CHECKLIST

DATA

□ Does data collector destroy media when it is no longer needed for business or legal reasons?

□ Have data and systems been formally classified based on the business value?

□ Are data backup procedures per the commands back up and recovery instruction?

□ What are the data collection and reporting considerations?

□ What sensitive data do you have that needs to be protected?

□ How can it get actionable insights from diverse data?

□ What are the data backup policies and procedures?

□ How do you secure your data centers and facilities?

□ How much data could be disclosed and how sensitive is it?

□ Did the investigator assure of the confidentiality of the data?

□ Does the secure design review process incorporate detailed data-level analysis?

□ Is there any sensitive data in configuration files?

□ Where do you store the metadata?

□ Does data collector store sensitive authentication data after authorization?

□ Is per project data for the cost of assurance activities collected?

□ Can the data collector identify all connections between the data network in your business?

□ Do any users have only partial access to certain types of system data?

□ Does data collector have a procedure for customers wishing to file a grievance or complaint?

□ Does data collector have a risk assessment process in place?

□ How should inputs, functionality, and data be restricted?

□ Does the api access critical data or functions?

□ Is all xml input data validated against an agreed schema?

□ Are you vulnerable to data exposure?

CHECKLIST

□ Is there any way to express how current the data is?

□ Are storage of data and investigating products locked?

□ Does the secure design review process incorporate detailed data level analysis?

□ Has your data been exposed – and would you know if it were?

□ Has the data been assessed as reliable?

□ What are the legal means required for a customers survival when data is corrupted or lost?

□ Who has access to sensitive data – internally and externally?

□ Does the cloud provider charge a fee to remove data upon termination of the contract?

□ Do you predict trends based on the collected data?

□ Is the data sent on encrypted channel?

□ Who is responsible for the oversight of vendors that may hold sensitive data?

□ Do you have control about who can see which data returned from your BI tools?

□ Who is responsible for protecting your sensitive data?

□ What is special about the database case?

□ Does data collector require an employees user name and password to be different?

□ Do you define what data leakage is and what factors can cause data leakage?

□ Are regular compliance checks regarding the collection of personal data and user consent in place?

□ Are users restricted to certain functions and data?

□ Does data collector record and document all investigations and findings?

□ NOTES: