

**BARRY WELSFORD**  
**CHANGE AND TRANSFORMATION CONSULTANT**

# VODAFONE GROUP SECURITY

**T** **echnology Security Services India** (TSSI) based in Bangalore, India is an essential part of Vodafone's worldwide capability to protect its brand, reputation and customer data. TSSI is part of an extensive cyber-security/defence organisation that works 24/7 to keep informational assets at Vodafone both safe and secure.

## GROUP BACKGROUND

Security operations is primary primary responsible for the oversight and monitoring of security systems which are deployed within the specific intent on protecting Vodafones informational assets additionally the TSSI maintains a frontline response team that works on a 24 x 7 basis to field route queries and manage incidents that may arise in relation to the security matters. The introduction of a new departmental head of cyber defence operations within Vodafone group security is that you desire for a full review of the current operational model underlying processes in the TSS I to determine the future shape and intent of the team. The introduction of a new departmental head of Cyber Defence Operations within the Vodafone group security has led to the desire for a full review of the current operating model and underline processes in TSSI to determine the future of the shape and intent of the team.

## Problem

One of the key issues that need to be investigated is that the capability had been taken from a Hungarian operations centre and then delivered to a Indian newly formed operational centre for security.

However it had been quite clear that the documentation and surrounding processes and procedures had not been transferred across to the Bangalore Security Operation Centre.

This meant that the operation centre was totally working in isolation from the rest of the organisation and was acting in what they believe were the right procedures and processes for the day-to-day operations.

There was no evidence of a operating model or functional line alignment to the rest of Vodafone Cyber Defence procedures and processes were very generic although maintained a stable management of problems and incidents it was clear that there was a real risk to Cyber Defence and therefore had to be an understood and a baseline in place to which to work from.

### Objective

- The primary objectives of this assignment were to:
- discover and understand the capabilities within TSS I as it relates to the performance of the daily operational activities
- assess what kind of operating model TSSI are working under and document the “as-is” operational processes within TSSI in a clear and consistent manner
- Identify the key interfaces of TSS I with other teams within Vodafone offering a view as to who is responsible accountable consulted or informed the racing model in each case
- review any existing documentation within TSSI including how it is structured, accessed by the team and other interested parties
- provide a range of longer term improvements within TSS site that will support the change intent of the team going forward
- aligned to the GSOC review findings to present outputs in a unified manner
- provide next step's aligned to the CDO reorganisation program currently underway

### Methodology

General overview:

In order to achieve the intended objectives of this of this discovery the consultant will carry out a variety of activities and use a number of different techniques to acquire the appropriate level of data such that a detailed report and the

deliverables i.e. process models RACI and operating model can be established. In summary the on-site activities/techniques include:

- discussions as to the provision of services by TSSI the Operating Model
- initial process questionnaires to be created ready for circulation prior workshops
- facilitated workshops with key process owners and teams to establish the “as-is” processes
- collection and review of any relevant documentation
- each process owner was interview for their input to the Operating Model and their view to processes involved and what they should look like.
- each identified process was had to go through a facilitated workshop to capture the level 1, level 2 and level 3 process mapping
- all of the documented processes and organisation to be mapped to the CMMI model
- all documented processes to have work instructions added to them
- all support systems reviewed and assessed

## Observations and Outcomes

1. Limited evidence of process or procedural level information found to be present
2. Documentation review relation to work instructions for products only transfer from hungry and not processed related
3. First line security support team will not perform in a triage function but performing a ticket management function assigning tickets to technical functional area
4. FLSS are providing a non-automated monitoring function
  - A. alerting monitoring creating tickets and assigning to functional teams
  - B. taking calls and emails creating tickets in remedy
  - C. resolving closing of tickets managing queues to problem management
  - D. health check in twice a day

- E. taking reports from remedy and distribution to functional teams
5. As an observation TSS I are working to remedies release level and maturity remedy should be raised to the level of stability or suitability for S SIs own business requirements
  6. The Remedy system does require further configuration in a number of areas. Required for the instance:
    - a supported and integrated CMDB
    - configuration items are mapped to services
    - configuration relationships
    - business applications map to the infrastructure
  7. Reporting is currently the responsibility of service management however because of the limitations of remedy the data output has to be managed in Excel to produce in informative report. Other consequences are:
    - F. spending too much time looking for information
    - G. spending too much time building reports
    - H. making decisions without the right information
  8. A common observation within TSSI was the use of key technical resources in all functional areas for project delivery
  9. Using the same in mind for organisation it was agreed that the current state was that ad hoc by assessing the organisation to standard set of questions
    1. structure based on organisation chart not on functions plus hybrid structure, some parts of the organation is aligned by functions
    2. job description defined but not mapped to skills matrix
    3. accountability/responsibilities not clearly articulated for the job
    4. low job satisfaction/morale
    5. distribution

10. Using CMMI for process it was agreed that current state was ad hoc by assessing the processes to be standard set questions

1. processes random, ad hoc, chaotic
2. support environment unstable
3. tendency to over commit
4. inability to repeat passed success

11. Using CMMI for tools it was agreed that current state was ad hoc by assessing the tools to be standard set questions

1. Minimal tools in place
2. Siloed applications and databases
3. Manual
4. Process aligned around tools
5. functionality gaps

12. Using CMMI for tools it was agreed that the current state was ad hoc by assessing the tools to be standard set questions

1. Metrics cannot provide a trusted baseline
2. Metric precision dubious
3. Metrics used defensively
4. Tendency to report any metric you can, rather than aligned to business/ service requirements
5. Unclear and understanding of how metrics are derived.

## Executive Summary

During this discovery phase the consultant has learnt that TSSI team have commented on their lack of structure in the documentation and processes with much of the day-to-day activities being intuitive, this exercise of process discovery has increased their understanding of their current working practices as they are now being documented .

With the plan introduction of some real improvements into remedy introduction of a service desk triage, reduction in and duplication of activity across the functions an improved reporting capability, standardisation of processes and more governance around change management with other key changes to their tool sets and of ways of working, operations can be improved considerably

By making easy incremental improvements and stabilising/formalising their operational activities we can start to bring some order and clarity into the way which they work also by merging TSSI and GCOS processes into the new operating model they can improve and show value of the TSSI capabilities