Cyreath.co.uk
Empirical Pragmatic Testing

Quality System Implementation.

A worked example involving a single team

Discussion Document
By Mark Crowther, Empirical Pragmatic Tester

1.0 INTRODUCTION

1.1 Initiation.
The client provided information, detailed below, to allow a limited demonstration of the application of the model and discussion around further development of their Quality Processes. With this remit it was agreed to identify an area that could be quickly transformed with a view to widening the scope of work at a later date. Full-scale review and planning was not undertaken as it was agreed a number of deliverables would be provided to qualify further activities.

1.2 Overview of the client.
The Client under review is responsible for the security aspects of a department within a company delivering Web products and services. Working in conjunction with a global security department (GSD) this UK based team deliver on a set of key functions and areas of responsibility while working within both their own local departments guidelines and the direction of the GSD.

1.3 Current status.
No formal Quality Management System currently exists though a number of operational guidelines and working practices are in place. Some of these have been developed and defined locally through the activities of the team. Others have been handed down from the GSD. Process interrelation with teams in the local department is not formally established but does occur on a mainly informal level, facilitated by the competency of the Security Analyst heading the local security team.

1.4 Key observations at document review.
Available documentation consisted of a number of presentations, uncontrolled copies of documents from the GSD, a document describing a process that was 'unclear... will need further investigation' and an email containing a number of pieces of information including the body copy of a questionnaire. Additionally a company intranet area was available but was seen to be out of date.

Two clear areas of activity were identified, Unsolicited and malicious email activities and Security Review activities. A number of additional activities and functions were identified but an exact relationship with these two areas was not obvious.

2.0 RECOMMENDATIONS

2.1 Scope of work.
The most complete information was available for the security review activities of the client. In looking for areas to demonstrate the application of the model this was seen as the most accessible area. Additionally, the presentations and supporting documents indicated that these could be brought up to date quickly. Both together would allow immediate benefits to be brought about and demonstrate the value of widening the scope of work at a later date.

2.2 Summary of actions
a) Create an operating procedure to define the Security Review activities.
b) Create a controlled document to capture information required by the procedure and help build auditable quality records.
c) Create a summary log to track repeated use of the procedure and provide management reporting data.
d) Identify process interrelations within the local department and update any existing procedures.
e) Update the intranet area to 'improve visibility throughout the UK business' and communicate the process changes.

2.3 Summary of deliverables

a) Security Review (OP-SEC-001)

This new procedure captures the activities around performing a Security Review with external partners. It identifies the need to address potential areas of security risk around projects and products involving third parties. This activity directly supports the activities of the teams within the local department.

b) Security Review Questionnaire (CD-SEC-001)

The Security Review Questionnaire provides both the business and the partner an opportunity to evaluate the security considerations and risks that may be present and recommend improvements to enhance security. This document forms the permanent quality records for this activity.

c) Security Review Log (CD-SEC-002)

The Security Review Log ensures that the progression of each Security Review issued can be tracked, the status easily reported and the details of the partner retained. This also forms part of the quality records.

d) Identify Process Interrelations

The local department to which the security team belongs operates a work request process. The operational procedure defining this is not formally defined but a control document is in place. It is the recommendation that the four key questions, detailed in section 4.1 of OP-SEC-001, are included in this as a checklist for customers to identify the need for a Security Review.

The operating procedure defining Test and Inspection, OP-QA-001, should also be modified to reflect the need to check for testable elements identified during Security Review. Additional interrelations for the other two teams are implied but not investigated at this time.

e) Update of the security teams Intranet area.

The Clients intranet area was updated to allow improved communication and visibility within the business. Local teams also gain access to updated information reflecting the work undertaken on the process improvements.

3.0 CONCLUSION

On presentation to the client a number of areas for future improvement were identified.

Unsolicited and Malicious Email

Review with the client identified the need for unsolicited and malicious email activities to be detailed in a less technical manner. This would allow these activities to be included in the process review.

Additional Guideline document

The need for a further Guideline document was also identified:
GD-SEC-001 – Overview of UK Security Operations
This Guideline document will provide an overview of the main areas of involvement, core activities and areas of consultancy that the UK Security team can provide the business and it's external partners. The information will also be made available on the company Intranet.

Work with team external to the department

The process noted as requiring 'further investigation' was believed to be the responsibility of two other departments external to the clients, this is out of scope of this current process review.

Total Project Time and Resource

The total resource required for this review was eight hours and one quality engineer