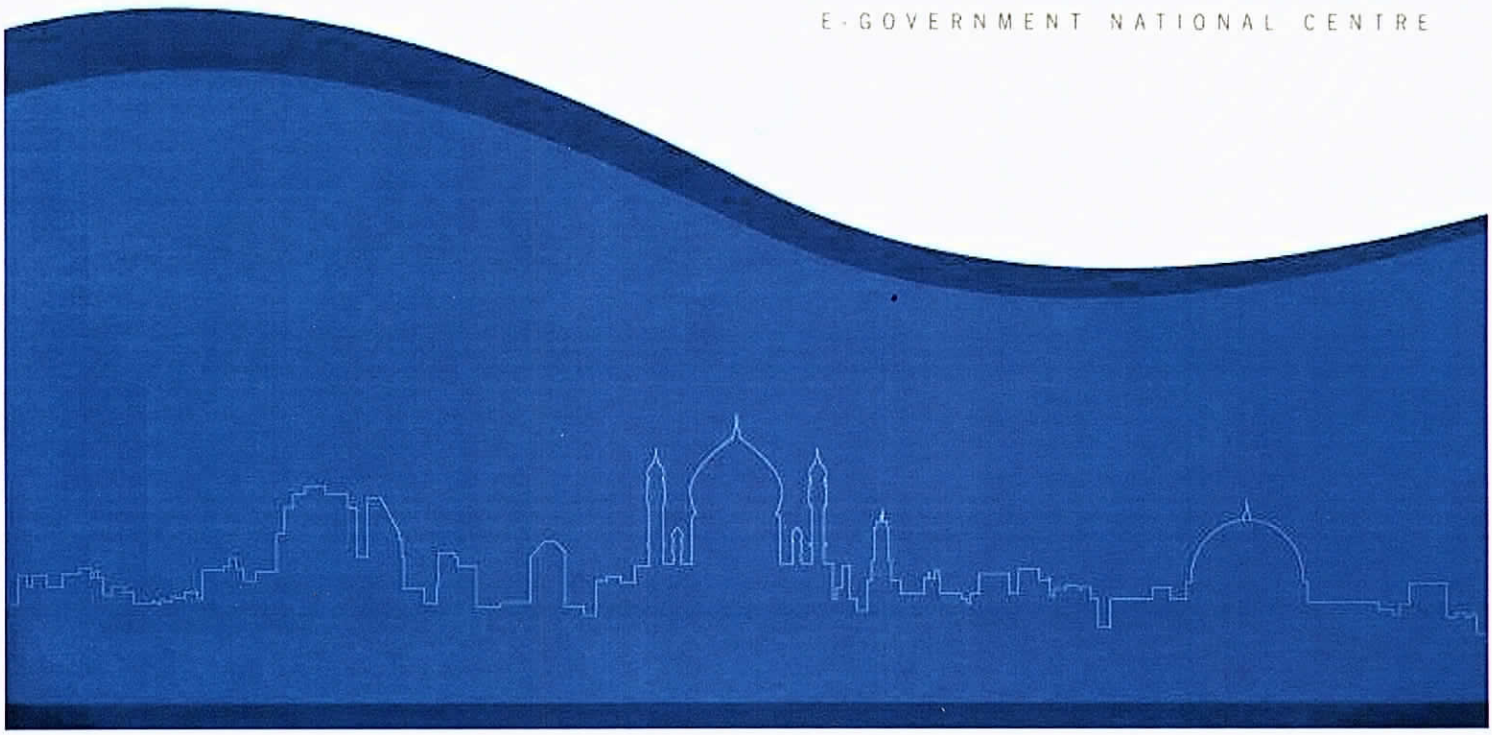
eGNC

E-GOVERNMENT NATIONAL CENTRE



KERTAS KERJA (1)

BAGI JAWATAN DI BAHAGIAN I

Incident Management For E-Government National Centre (EGNC)

Document Control

Document Information

Item	Information
Document Writer	*Hj Ibnu Khairinuddin bin Hj Ibrahim*
Issue Date	24/04/2018
Last Saved Date	28/04/2018
File Name	*Working Paper 1- Incident Management*

Document History

Version	Issue Date	Changes
1.0	24/04/2018	First Draft
2.0	28/04/2018	After COO's review. Added RACI matrix and Statistics.

