

S. No.	Page #	Point / Clause #	Clarification point as stated in the tender	Comment/ Suggestion/ Deviation	IFTAS Response
1	Page 6	7 - Eligibility Criteria. Sr. No. 2	Audited financial statements indicating the net profit and the networth as required set forth in the eligibility criteria. and Auditor / Chartered Accountant Certificate in support of the criterion.	<p>Since, we are submitting Audited Balance Sheet and P&L Account statement, is the <u>Auditor / Chartered Accountant Certificate</u> still required.</p> <p>In case it is not required, please ask them to amend clause as "Audited financial statements indicating the net profit and the networth as required set forth in the eligibility criteria or Auditor / Chartered Accountant Certificate in support of the criterion".</p>	Audited financial statements indicating the net profit and the networth OR Chartered Accountant Certificate in support of the criterion to be submitted
2	Page 6	7 - Eligibility Criteria. Sr. No. 2	Audited financial statements indicating the net profit and the networth as required set forth in the eligibility criteria. and Auditor / Chartered Accountant Certificate in support of the criterion.	<p>Since, we are submitting Audited Balance Sheet and P&L Account statement, is the <u>Auditor / Chartered Accountant Certificate</u> still required.</p> <p>In case it is not required, please ask them to amend clause as "Audited financial statements indicating the net profit and the networth as required set forth in the eligibility criteria or Auditor / Chartered Accountant Certificate in support of the criterion".</p>	Audited financial statements indicating the net profit and the networth OR Chartered Accountant Certificate in support of the criterion to be submitted
3	Page 6	7 - Eligibility Criteria. Sr. No. 2	Audited financial statements indicating the net profit and the networth as required set forth in the eligibility criteria. and Auditor / Chartered Accountant Certificate in support of the criterion.	<p>Since, we are submitting Audited Balance Sheet and P&L Account statement, is the <u>Auditor / Chartered Accountant Certificate</u> still required.</p> <p>In case it is not required, please ask them to amend clause as "Audited financial statements indicating the net profit and the networth as required set forth in the eligibility criteria or Auditor / Chartered Accountant Certificate in support of the criterion".</p>	Audited financial statements indicating the net profit and the networth OR Chartered Accountant Certificate in support of the criterion to be submitted

4	Page 7	7 - Eligibility Criteria. Sr. No. 4	The Bidder should provide reference of any 3 clients for whom the bidder has supplied or implemented similar Solution including at least one Government/public/BFSI in India	We suggest that instead can we have the following statement as the Eligibility Criteria - "The Bidder /OEM should provide reference of any 3 clients for whom the bidder has supplied or implemented similar Solution including at least one Government/public/BFSI in India".	As per RFP
5	Page 7	7 - Eligibility Criteria. Sr. No. 4	The Bidder should provide reference of any 3 clients for whom the bidder has supplied or implemented similar Solution including at least one Government/public/BFSI in India	We suggest that instead can we have the following statement as the Eligibility Criteria - "The Bidder /OEM should provide reference of any 3 clients for whom the bidder has supplied or implemented similar Solution including at least one Government/public/BFSI in India".	As per RFP
6	Page 7	7 - Eligibility Criteria. Sr. No. 4	The Bidder should provide reference of any 3 clients for whom the bidder has supplied or implemented similar Solution including at least one Government/public/BFSI in India	We suggest that instead can we have the following statement as the Eligibility Criteria - "The Bidder /OEM should provide reference of any 3 clients for whom the bidder has supplied or implemented similar Solution including at least one Government/public/BFSI in India".	As per RFP
7	Page 7	7 - Eligibility Criteria. Sr. No. 5	The bidder should have certified with ISO 27001:2013 standards	We suggest that instead can we have the following statement as the Eligibility Criteria - "The Bidder /OEM should have certified with ISO 27001:2013 standards".	As per RFP
8	Page 7	7 - Eligibility Criteria. Sr. No. 5	The bidder should have certified with ISO 27001:2013 standards	We suggest that instead can we have the following statement as the Eligibility Criteria - "The Bidder /OEM should have certified with ISO 27001:2013 standards".	As per RFP
9	Page 15	Annexure- I: Technical Requirement Data Discovery Module Sl. No.:- 11	<u>Technical Description :-</u> Search data sets by facets, keywords or business terms	We need more clarification on this (except for keyword), if possible please give an example.	Solution must support data search by facets, keywords OR business terms

