MATT BACAK'S CHECKLIST

Checklist 7 - Implementing SSL Data Encryption

Project Name: _____ **Date:** _____

		Yes	No
	Secure sockets layer (SSL) is a standard networking protocol that establishes encrypted communication (link) between a web server and the browser. The established link ensures that all communication between the web server and the browser remain secure and private. The SSL works by initiating a handshake (the SSL handshake), which allows the browser to establish a secure connection and verify the web server before undertaking any transfer of data. Essentially, the SSL handshake encompasses authentication, decryption, and encryption with a session key, thus validating the session. SSL certificates vary with the number of domains they secure, as well as validation level. SSL certificates based on validation level include organization validated (OV), domain validated (DV), and extended validated (EV) certificates while those based on number of domains they secure include single domain, multi-domain, and wildcard SSL certificates. There are numerous SSL certificate vendors in the market and it is always important to understand which suites your business' needs. Here are factors to consider when implementing an SSL certificate.		
	Part 1 – Reviewing SSL Policies		
1	Identify approved security authorities (CAs).	☐	☐
2	Establish certificate management policies such as minimum renewal period.	☐	☐

Notes

MATT BACAK'S CHECKLIST

Checklist 7 - Implementing SSL Data Encryption

3 Establish private key management policies. ☐ ☐

4 Pinpoint webserver cipher suites and SSL versions. ☐ ☐

5 Implement logging requirements for ease when auditing management operations. ☐ ☐

Part 2 – Verifying Accuracy of Certificates

6 Establish well-defined registration procedures for certificate registrations. ☐ ☐

7 Collect key attributes of the certificates for inventory (i.e. validity periods, key lengths). ☐ ☐

8 Name and identify owners of all certificates and domains. ☐ ☐

Notes

MATT BACAK'S CHECKLIST

Checklist 7 - Implementing SSL Data Encryption

9

Identify where servers are located. ☐ ☐

10

Perform network scans periodically. ☐ ☐

11

Check that all certificates and private keys are reviewed. ☐ ☐

12

Evaluate compliance with corporate EKCM regulations. ☐ ☐

Part 3 – Remediating

13

Ensure all default vendor certificates are controlled. ☐ ☐

14

Check that cipher suites, hashes and weak keys are removed. ☐ ☐

15

Ensure all appropriate certificate types are deployed. ☐ ☐

Notes

MATT BACAK'S CHECKLIST

Checklist 7 - Implementing SSL Data Encryption

16

Check that all management operations are logged to a secure audit log. ☐ ☐

17

Install updated patches on all web services. ☐ ☐

Part 4 – Protecting the Certificates

18

Check that certificates are renewed on time. ☐ ☐

19

Consider automating the renewal process. ☐ ☐

20

Check that certificates and private keys are installed securely. ☐ ☐

21

Avoid reusing private keys when certificates are being renewed. ☐ ☐

Notes

Checklist 7 - Implementing SSL Data Encryption

Part 5 – Monitoring Effectiveness

22

Identify rogue certificates by checking certificate transparency (CT) logs. ☐ ☐

23

Check for dual control and separation of duties. ☐ ☐

24

Review audit logs for compliance and reliability. ☐ ☐

25

Prevent unauthorized certificate requests through theca. ☐ ☐

Notes:

•Avoid improper SSL certificates to mitigate downtimes and prevent access by unauthorized users.

Notes