Distribution for Approval

No	Name	Position	Organisation	Date
1	Dyg Mazriyani binti Hj Abd Ghani	Director	E-Government National Centre [EGNC]	
2	Awg Rudy bin Hj Harun	Chief Operations Officer [COO]	E-Government National Centre [EGNC]	

Document References

Document Name/Website	Created By
Digital Government Strategy 2015-2020, Brunei Darussalam	EGNC, Prime Minister's Office
ITIL Service Operations (IV3-434 5.20) Student Workbook	Quint Wellington Redwood
ITIL Service Operation (2011 Edition)	The Stationary Office (TSO), United Kingdom
Foundation of IT Service Management, Based on ITIL V3	itSMF International

Table of Contents

1. Synopsis

In Information Technology (IT), one of the industries' best practices that is being widely used across governments and companies is the Information Technology Infrastructure Library, known in short as ITIL.

In ITIL terminology, an Incident is defined as an unplanned interruption to an IT service or reduction in the quality of an IT service or a failure of a Configuration Item (CI) that has not yet impacted an IT service.

Hence, this paper outlines the development and implementation of Incident Management in E-Government National Centre, according to the ITIL Version 3 (2011) guidance.

2. Introduction

2.1 Background

2.1.1 E-Government National Centre (EGNC)

Before 2008, E-Government Centre (EGC) was a division under the then Information Technology and State Store Department (ITSSD), Ministry of Finance, assigned to look into E-Government initiatives.

Recognising the importance on developing and implementation of E-Government for Brunei Darussalam to strive forward, a new Department was formed directly under the Prime Minister's Office on the 1st April 2008, known as the E-Government National Centre (EGNC).

EGNC was made responsible to manage the whole IT personnel within the public sector, which at that time was amounting to about 350. In addition, EGNC also provided core IT services to both the public and private sectors, such as E-mail, Co-location and Co-hosting.

Over the years, EGNC has expanded its key IT services, including the capabilities and capacities. Some of the new IT shared services provided includes Central Web Hosting, One-Government Private Cloud and One Government Network.

2.1.2 Brunei Vision 2035

In 2007, Brunei announced the Wawasan Brunei 2035 (Brunei Vision 2035) as a long-term development strategy, aiming to transform the country into a fully developed nation by the year 2035.

The vision is for Brunei Darussalam to be recognised everywhere for:

1. The accomplishment of its well-educated people
2. The quality of life
3. The dynamic, sustainable economy

2.1.3 Digital Government Strategy 2015 - 2020

The Digital Government Strategy 2015-2020 was introduced on the 8th June 2015, during the Fourth ASEAN Chief Information Officers (CIO) Forum, held in Brunei Darussalam.

It is driven by the Brunei Vision 2035, using Information Technology (IT) as an enabler to align and support programmes of the Nation towards those goals.

The Digital Government Strategy has six focus areas, namely: -

1. Service Innovation
2. Collaboration and Integration
3. Capability and Mind-Set
4. Optimisation
5. Security
6. Enterprise Information Management

This paper is supporting the fourth focus area, which is Optimisation. To ensure IT Services can be delivered efficiently, it is imperative that the use of Government assets is optimised, thus maximising the value for money.

2.2 Rational

In order to support the Digital Government Strategy 2015-2020 and Brunei Vision 2035, additions and introductions of new technologies and services by EGNC would be inevitable.

With the increase of latest technologies, application programs, services and connected clients, the IT environment controlled by EGNC will continuously becoming more complex. With that, IT related incidents will become much more challenging to be managed, if not handled in the best way possible.

As such, the need for the development and implementation of Incident Management Process for EGNC, aligning to international best practices standard – ITIL Version 3, was vital.

2.3 Objectives

The objective of this paper is to document the development and implementation of Incident Management Process for EGNC, in order to achieve the followings: -

1. To ensure that standardized methods and procedures are used for efficient and prompt response, analysis, documentation, ongoing management and reporting of incidents.
2. Increase visibility and communication of incidents.
3. To improve the cost-effectiveness of IT services provisions.
4. Enhance the perception of IT through use of an industries' best practices approach in quickly resolving and communicating incidents when they occur.
5. Align Incident Management activities and priorities with those of the EGNC
6. Maintain user satisfaction with the quality of IT services delivered.