10	Page 15	Annexure- I: Technical Requirement Data Discovery Module Sl. No.:- 11	<u>Technical Description :-</u> Search data sets by facets, keywords or business terms	We need more clarification on this (except for keyword), if possible please give an example.	Solution must support data search by facets, keywords OR business terms
11	Page 15	Annexure- I: Technical Requirement Data Discovery Module Sl. No.:- 11	<u>Technical Description :-</u> Search data sets by facets, keywords or business terms	We need more clarification on this (except for keyword), if possible please give an example.	Solution must support data search by facets, keywords OR business terms
12	Page 15	Annexure- I: Technical Requirement Data Discovery Module Sl. No.:- 14	<u>Technical Description :-</u> The solution must have ability to encrypt data elements of interest.	We need more clarification on this as to which encryption solution is expected to be implemented.	Any inbuilt, available with the proposed Solution
13	Page 15	Annexure- I: Technical Requirement Data Discovery Module Sl. No.:- 14	<u>Technical Description :-</u> The solution must have ability to encrypt data elements of interest.	We need more clarification on this as to which encryption solution is expected to be implemented.	Any inbuilt, available with the proposed Solution
14	Page 15	Annexure- I: Technical Requirement Data Discovery Module Sl. No.:- 14	<u>Technical Description :-</u> The solution must have ability to encrypt data elements of interest.	We need more clarification on this as to which encryption solution is expected to be implemented.	Any inbuilt, available with the proposed Solution
15	Page 15	Annexure- I: Technical Requirement Data Discovery Module Sl. No.:- 16	<u>Technical Description :-</u> The solution must have the capability to Discover, Classify and Protect the documents without any user intervention.	We need to understand if any DRM solution is deployed or likely to be deployed. As Klassify data discovery and compliance suite has an ability to protect documents with the help of in-built integration with Seclore-DRM solution once the sensitive data is discovered. This also stands true when the data is classified while being generated.	IRM/DRM deployment will be done in later phase and The Solution must integrate with the IRM/DRM

16	Page 15	Annexure- I: Technical Requirement Data Discovery Module Sl. No.:- 16	<u>Technical Description :-</u> The solution must have the capability to Discover, Classify and Protect the documents without any user intervention.	We need to understand if any DRM solution is deployed or likely to be deployed. As Klassify data discovery and compliance suite has an ability to protect documents with the help of in-built integration with Seclore-DRM solution once the sensitive data is discovered. This also stands true when the data is classified while being generated.	IRM/DRM deployment will be done in later phase and The Solution must integrate with the IRM/DRM
17	Page 15	Annexure- I: Technical Requirement Data Discovery Module Sl. No.:- 16	<u>Technical Description :-</u> The solution must have the capability to Discover, Classify and Protect the documents without any user intervention.	We need to understand if any DRM solution is deployed or likely to be deployed. As Klassify data discovery and compliance suite has an ability to protect documents with the help of in-built integration with Seclore-DRM solution once the sensitive data is discovered. This also stands true when the data is classified while being generated.	IRM/DRM deployment will be done in later phase and The Solution must integrate with the IRM/DRM
18	Page 15	Annexure- I: Technical Requirement Data Discovery Module Sl. No.:- 7	<u>Technical Description :-</u> The solution must have ability to identify what objects within a system contain personal information about a data subject before retrieving the data.	We need more clarification on this, if possible please give an example.	Object is referred to "set of information", it can be a file
19	Page 15	Annexure- I: Technical Requirement Data Discovery Module Sl. No.:- 7	<u>Technical Description :-</u> The solution must have ability to identify what objects within a system contain personal information about a data subject before retrieving the data.	We need more clarification on this, if possible please give an example.	Object is referred to "set of information", it can be a file
20	Page 15	Annexure- I: Technical Requirement Data Discovery Module Sl. No.:- 7	<u>Technical Description :-</u> The solution must have ability to identify what objects within a system contain personal information about a data subject before retrieving the data.	We need more clarification on this, if possible please give an example.	Object is referred to "set of information", it can be a file

