



Virginia Information Technologies Agency

2016 COV IS Conference

April 7-8, 2016



Compliance for BIA & Risk Assessments

I. Introduction

Jon Smith, CSRM

II. BIA

Renea Dickerson, CSRM

III. Risk Assessments

Mauri Shaw, CSRM

IV. Wrap- up/Questions

Jon Smith, CSRM



Authority

Code of Virginia, §2.2-2009

(Additional Powers of the CIO relating to security): ...

H. the CIO shall also develop policies, procedures, and standards that shall address the creation and operation of a risk management program designed to identify information technology security gaps and develop plans to mitigate the gaps. All agencies in the Commonwealth shall cooperate with the CIO. Such cooperation includes, but is not limited to, (I) providing the CIO with information required to create and implement a Commonwealth risk management program; (ii) creating an agency risk management program; and (iii) complying with all other risk management activities.



Risk Management

- IT risk Management is a process to:
 - assess risk in an organization with regards to IT;
 - determine if the amount of risk is appropriate;
 - and administer corrective actions or mitigating controls to bring unacceptable levels of risk within the organization to an risk level



Risk Management (cont'd)

- Some inputs to determine IT risks include:
 - Business impact analysis (BIA)
 - Risk assessments
 - IT system security plans
 - IT security audits
 - IT risk assessments
 - Vulnerability scanning
 - Threat and vulnerability data
 - Asset management
 - Security incidents



Business Impact Analysis Process

The Business Impact Analysis (BIA) is the process of determining the potential consequences of a disruption or degradation of business functions.

The process entails identifies all business functions, identifies mission essential agency functions and identifies the resources required to support the functions.



Why Conduct a Business Impact Analysis

Once the Business Impact Analysis is successfully completed, the results are instrumental in identifying agency risks to mission critical agency business processes and IT resources.

The information assists with data classification and data identification activities used in identifying and remediating risks and can also be valuable to developing agency recovery strategies.



How Business Impact Analysis Information is Used

The Business Impact Analysis (BIA) also collects information on the systems used by agencies. The IT system information as well as additional collected BIA data is imported into Archer where it is used in rating business functions for availability, confidentiality and integrity.

Used in aggregate, it can assist in identifying agency IT dependencies. Combining the data with information from other COV agencies is valuable in painting a picture of Commonwealth-wide IT risk.



Business Impact Analysis Template Extract

Listed below is a section of the BIA template header. The entire template can be found on the VITA Home Page at: <http://www.vita.virginia.gov/default.aspx?id=537>

The screenshot shows a Microsoft Excel spreadsheet titled "BIA_Spreadsheet_Example for Presentation.xlsx". The spreadsheet is on "Sheet2" and displays the header for a Business Impact Analysis template. The columns are labeled A through AC, and the rows are numbered 1. The header text is as follows:

Agency	Business Function	Primary Function Objective	If Function Requires External Systems, Please List Them	If Function Requires Internal Systems, Please List Them	Is this Function a Mission Essential Business Function or Supports a Mission Essential Business Function? Yes or No	Provide the RTO (Days) for this function	Provide the RPO (Days) for this function	Does This Function Process or Store Data Sensitive Relative to Confidentiality? Yes or No	If the Function Processes or Stores Data Sensitive Relative to Confidentiality, Describe the System and the Confidential Data	Provide the Number of Confidential Records Stored or Processed	Life	Safety	Finances	Legality	Regulation/Compliance	Customer Service/Publicity	Privacy Impact on Agencies and Citizens
--------	-------------------	----------------------------	---	---	---	--	--	---	---	--	------	--------	----------	----------	-----------------------	----------------------------	---