2.4 Value to the Department

The value of Incident Management to EGNC would include the followings: -

1. The ability to reduce unnecessary or unplanned labour and costs caused by Incidents.
2. The ability to detect and resolve Incidents which results in lower downtime to the business, which in turn means higher availability of the services provided. This would enable EGNC to exploit the functionality of the services as designed.
3. The ability to align IT activity to real-time priorities, such as the Digital Government Strategy 2015-2020 and Brunei Vision 2035. This is because Incident Management includes the capability to identify business priorities and dynamically allocate resources as necessary.
4. The ability to identify potential improvements to the services. This happens as a result of understanding what constitutes an Incident and also from being in contact with the activities of the operational staffs.
5. The Help Desk can, during its handling of incidents, identify additional service or training requirements.

3. Implementation

3.1 Project Objectives

The objectives of this project are as the followings: -

1. To restore normal operations as quickly as possible
2. To minimize adverse impact on business
3. To ensure best possible levels of service

3.2 Information and Data Collection

Before 2012, there is no dedicated Incident Management Process in place for EGNC. Back then, there was dedicated Helpdesk Team providing support to the IT Services provisioned, with no real emphasis on closely following international best practices.

In 2012, following the restructuring of EGNC Organization Structure, a new division was established, known as Service Management Division (SMD). Under SMD, one of the section is Problem and Incident Management.

For Incident Management, some of the key tasks are as the followings: -

1. Develop, maintain and imply end-to-end management for supervising, controlling or directing how incidents should be handled by communicating with internal or external resources including incident closure (according to ITIL).
2. Involve in the crisis management team for major incidents.
3. Ensure all incidents are reported and correctly categorized and resolved quickly and efficiently.
4. Develop escalation procedure from incident to Problem Management Section.

Hence, the process of establishing Incident Management Process for EGNC started.

3.3 Incident Management Procedure

The Incident Management Procedure is basically the Standard Operation Procedure (SOP) on how to handle IT incidents according to international best practices standard, ITIL version 3 (2011).

It includes the workflow that clearly shows how incident should be handled, as shown in the diagram below.