21	Page 15	Annexure- I: Technical Requirement Data Discovery Module Sl. No.:- 8	<u>Technical Description :-</u> The solution must have ability to control the amount of personal information retrieved in response to a data subject access request to manage volume of data.	We need more clarification on this, if possible please give an example.	The is not a core feature of Data Discovery and will be treated as Optional Specification
22	Page 15	Annexure- I: Technical Requirement Data Discovery Module Sl. No.:- 8	<u>Technical Description :-</u> The solution must have ability to control the amount of personal information retrieved in response to a data subject access request to manage volume of data.	We need more clarification on this, if possible please give an example.	The is not a core feature of Data Discovery and will be treated as Optional Specification
23	Page 15	Annexure- I: Technical Requirement Data Discovery Module Sl. No.:- 8	<u>Technical Description :-</u> The solution must have ability to control the amount of personal information retrieved in response to a data subject access request to manage volume of data.	We need more clarification on this, if possible please give an example.	The is not a core feature of Data Discovery and will be treated as Optional Specification
24	Page 11	Annexure- I: Technical Requirement Sl. No.:- 29	<u>Technical Description :-</u> The solution should support the ability to warn or prevent users from sending password-protected Microsoft Office documents via email. (The metadata in password-protected Office documents is encrypted, so this capability provides an alternative way to enforce policy.)	We need more clarification, whether the end-user can skip the password protected file or to enforce users to type the password so that metadata can be read and classification of the email can be decided.	User sending sensitive data via MS Office password protected files can be controlled with warn and prevent method
25	Page 11	Annexure- I: Technical Requirement Sl. No.:- 29	<u>Technical Description :-</u> The solution should support the ability to warn or prevent users from sending password-protected Microsoft Office documents via email. (The metadata in password-protected Office documents is encrypted, so this capability provides an alternative way to enforce policy.)	We need more clarification, whether the end-user can skip the password protected file or to enforce users to type the password so that metadata can be read and classification of the email can be decided.	User sending sensitive data via MS Office password proeted files can be controlled with warn and prevent method
26	Page 11	Annexure- I: Technical Requirement Sl. No.:- 29	<u>Technical Description :-</u> The solution should support the ability to warn or prevent users from sending password-protected Microsoft Office documents via email. (The metadata in password-protected Office documents is encrypted, so this capability provides an alternative way to enforce policy.)	We need more clarification, whether the end-user can skip the password protected file or to enforce users to type the password so that metadata can be read and classification of the email can be decided.	User sending sensitive data via MS Office password proeted files can be controlled with warn and prevent method

27	Page 13	Annexure- I: Technical Requirement Sl. No.:- 51	<u>Technical Description :-</u> The solution must provide the capability where the Classification solution can add special tags to email messages and the messages are then automatically secured from unauthorized access, especially when shared externally.	We need more clarification as to what special tags are referred as. Also, please confirm if securing the email after classification is expected through DRM.	1. Special tags can be a added in metadata. 2. Yes, once IRM/DRM is available
28	Page 13	Annexure- I: Technical Requirement Sl. No.:- 51	<u>Technical Description :-</u> The solution must provide the capability where the Classification solution can add special tags to email messages and the messages are then automatically secured from unauthorized access, especially when shared externally.	We need more clarification as to what special tags are referred as. Also, please confirm if securing the email after classification is expected through DRM.	1. Special tags can be a added in metadata. 2. Yes, once IRM/DRM is available
29	Page 13	Annexure- I: Technical Requirement Sl. No.:- 51	<u>Technical Description :-</u> The solution must provide the capability where the Classification solution can add special tags to email messages and the messages are then automatically secured from unauthorized access, especially when shared externally.	We need more clarification as to what special tags are referred as. Also, please confirm if securing the email after classification is expected through DRM.	1. Special tags can be a added in metadata. 2. Yes, once IRM/DRM is available
30	Page 13	Annexure- I: Technical Requirement Sl. No.:- 58	<u>Technical Description :-</u> The solution should support customizable visual markings in email and documents (e.g. font (name/size/features), size, Colour, and content).	We need more clarification specially on features option.	Here features referred to various formatting options available with the fonts.
31	Page 13	Annexure- I: Technical Requirement Sl. No.:- 58	<u>Technical Description :-</u> The solution should support customizable visual markings in email and documents (e.g. font (name/size/features), size, Colour, and content).	We need more clarification specially on features option.	Here features referred to various formatting options available with the fonts.
32	Page 13	Annexure- I: Technical Requirement Sl. No.:- 58	<u>Technical Description :-</u> The solution should support customizable visual markings in email and documents (e.g. font (name/size/features), size, Colour, and content).	We need more clarification specially on features option.	Here features referred to various formatting options available with the fonts.
33	Page 17	Annexure- III: Commercial (Quotation) Format	Commercial details format contains both the Subscription Model and Perpetual Model details.	FOR THE BIDDER - If we can quote on subscription based commercials and ignore Perpetual. Kindly confirm as both (Subscription Model and Perpetual Model) format are mentioned.	IFTAS prefer "Perpetual" model. The bidder must propose all the licensing model available by OEM

