### Archer GRC Tool- Risk Assessment Overview

**Inventory Gathering**

Risk Assessment is done on IT assets: applications, databases, workstations and servers used to access, store or process healthcare related information. The Excel spreadsheet is used to capture the IT inventory, business units and Divisions names where the healthcare information is hosted or used. Names of individuals who are responsible for the support, maintenance and compliance of the inventory are also captured in the spreadsheet.

Excel spreadsheet template is available HERE. (insert link here)

If you have any questions on how to complete the inventory gathering spreadsheet- please check the Frequently Asked Questions- FAQs section on the website.

If you still need assistance, please submit a Service Now ticket or send email to xxx@emory.edu to create the Service Now ticket for you and a member of Enterprise Security- IT Compliance team will answer your question.

Please send the completed spreadsheet to archer-support@emory.edu

**Archer Inventory Loading**

Archer admin will load the inventory into Archer tool. Risk Assessments in Archer can be completed as needed. Once you decide to start the assessment, please let Enterprise Security- IT Compliance team at archer-support@emory.edu know that you are ready and assessment will be activated for you.

Once the assessment starts, you have 30 days to complete it, the countdown will start within Archer tool and your items will be tracked and may become overdue if not completed. The compliance score for your area will also start calculating based on the added assessments and results of the assessments.

**Archer Risk Assessment counts**

Once as assessment is activated- you have 30 days to complete the assessment, review it and Reject or Approve.

High Severity Findings have 30 business days to create a remediation plan and complete it or create an exception request and review, reject/approve it.

Medium Severity Findings have 60 business days to create a remediation plan and complete it or create an exception request and review, reject/approve it.

Low Severity Findings have 90 business days to create a remediation plan and complete it or create an exception request and review, reject/approve it.

All overdue items will affect the overall compliance scores for your IT assets, business unit, division and overall Emory compliance.

**Risk Assessment roles in Archer**

**Assessment Submitter**- a user who is most familiar with application, database, workstations, server or business unit used to access, store or process sensitive healthcare information

**HWGM/Reviewer**- a user who oversees and have authority to approve the compliance state of the application, database, workstations, server or business unit used to access, store or process sensitive healthcare information

**Responsible Party**- a user who is responsible for the overall compliance, security and operations for the application, database, workstations, server or business unit used to access, store or process sensitive healthcare information.

**Risk Assessment Workflow**

***Completing the Risk Assessment***

1. Archer admin activates the assessment in Archer
2. Auto generated email is sent to Assessment Submitter to say that the assessment is ready to be completed
3. Assessment Submitter completes the assessment and Submits it for the review
4. Auto generated email is sent to HWGM/Reviewer to say that the assessment is ready to be reviewed
5. HWGM/Reviewer reviews the assessment
	1. If HWGM/Reviewer doesn’t not agree with some answers, HWGM/Reviewer Rejects the assessment with notes back to Assessment Submitter
	2. If HWGM/Reviewer agrees with all provided answers, HWGM/Reviewer Approves the assessment.
6. Auto generated email is sent to Assessment Submitter to say that the assessment is either Rejected or Approved
7. If the assessment is Rejected, Assessment Submitter corrects the Assessment and re-Submits
8. Auto generated email is sent to HWGM/Reviewer to say that the assessment is ready to be reviewed
9. HWGM/Reviewer reviews the assessment and Rejects or Approves it

Once the Assessment is approved, every NO answer will generate a finding.

All outstanding Assessment and all available Assessment can be viewed via dashboards in Archer to track the progress and check on the status of the assessments.

***Addressing the Findings***

1. If the assessment is Approved, NO answers are converted to findings
2. Each finding is auto assigned to Assessment Submitter
3. Auto generated email is sent to Assessment Submitter to say that findings are ready to be addressed
4. Assessment Submitter or HWGM/Reviewer can reassign the finding to another user in Archer if Assessment Submitter is not the correct person to remediate the finding.
5. Assessment Submitter or a reassigned findings owner creates a remediation plan for each finding or creates one remediation plan for multiple findings and Submits.

Each Remediation Plan is executed until completion.

All outstanding Findings and Remediation Plans and all available Findings and Remediation Plans can be viewed via dashboards in Archer to track the progress.

***Creating the Exception Requests***

A very small number of findings could not be remediation and will require an Exception Request. Each Exception needs 2 levels of approvals.

1. Assessment Submitter or reassigned finding owner creates an Exception Request for each finding or one Exception Request for multiple findings and Submits it
2. Auto generated email is sent to HWGM/Reviewer to say that an exception is ready to be reviewed
3. HWGM/Reviewer reviews the exception
4. If HWGM/Reviewer doesn’t agree with the provided reason for the exception, HWGM/Reviewer Rejects the request with notes back to Assessment Submitter or reassigned findings owner
5. If HWGM/Reviewer agrees with the provided reason, HWGM/Reviewer Approves the request.
6. Auto generated email is sent to Assessment Submitter to say that the request is either Rejected or Approved
7. If the Exception Request is Rejected, Assessment Submitter either corrects the request and re-Submits or creates a remediation plan and Submits it.
8. Auto generated email is sent to HWGM/Reviewer to say that the updated request is ready to be reviewed
9. HWGM/Reviewer reviews the Exception Request and Rejects or Approves

If HWGM/Reviewer approves the Exception Request, the 2nd level of approval is initiated and the request is sent to the Responsible Party

1. Auto generated email is sent to Responsible Party to say that an exception is ready to be reviewed
2. Responsible Party reviews the exception
	1. If Responsible Party doesn’t agree with the provided reason for the exception, Responsible Party Rejects the request with notes back to Assessment Submitter or reassigned findings owner
	2. If Responsible Party agrees with the provided reason, Responsible Party Approves the request.
3. Auto generated email is sent to Assessment Submitter to say that the request is either Rejected or Approved
4. If the Exception Request is Rejected, Assessment Submitter either corrects the request and re-Submits it to HWGM/Reviewer for 1st round of approval or creates a remediation plan and Submits it.

Each Exception Request is reviewed and re-evaluated according to the Emory Enterprise HIPAA Security Policies.

All outstanding Exception Requests and all available Exception Requests can be viewed via dashboards in Archer to track the progress.