Business Impact Analysis Example Condensed

BIA_Spreadsheet_Example for Presentation.xlsx - Microsoft Excel

File Home Insert Page Layout Formulas Data Review View

A1 Agency

	A	B	C	J	N	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	
	Agency	Business Function	Primary Function Objective	Describe Data Used As Input	If Function Requires External Systems, Please List Them	If Function Requires Internal Systems, Please List Them	Is this Function a Mission Essential Business Function or Supports a Mission Essential Business Function? Yes or No	Provide the RTO (Days) for this function	Provide the RPO (Days) for this function	Does This Function Process or Store Data Sensitive Relative to Confidentiality? Yes or No	If the Function Processes or Stores Data Sensitive Relative to Confidentiality, Describe the System and the Confidential Data	Provide the Number of Confidential Records Stored or Processed	Life	Safety	Finances	Legality	Regulation/Compliance	Customer Service/Publicity	Privacy Impact on Agencies and Citizens	
1																				
2	PPP	Administer Restaurant Licenses	Provide licenses for restaurants	Personally Identifiable information - birth certificates, etc.	Violations Database	Licensee System, Vital Statistics System	Yes	6	7	Yes	Vital Statistics System - Personally Identifiable Information	50,000	0	0	2	1	2	2	3	
3	PPP	Administer Health Care Licenses	Provide licenses for healthcare providers	Personally Identifiable information - birth certificates, etc.	Violations Database	Licensee System, Vital Statistics System	Yes	6	7	Yes	Vital Statistics System - Personally Identifiable Information	50,000	0	0	2	1	2	2	3	

VITA BIA Spreadsheet Sheet2

Select destination and press ENTER or choose Paste

Average: 5002.3 Count: 87 Sum: 100046 100%



Business Impact Analysis Requirements (Highlights)

Reporting requirements:

Each agency ISO is required to submit the results of the periodic review and revision of the agency BIA to the CISO annually.

- An online template to capture the required information is provided on the VITA Website.
- Provide the required Recovery Time Objective (RTO) based on agency and COV goals, objectives, and Mission Essential Functions (MEFs)
- Provide the Recovery Point Objectives (RPO)



Business Impact Analysis - RTO - RPO

BIA_Spreadsheet_Example for Presentation.xlsx - Microsoft Excel

File Home Insert Page Layout Formulas Data Review View

A1 Agency

	A	B	C	N	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC
	Agency	Business Function	Primary Function Objective	If Function Requires External Systems, Please List Them	If Function Requires Internal Systems, Please List Them	Is this Function a Mission Essential Business Function or Supports a Mission Essential Business Function? Yes or No	Provide the RTO (Days) for this function	Provide the RPO (Days) for this function	Does This Function Process or Store Data Sensitive Relative to Confidentiality? Yes or No	If the Function Processes or Stores Data Sensitive Relative to Confidentiality, Describe the System and the Confidential Data	Provide the Number of Confidential Records Stored or Processed	Life	Safety	Finances	Legality	Regulation/Compliance	Customer Service/Publicity	Privacy Impact on Agencies and Citizens
1																		
2	PPP	Administer Restaurant Licenses	Provide licenses for restaurants	Violations Database	Licensee System, Vital Statistics System	Yes	6	7	Yes	Vital Statistics System - Personally Identifiable Information	50,000	0	0	2	1	2	2	3
3	PPP	Administer Health Care Licenses	Provide licenses for healthcare providers	Violations Database	Licensee System, Vital Statistics System	Yes	6	7	Yes	Vital Statistics System - Personally Identifiable Information	50,000	0	0	2	1	2	2	3

BIA Spreadsheet

Ready

104%



Business Impact Analysis (Highlights cont.)

Reporting requirements (cont.):

Provide the following additional BIA data information:

- Business Function Name
- Primary Objective of each Business Function
- Description of the data used as input to each business function
- The external and internal systems used by each function
- Each of the internal agency systems that is still being used, should be associated with one or more of the agency business functions.