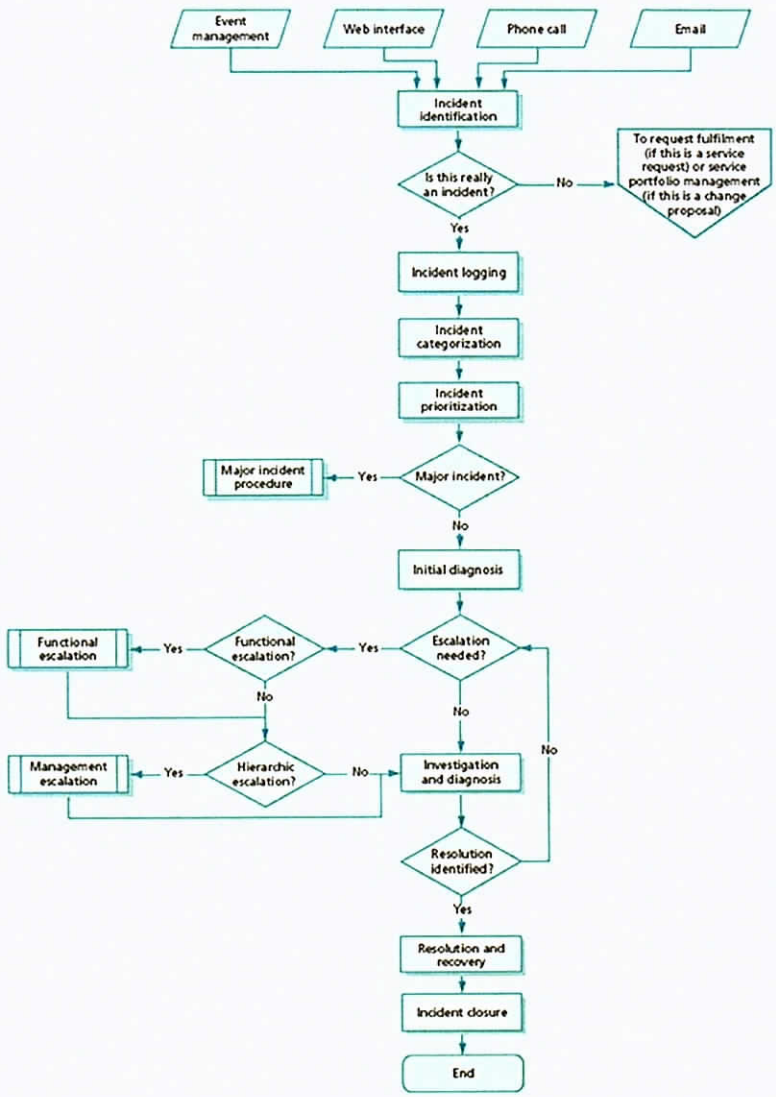


Diagram 1. Incident workflow

3.3.1 Roles and Responsibilities in Incident Management Process

Incident Management Process Owner

The Incident Management Process Owner is accountable for the Incident Management Process and is responsible for identifying improvements to ensure that the process continues to be effective and efficient.

The main roles and responsibilities are:

1. Accountable for the Incident Management Process.
2. Responsible for identifying improvements in ensuring the Incident Management Process continues to be effective and efficient.
3. Ensuring the Incident Management Process is performed in accordance with the agreed and documented process.
4. Documents and publicizes the Incident Management Process.
5. Enforces policy compliance and communication.
6. Evaluate policy effectiveness.

Incident Manager

The Incident Manager is responsible for the effective implementation of the Incident Management Process. It is a much more of a hands-on role and is responsible for the Planning and Coordinating activities of the process.

The main roles and responsibilities are:

1. Responsible for the effective implementation of the Incident Management Process and makes recommendations for improvement.
2. Responsible for the Planning and Coordinating activities of the Incident Process.
3. Drives the effectiveness and efficiency of the Incident Management Process.
4. Manage co-workers handling incident support (First Level & Second Level Support).

5. Manage the Incident Management Systems, to ensure Incident Records are recorded accurately.
6. Work with Change Manager to link Incidents to Changes.
7. Work with Problem Manager to link Incidents to Problems.
8. Convene Major Incident Committee meeting when Major Incident occurs.

First Level Support – Help Desk

The Help Desk is the vital part of the process because it acts as the point of contact for IT users.

The main roles and responsibilities are:

1. Log and classify received Incidents and to undertake an immediate effort in order to restore a failed IT Service as quickly as possible.
2. If no ad-hoc solution can be achieved, First Level Support will transfer the Incident to the Functional Support Team (Second Level Support).

Second Level Support – Functional Support

The Functional Support team consist of Information Security, Data Centre Facilities, Hosting & Storage, Networking, End User Computing, Common Applications and other Service Custodians.

The main roles and responsibilities are:

1. To take over an Incident which cannot be solved immediately with the means of First Level Support.
2. To respond, coordinate and resolve a failed IT Service as quickly as possible.
3. Request external support, e.g. from software or hardware manufacturers, when required.

Third Level Support

The Third Level Support are the Vendors i.e. the suppliers and/or maintainers.

They are also referred to as the Subject Matter Expert, who will provide assistance to the First and/or Second Level Support, when required, in resolving Incidents.

Head of Operations & Infrastructure (OPI)

The main roles and responsibilities are:

1. To coordinate Major Incident resolution, as quickly as possible.
2. Providing inputs for Major Incident Committee on the decision to activate the Emergency Procedure.

Problem Manager

The main roles and responsibilities is:

1. To work with Incident Manager as some incidents may require Problem Manager involvement to investigate and resolve the underlying cause to prevent or reduce the impact of recurrence.

Business Relationship Manager (BRM)

The main roles and responsibilities are:

2. To establish formal communications strategy between EGNC and its clients
3. To inform and update EGNC clients on related IT incidents and dissemination of relevant information appropriately.

