention to the Staff response to the system as well as the accuracy of the recorded incidents.

It is also important to monitor staff to ensure there are no conflicts of interest, for example, a member of staff with access to NIMS should not have friends or relatives involved in a claim against the state.

Further, the rollout of NIMS to more remote satellite locations should be prioritised and monitored closely, these smaller sites are more likely to have more lax security procedures and therefore present a risk of data leakage.

# **Conclusion**

NIMS and the SCA are carrying out a vital role in the day to day operations of the Irish state. They have operated to save the millions of euro and worked to prevent a significant number of accidents.

This report detailed the function of the State Claims Agency and the operation of the National Incident Management System, it provided a SWOT analysis and Stakeholder Analysis of the system and an IT Risk Analysis for the organization. It also provided three core strategic proposals as well as suggesting areas to monitor going forward.

The goal of this report was to provide a greater understanding of the SCA, NIMS and how they operate together.

# **References**

Holmes O'Malley Sexton. (2010, 6 2). *Over 117,000 reported slips, trips and falls in hospitals (2.6.2010)*. Retrieved from Holmes O'Malley Sexton: http://www.homs.ie/whatsnew-publication-120-Over\_117,000\_reported\_slips,\_trips\_and\_falls\_in\_hospitals\_(2.6.2010)

Mudiwa, L. (2013, March 18). *Major upgrade of ‘STARSWeb’ due in September*. Retrieved from Irish Medial Times: http://www.imt.ie/news/latest-news/2013/04/major-upgrade-of-starsweb-due-in-september.html

Mudiwa, L. (2014, June 6). *NAEMS upgrade rollout this month*. Retrieved from Irish Medical Times: http://www.imt.ie/news/latest-news/2014/06/naems-upgrade-rollout-this-month.html

State Claims Agency. (2015, 12 20). *State Claims Agency*. Retrieved from State Claims Agency: http://stateclaims.ie/

# **Table of Figures**

[Figure 1: Organizational Structure of the NTMA 2](file:///C:\Users\Matthew\Desktop\CollegeWork\IM\CA2%20Major\IM%20Major%20CA.docx#_Toc438749020)

[Figure 2:SCA Organizational Chart 3](#_Toc438749021)

[Figure 3:NIMS Logo 4](file:///C:\Users\Matthew\Desktop\CollegeWork\IM\CA2%20Major\IM%20Major%20CA.docx#_Toc438749022)

[Figure 4: SWOT Matrix 7](#_Toc438749023)

[Figure 5:Stakeholder Chart 8](#_Toc438749024)