Business Impact Analysis Function - Name, Function Objective & Systems

Microsoft Excel

BIA_Spreadsheet_Example for Presentation.xlsx

	A	B	C	N	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC
1	Agency	Business Function	Primary Function Objective	If Function Requires External Systems, Please List Them	If Function Requires Internal Systems, Please List Them	Is this Function a Mission Essential Business Function or Supports a Mission Essential Business Function? Yes or No	Provide the RTO (Days) for this function	Provide the RPO (Days) for this function	Does This Function Process or Store Data Sensitive Relative to Confidentiality? Yes or No	If the Function Processes or Stores Data Sensitive Relative to Confidentiality, Describe the System and the Confidential Data	Provide the Number of Confidential Records Stored or Processed	Life	Safety	Finances	Legality	Regulation/Compliance	Customer Service/Publicity	Privacy Impact on Agencies and Citizens
3	PPP	Administer Health Care Licenses	Provide licenses for healthcare providers	Violations Database	Licensee System, Vital Statistics System	Yes	6	7	Yes	Vital Statistics System - Personally Identifiable Information	50,000	0	0	2	1	2	2	3

BIA Spreadsheet

Ready 104%



Business Impact Analysis (Highlights cont.)

Reporting requirements (cont.):

- Identify Mission Essential Functions (MEFs).
- Indicate whether the business function uses sensitive data.
- When the business function uses sensitive data, provide a description of the data and the number of records.



Business Impact Analysis Function – MEF & Confidential Records

Microsoft Excel

File Home Insert Page Layout Formulas Data Review View

A1 Agency

BIA_Spreadsheet_Example for Presentation.xlsx

	A	B	C	N	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC
1	Agency	Business Function	Primary Function Objective	If Function Requires External Systems, Please List Them	If Function Requires Internal Systems, Please List Them	Is this Function a Mission Essential Business Function or Supports a Mission Essential Business Function? Yes or No	Provide the RTO (Days) for this function	Provide the RPO (Days) for this function	Does This Function Process or Store Data Sensitive Relative to Confidentiality? Yes or No	If the Function Processes or Stores Data Sensitive Relative to Confidentiality, Describe the System and the Confidential Data	Provide the Number of Confidential Records Stored or Processed	Life	Safety	Finances	Legality	Regulation/Compliance	Customer Service/Publicity	Privacy Impact on Agencies and Citizens
3	PPP	Administer Health Care Licenses	Provide licenses for healthcare providers	Violations Database	Licensee System, Vital Statistics System	Yes	6	7	Yes	Vital Statistics System - Personally Identifiable Information	50,000	0	0	2	1	2	2	3

BIA Spreadsheet

Select destination and press ENTER or choose Paste

Average: 5002.3 Count: 87 Sum: 100046 104%



Business Impact Analysis (Highlights cont.)

Reporting requirements (cont.):

- Evaluate each function for the impact of non-performance. The impacts requested in the business impact analysis template are:
 - Life
 - Safety
 - Finances
 - Legality
 - Regulation/Compliance
 - Customer Service/Publicity
 - Privacy Impact on Agencies and Citizens
- Business Function Owner Name.
- Date BIA completed.
- Person Completing the BIA.



Business Impact Analysis Function – Function Ratings

Microsoft Excel

File Home Insert Page Layout Formulas Data Review View

A1 Agency

BIA_Spreadsheet_Example for Presentation.xlsx

	A	B	C	N	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC
1	Agency	Business Function	Primary Function Objective	If Function Requires External Systems, Please List Them	If Function Requires Internal Systems, Please List Them	Is this Function a Mission Essential Business Function or Supports a Mission Essential Business Function? Yes or No	Provide the RTO (Days) for this function	Provide the RPO (Days) for this function	Does This Function Process or Store Data Sensitive Relative to Confidentiality? Yes or No	If the Function Processes or Stores Data Sensitive Relative to Confidentiality, Describe the System and the Confidential Data	Provide the Number of Confidential Records Stored or Processed	Life	Safety	Finances	Legality	Regulation/Compliance	Customer Service/Publicity	Privacy Impact on Agencies and Citizens
3	PPP	Administer Health Care Licenses	Provide licenses for healthcare providers	Violations Database	Licensee System, Vital Statistics System	Yes	6	7	Yes	Vital Statistics System - Personally Identifiable Information	50,000	0	0	2	1	2	2	3