In summary, the accountability and responsibility of the roles, in relation to the processes and activities can be shown in the RACI matrix below: -

RACI Diagram **Key to Abbreviations:** **R** - Process / Function Responsible **A** - Process / Function Accountable **C** - Process / Function Consulted **I** - Process / Function Informed **S** - Process / Function Supportive	**Major Roles**					**Secondary Roles**		
Activities \ Roles	Incident Manager	First Level Support	Second Level Support	Third Level Support	Incident Process Owner	Head of OPI	Problem Manager	Business Relationship Manager
Creating the Process								
1- Creating a new process								
Assign Incident Manager role	I	I	I		AR		I	I
Document goals, objectives, and scope	S	I	I		AR		I	I
Adopt and adapt Incident Management process	AR	R	R		S		S	S
Identify Incident categories	AR	S			S		S	I
Decide what data needs to be managed	AR	S	S		C		S	I
Identify granularity of data to be stored in the IMS	AR	S	S		C		S	I
Define interfacing lines with other processes	AR	I	I		S		C	C
Define RACI Chart	S	I	I		AR			
Define CSFs and KPIs	S	I	I		AR			
Incident Management - Activities								
1- Record the users information								
Collect neccessary user data	A	R						
Record details of the Incident	A	R						
2- Classify Incident								
Categorize Incident	A	R						
Determine supportability	A	R						
Prioritize Incident	A	R						
3- Incident Resolution								
Troubleshoot Incident	A	R	R	R			R	
Escalate Incident	A	R	CR	CR			CR	
Send Notification to user	A	R	C	C				R
Apply fix or workaround	A	R	R	R			CR	
To coordinate Major Incident Resolution	A				I	CR	I	I
Update the Incident Record	A	R	R	R			I	
4- Validate, Verify and Close								
Verify Incident resolution with User	A	R					I	
Update and Close Incident Record	A	R					I	
Maintaining the Incident Management Process								
ONGOING								
Review - Ensure Good Service	AR	R			R			
Service Level Monitoring	AR	R			R			
Measure adoption	AR	R			R			
Create improvement plans	AR	R			R			
Execute improvement plans	AR	R			CI			

3.3.2 Incident Categorization

An Incident can be categorized as major or normal incident depending on its severity.

A major Incident can be described as Incident which have the highest level of severity, for example:

1. Having catastrophic business impact i.e. disaster to the enterprise or critical service.
2. Causing complete loss of core (mission critical) business processes / services and work cannot reasonably continue.
3. Disaster Recovery (DR) is required to continue business function or service.

A normal Incident can be described as Incident which may has a high or medium or low level of severity. The table below describes the prioritization code of Normal Incident:

Prioritization Code	Severity Level	Situation
1	**High**	• **Major loss** of a business function / service • **VIP(s) are affected i.e. Deputy Permanent Secretary Level and above** • Example: ▪ **OGN Network / OGPC is almost completely unavailable**
2	**Medium**	• **Partial loss or Degraded service** of one or some business functions / services • Example: ▪ **Some websites under CWH are down** ▪ **Some ministries' OGN are down** o Moderate slow Internet access / Intermittence connections o Some links on EGNC website not accessible
3	**Low**	• No loss of overall business function / service • Example: o Single user not receiving / sending emails, no internet connection, password issue, etc.

3.3.3 Major Incident

When Major Incident occurs, the Major Incident Committee must convene to discuss on the nature of the Incident and make a decision to activate the Emergency Procedure.

After every major incident, the Major Incident Report should be produced in by the relevant service custodian. A review should then be conducted to discuss the report, in order to learn any lessons for the future. Specifically, the review should examine:

1. Things that were done correctly
2. Things that were done wrong
3. What could be done better in the future
4. How to prevent recurrence
5. Whether there has been any third-party responsibility
6. Whether follow-up actions are needed, such as escalation to Problem Management, submission of Request for Change (RFC), etc.

The review should be attended by the respective major incident committee member and the relevant service custodian involve with the respective Incident.

The report and knowledge gained from the review should be documented and stored appropriately, so that it can be used as part of training and awareness activities, in order to prevent or be prepared for similar incidents.

3.4 Incident Management Policy

In addition to the Incident Management Procedure, the establishment of Incident Management Policy was also seen as essential. This is to ensure that the Incident Management Procedure would be carried out in accordance to a set of rules, in alignment to the international best practices standard – ITIL version 3.