BIA Spreadsheet

Ready Average: 5002.3 Count: 87 Sum: 100046 104%



Probability of Occurrence

Life: Probability that someone might lose their life if function is not performed (Recommend using Level 0 or 3)
Safety: Probability someone would be harmed if function is not performed
Finances: Probability that assets or dollars would be lost if function is not performed
Legality: Probability that the agency would be subject to lawsuits/sanctions if function not performed
Regulation/Compliance: Probability that the agency would violate or be non-compliant with laws or regulations if function not performed
Customer Service/Publicity: Probability that the customer service level/base will lose access to data required to perform essential/primary business processes and adverse publicity if this function is not performed
Privacy Impact on Agencies & Citizens: Probability that unauthorized data would be disclosed to individuals or information systems if the applications supporting this function are unavailable or compromised



Business Function Ratings Scale

Level Rating Table	
Level	Description
3	Direct high impact and high likelihood of occurrence
2	Direct minimal impact and high likelihood of occurrence or direct high impact and minimal likelihood of occurrence
1	Indirect high impact and minimal likelihood of occurrence
0	Indirect minimal impact and minimal likelihood of occurrence



Business Impact Analysis Results

This presentation revolved around the fields that receive the most questions, however the remaining fields are also important and play an important role in the business impact process.

The IT information collected during the process can be used as a primary input to:

- IT System and Data Sensitivity Classification
- Risk Assessments
- IT security audit plan
- System Security Plans
- Contingency Planning



Risk Assessment (RA)

Risk Assessment Overview Mauri Shaw



Risk Assessment (RA) – Process - Benefit

- ❑ Process - an assessment of risk, from unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and/or the information it processes, stores, or transmits.
- ❑ The benefit will provide an evaluation of security controls in place to determine if the risks identified will negatively impact the agency's mission with respect to a potential breach in Confidentiality, Integrity and Availability.



RA Reporting requirements

- IT Risk Management Standard (SEC520-00)
 - ❖ Risk Assessment Plan (3.3.2)
 - ❖ Risk Assessment Template (3.3.5)
 - ❖ Risk Assessment Treatment Plan (3.3.5)
- IT Security Standard (SEC501.9)
 - ❖ Risk Assessment Report (RA-3)



RA Process - Step by Step

- From the BIA Process – we have identified:
 - 1) Mission Essential Functions (MEFs).
 - 2) MEFs using sensitive data.
 - 3) Mapping the sensitive data to Internal IT applications supporting Business Functions.
 - 4) Data Classifications for sensitive data.



RA (Process - Step by Step)

5. Complete Risk Assessment Plan (RAP)

- (Sensitive Systems and Proposed RA Dates)

6. Complete Risk Assessment

- Identify security controls in place > SEC501 Questionnaire.
- Complete RA Risk Template > using Questionnaire responses
- Complete the Risk Treatment Plan > Risk Template
- Create the Risk Report (e.g. Summary using Treatment Plan)



RA (Risk Assessment Plan Example)

Agency Information		Contact Information					
Agency Name	Virginia Information Technologies Agency	Name	Jonathan Smith				
Agency Acronym	VITA	Title	Director, VITA CSRM, Risk Management				
Agency Number	136	E-mail	jonathan.smith@vita.virginia.gov				
Date of submission	May 20, 2016	Phone	804-416-7167				
IT System Acronym *	IT System Name	Planned Assessor	Date Last Assessed (MM/YY)	Scheduled Assessment Completion Date (Minimum once every 3 years)			Areas for Special Emphasis and Additional RA Requirements
				2015 (MM/YY)	2016 (MM/YY)	2017 (MM/YY)	
VLS	Licensee System	M Shaw	12/14			12/17	
XYZ	Xtra Years of Zest	M Shaw	New		06/16		New application found during dataset inventory Nov 2015.



RA (Security Control Questionnaire – SEC501.9)

LICENSEE System Example Questionnaire

<u>Control Family</u>	#	System Risk Assessment (Application Security)	Control in Place? (Yes)/(No)	Comments (e.g. "If control not in place", state compensating Control)
SI-2	12	Is System data in test/development sanitized? (e.g. Sensitive information is removed from a record for testing)	No	Test system is accessible only to authorized users same as production system. For replicating production issues, data from production is cloned to test system as needed. Confidentiality of data is rated as "Low".
SI-4	13	Do developers have access to sensitive System data? (describe developer access controls)	No	Access to Dev, Test, and Production systems is controlled through different Application Security Application instance. Only authorized users are granted access to Test and Prod instances as deemed appropriate based on their job function.
	23	System Owners ensure that system administrators have both an administrative account and user account?	No	As of now, single COV AD account is used by system administrators to access the system.
AU 1-11	31	Are there compensating controls in place for SysAdmins with modify rights to the audit log to ensure that unauthorized changes to it are detected? (e.g. all changes to any audit logs are detected and reviewed and approved by mgmt).	No	



RA Risk Assessment Template Example

LICENSEE EXAMPLE SYSTEM - Risk Assessment Template														
Risk ID (Question#)	Confidentiality	Integrity	Availability	Risk Assessment Completion Date MM/YY	Risk Vulnerability Family (Ref. SEC 501)	SEC 501 Control ID (e.g. AC-1, RA-5, etc.)	Cybersecurity Framework Subcategory	Risk Vulnerability	Risk Threat	Risk Summary	Magnitude of Impact	Controls in Place (ref. Misc. Comments)	Exception on file	Misc. Comments
#12	Low			12/14	SI - System and Information Integrity	SI-2	PR.IP-2: A System Development Life Cycle to manage systems is implemented	Procedures are not in place for removing test data.	Sensitive system data integrity is exposed while in test/development environment.	Limiting access to authorized users for testing still allows access to sensitive data .	Low	Yes	No	Test system is accessible only to authorized users same as production system. For replicating production issues, data from production is cloned to test system as needed. Confidentiality of data is rated as "Low".
#13	Low			12/14	SI - System and Information Integrity	SI-4	PR.DS-1: Data-at-rest is protected	Procedures are not in place for sensitive system data changes by system development staff.	Data integrity for Sensitive System data is at risk when sensitive data is not removed for testing.	Limiting access to authorized users for testing still allows access to sensitive data	Low	Yes	No	Access to Dev, Test, and Production systems is controlled through different Application Security Application instance. Only authorized users are granted access to Test and Prod instances as deemed appropriate based on their job function.
#23		Medium		12/14	AC - Access Control	Ac-6	PR.AT-2: Privileged users understand roles & responsibilities	Procedures are not in place to allow system admins to use one logon for admin purposes and one logon for regular duties	Improper segregation of duties	System integrity is at risk when using admin privileges for both environments.	Medium	No	No	As of now, single COV AD account is used by system administrators to access the system.



RA _ IT Risk Treatment Plan

Licensee_Security_RiskTreatmentPlan.xlsx v2.xlsx - Microsoft Excel

File Home Insert Page Layout Formulas Data Review View

E11 Risk Summary

A B C D E F G H I J

1
2
3
4
5
6
7

Risk Treatment Plan

PURPOSE: This Risk Treatment Plan used to document planned corrective actions for identified information technology security gaps.