The policy statement for the Incident Management are as the followings: -

1. All Incidents must be reported to the First Level Support i.e. assigned Help Desk and logged as Incident Record.
2. Incident Record shall only be opened, closed and re-assigned by the Help Desk, in accordance with the documented Incident Management Procedures.
3. Incidents are classified by priority and categorized according to the Incident Prioritization.
4. The Incident priority may not be downgraded or upgraded unless approved by the Incident Manager.
5. Incidents that require escalation, notification and Change Request, for both Normal and Major Incidents, must follow formally approved procedures, in accordance with the documented Incident Management Procedures.
6. All incidents must be managed in accordance with the EGNC's Operational Level Agreement (OLA) and Service Level Agreement (SLA). Any updates on an Incident must be immediately reflected on the respective Incident Record.
7. Incidents must be correctly prioritized and categorized. If doubt exists, the Incident Manager must assist in the classification and prioritization.
8. Client's feedback must be obtained before closing the Incident Record.
9. Resolved Incidents that are pending while waiting for client's feedback can be closed after 7 working days.
10. Incidents that require pending status must be carried out in accordance with the documented Incident Management Procedures.

The policy also includes the remediation steps for any non-compliance.

3.5 Findings

With the establishment of the Incident Management Process, the next step was to closely monitor the progress and continuously making improvements. One of the way identified was by producing monthly report on how incidents were handled and use it as a benchmark to improve from time to time.

Year	Total Incident Record	Should be Service Request
2012	278	197
2013	327	141
2014	136	5
2015	33	1
2016	53	1
2017	1162	0
2018 (Till Apr)	92	0

Based on the statistic table above, it clearly shows that at the initial stage, there was no clear segregation of recording actual incident and service request. There were too many service requests recorded as an incident, with much of that was a simple password reset request.

According to ITIL guidance, it is important to segregate incidents and service request, so that the monthly reports can reflect clearly on how real incidents are being handled, before improvements could be done.

Hence, several awareness sessions were held, to ensure that the team understand clearly the difference of service request and incident, including the proper way to record it into the system. Compliance to the incident management procedure is indeed the key to success.

Over time, the incident capturing process was more accurate. With that, the next step was to further improve the incident management process. Through continuous discussions amongst the team, a couple of feedbacks were received as suggestions for improvement, such as the followings:

1. Refining the incident categories in the system
2. Adding client notifications step in the workflow
3. Addressing pending incidents
4. Redefining incident prioritizations
5. Redefining roles & responsibilities

With all these improvements, incidents are now better managed in EGNC. The team has better understanding on how to act upon incidents including the resolutions.

Another important use of capturing incident is also to assist in identifying a Problem. In ITIL terminology, a Problem is defined as the underlying cause of one or more incidents. The cause is not usually known at the time a problem record is created, and the problem management process is responsible for further investigation.

Hence, through incidents monthly report, the incident management team was able to identify re-occurring incidents and escalated those to the problem management team. The problem management team was then made responsible to do further investigations on those incidents to find the root-cause.

By resolving the root-cause, it will definitely give positive impact to incidents management, as it will help prevent recurrence of incidents and built solutions database, termed as Known Error Database (KEDB), which will allow the team to use it as a reference if similar problem happening again in the future. This KEDB can also be shared across ministries to act as a knowledge sharing platform, which may help the Government to save cost and time from doing the same thing again and again.

3.6 Challenges and Implications

In order to have a successful Incident Management Process in EGNC, some challenges and implications are inevitable, such as the followings:

1. **Convincing all staff (including users) that all incidents must be recorded**
   Some users have a tendency on not reporting incidents to the Helpdesk. This will inhibit the incident management team from having accurate data on incidents, thus preventing the necessary improvements that could have been done.

2. **Recording incident as early as possible**
   Incidents are sometimes not recorded immediately, which has delayed the resolution of it by the technical team. If this is not addressed, it may lead to damaging reputation for EGNC.

3. **Insufficient human resource**
   Inadequate human resource has led to having one person managing multiple processes. This may cause inefficiency in the long run. Incident Management Process should not be taken as a one-off project; it should constantly be closely monitored.