8	Risk Name	Ref Below								
9	Agency Name	VITA								
10	IT Systems Affected	Licensee								
11	Risk Finding ID #	Authoritative Source (SEC 501, Enterprise Policy, Operating Instruction, etc)	Control ID (e.g. AC-2, policy number, operating instruction, etc)	Date Risk Identified	Risk Summary	Remediation Plan	Risk Rating (Low, Med, High, Critical)	Status (Identification Stage, ISO Notification, Risk Treatment Plan Underway, Closed, Escalation - Agency Head Notification, Escalation - CID Notification, Escalation - Cabinet Secretary Notification)	Status Date	Remediation Completion Date
12	#12	SEC501.8	SI-2	12/14	Limiting access to authorized users for testing still allows access to sensitive data	Plan to further restrict access to sensitive system testing data and develop procedures to ensure testing data is purged.	Low	Risk Treatment Plan Underway	9 30 2015	Updated Status has been requested
13	#13	SEC501.8	SI-4	12/14	Limiting access to authorized users for testing still allows access to sensitive data	Plan to further restrict access to sensitive system testing data and develop procedures to ensure testing data is purged.	Low	Risk Treatment Plan Underway	9 30 2015	Updated Status has been requested
14	#23	SEC501.8	AC-6	12/14	System integrity is at risk when using admin privileges for both environments.	Sys Admin duties/tasks need to be performed while logged in as a Sys Admin - separate Sys Admin account S/B established.	Medium	Risk Treatment Plan Underway	9 30 2015	Updated Status has been requested
15	#31	SEC501.8	AU 1-11	12/14	Unintentional or intentional changes to the system audit log are possible.	System audit log file procedures are needed and should include responsibility for audit log file changes.	High	Risk Treatment Plan Underway	9 30 2015	Updated Status has been requested
16	#40	SEC501.8	CP-2	12/14	The IT DRP (Disaster Recovery Plan) for the sensitive system environment does not support the restoration of VAS.	Review/create plan for restoration of VAS.	Medium	Risk Treatment Plan Underway	9 30 2015	DR Plan update underway - status

Ready Risk Treatment Plan



RA – (Summary Report – Partial)

IT System Risk Assessment Summary

For

Virginia Information Technologies Agency

April 2015



Risk Assessment – (Report – Partial)

VITA Risk Assessment Summary Contents

<u>EXECUTIVE SUMMARY</u>	<u>1</u>
<u>INTRODUCTION</u>	<u>3</u>
<u>GOALS AND OBJECTIVES</u>	<u>3</u>
<u>Methodology</u>	<u>3</u>
<u>Methodology (cont.)</u>	<u>4</u>
<u>CONCLUSIONS</u>	<u>4</u>
<u>RECOMMENDATIONS</u>	<u>4</u>
<u>APPENDICES</u>	<u>6</u>
<u>Key Roles</u>	<u>6</u>
<u>Threat, Vulnerability and Risk Definitions</u>	<u>6</u>
<u>Risk Assessment Results</u>	<u>6</u>
<u>Definitions</u>	<u>6</u>
<u>Key Roles</u>	<u>7</u>
<u>Key Roles (Cont.)</u>	<u>8</u>
<u>Threat, Vulnerability and Risk Definitions</u>	<u>9</u>
<u>Risk Assessment Results</u>	<u>10</u>



What does VITA do with this information

VITA/CSRM actively use the information from the results as inputs to decision making:

- Prioritization of restoration (outage/security incident)
- IT governance and security oversight of IT projects, procurements, and hosting requests
- Seek enterprise solutions for widespread issues
- Track remediation/mitigation of identified risks and findings
- Prioritize efforts to provide audit and security services for the new service centers, based on risk



How does VITA use the data

VITA/CSRM utilizes a GRC tool (RSA Archer) as a relational database to assess and assist perform governance, risk and compliance processes

Reports are loaded into Archer in order to associate:

- Business processes
- Applications
- Devices (servers, etc...)
- Audit findings
- Risk assessment findings
- Vulnerability scan results
- Threat and vulnerability information
- IT security incidents



Future state

VITA is currently loading the rest of the 2015 BIA data into Archer

Agencies may be required to directly enter or update business process information into Archer as the system of record – no more spreadsheets! (unless by exception)

VITA will be creating risk profiles for agency applications based on the documentation submitted by the agencies as well as additional inputs, such as vulnerability scanning results

VITA will review with agencies where apparent gaps, misclassification of IT systems, or significant risks exist



More Questions???

For additional information please contact:
CommonwealthSecurity@vita.virginia.gov

Thank You!



RA Overview

End of Presentation



Risk Assessment (RA)

Risk Assessment Overview Mauri Shaw