4. **Having the right tool to manage Incident Management Process**
   Without the help of well working tools, it will definitely slow down the process. This may lead to dissatisfactions amongst the team and will cause loss of interest in following Incident Management Process.

5. **Lack of training**
   In order to fully benefit the implementation of Incident Management Process and ITIL, the whole organisation should at least have the basic understanding on ITIL. Without this, some may not understand what ITIL is for and resist it.

3.7 Review

Implementing Incident Management Process is not like a project with a completion date. It has to be continuously monitored and improved.

Challenges will appear no matter what the situation are, but the most important thing is to approach and solve it in the best way possible, that would lead to positive impact. Thus, creating beneficial effect.

Last but not least, management support is highly required. Such support would help push EGNC to work together as a whole, in implementing a set of practice used internationally.

4. Proposal and Recommendations

4.1 Critical Success Factor (CSF)

In making sure the Incident Management Process will continue to run successfully, the following are the important Critical Success Factor (CSF): -

1. To continue resolving incidents as quickly as possible, thus minimizing impacts on the business.
2. To continue maintaining the quality of IT services provided by EGNC, together with user satisfaction.
3. To increase awareness and communication of Incident Management Process to the whole EGNC personnel.
4. Align incident management activities and priorities with those of EGNC, hence gaining management support.
5. Ensure continuous service improvement activities take place, to maintain the efficiency of the process and increase value for money.

By doing all the above, it is hoped that over time, people will synergise fully with the Incident Management Process, not talking about them. It must be admitted that this may take several years to achieve, but eventually the goal is to have a situation similar to when people are driving a car and reached a stop sign, they do not analyse the sign, but just stop the car. When people are not questioning it or thinking about it indicates that it is working.

4.2 Government-wide Implementation

By taking into account the success of Incident Management Process implementation in EGNC, another way to expand the value to the Government would be implementing it across Ministries, through their respective IT Centre.

Every IT Centre should have its dedicated support team, using the same Help Desk System. The responsibilities of the support team should include managing incident in their Ministry and Departments and any other incidents within the Government. Incidents that do not belongs to them can easily be assigned accordingly to the respective Ministry's support team, simply by assigning the incident ticket through the system.

In addition, the knowledge gained by each support team should be kept under one depository – Central Known Error Database (CKEDB), based in EGNC, which will allow knowledge sharing across the Government. This will allow the ability to resolve incidents much faster on similar incidents, without the need to consume more effort solving what has been solved.

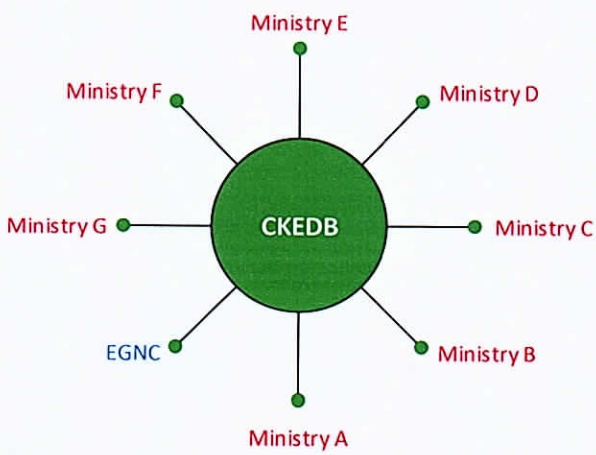


Diagram 2. Government Support Service Structure

5. Summary

Incident Management Process is highly visible to the business, and it is therefore easier to demonstrate the value. Taking this into account, it must be accepted that the successful implementation of Incident Management Process will continue facing challenges.

Hence, it is important that those challenges are not taken lightly and dealt with accordingly. In the long run, this will surely prove beneficial as it may enhance EGNC business image and capabilities.

Such success story then can be replicated across the Government, which may elevate the Government into the elite class that is using the international best practices standard, namely ITIL.

In a larger picture, this will support the Digital Government Strategy 2015-2020, using Information Technology (IT) as an enabler to align and support programmes of the Nation towards the Brunei Vision 2035 goals.