34	Page 17	Annexure- III: Commercial (Quotation) Format	Commercial details format contains both the Subscription Model and Perpetual Model details.	Kindly confirm as both Subscription Model and Perpetual Model format are mentioned.	IFTAS prefer "Perpetual" model. The bidder must propose all the licensing model available by OEM
35	Page 17	Annexure- III: Commercial (Quotation) Format	Commercial details format contains both the Subscription Model and Perpetual Model details.	FOR THE BIDDER - If we can quote on subscription based commercials and ignore Perpetual. Kindly confirm as both (Subscription Model and Perpetual Model format are mentioned.	IFTAS prefer "Perpetual" model. The bidder must propose all the licensing model available by OEM
36	NA	Public Procurement (Preference to Make in India), Order 2017	Not mentioned/covered	IFTAS is requested to follow the guidelines on Public Procurement (Preference to Make in India), Order 2017 (PPP-MII Order), Order No. P-45021/2/2017-BEII dated 15.06.2017, as amended by Order No. P-45021/2/2017-BE-II dated 28.05.2018 and Order No.P-45021/2/2017-BE-II dated 29.05.2019 and revision issued vide letter No. P-45021/2/2017(BE-II) dated 04.06.2020.	As per RFP
37	NA	Public Procurement (Preference to Make in India), Order 2017	Not mentioned/covered	IFTAS is requested to follow the guidelines on Public Procurement (Preference to Make in India), Order 2017 (PPP-MII Order), Order No. P-45021/2/2017-BEII dated 15.06.2017, as amended by Order No. P-45021/2/2017-BE-II dated 28.05.2018 and Order No.P-45021/2/2017-BE-II dated 29.05.2019 and revision issued vide letter No. P-45021/2/2017(BE-II) dated 04.06.2020.	As per RFP

38	NA	Public Procurement (Preference to Make in India), Order 2017	Not mentioned/covered	IFTAS is requested to follow the guidelines on Public Procurement (Preference to Make in India), Order 2017 (PPP-MII Order), Order No. P-45021/2/2017-BEII dated 15.06.2017, as amended by Order No. P-45021/2/2017-BE-II dated 28.05.2018 and Order No.P-45021/2/2017-BE-II dated 29.05.2019 and revision issued vide letter No. P-45021/2/2017(BE-II) dated 04.06.2020.	As per RFP
39	10b	Payment Terms and Conditions	Subscription cost will be paid quarterly in arrears.	Request change to annual advance	As per RFP
40	10c	Payment Terms and Conditions	In-case of perpetual license, 100% license cost will be paid post license deployment and AMC charges will be paid quarterly in arrears post expiry of warranty.	Request change to annual advance for AMC charges	As per RFP
41		Annexure- I: Technical Requirement	The solution should trigger classification for document on Save, Save As, print etc. and should be configurable using a management mechanism.	Differs from point 'e' on page 6 of RFP which talks about other events like Open, Print, etc Suggested Point: The solution should trigger policy and classification actions based on different events, such as Save, Save-as, Open, Print, Forward, Close, Send or Classification Change	As per RFP, Bidder to propose the best practices in the RFP response
42		Annexure- I: Technical Requirement	The solution shall have capability to send emails from mobile with classification applied for both IOS and Android based mobiles.	MDM is required for enforcement of policies on mobile devices hence this needs to integrate with existing MDM or it can be covered in phase 2. Suggested Point: The solution should enable the classification of email on iOS and Android mobile devices by integrating with MDM solutions like Vmware, Blackberry.	As per RFP, Bidder to propose the best practices in the RFP response
43		Annexure- I: Technical Requirement	The solution should provide built-in reports and dashboards to analyse user behaviour and system health. Roadmap	Not sure what 'Roadmap' means here.	Please read as "The solution should provide built-in reports and dashboards to analyse user behaviour and system health."

44		Annexure- I: Technical Requirement	The solution should have a capability to deploy, upgrade, uninstall the component without the use of any 3rd party software.	Many solutions are deployed using 3rd party tools like GPO, SCCM. This point also contradicts point 49 mentioned below hence suggest removal or change as suggested Suggested Point: The solution should have a capability to deploy, upgrade, uninstall the component with/without the use of any 3rd party software but the same should be done centrally.	As per RFP, Bidder to propose the best practices in the RFP response
45		Annexure- I: Technical Requirement	The solution should have capability to deploy policies basis users, machines, groups etc.	Suggested Point: The solution should have the ability to integrate with AD natively and enforce policies based on AD groups and enable administrators to tailor configurations to individual users machines or groups of users	As per RFP, Bidder to propose the best practices in the RFP response
46		Annexure- I: Technical Requirement	Solution should provide classification logs inside the classified file and at the centralized repository.	Logs are stored in central repository and only Metadata is added to file. Logs addition to files would change integrity of the file. Suggested Point: Solution should provide classification Metadata inside the classified file and logs at the centralized repository.	As per RFP, Bidder to propose the best practices in the RFP response
47		Annexure- I: Technical Requirement	The solution should support the ability to quarantine files stored inappropriately, flag files for follow-up, or act based on results of the scan. This may include quarantine, delete, encrypt through 3rd party encryption tools, etc.	Needs to be under discovery section	Treat this requirement under as technical specification of "Data Discovery"
48		Annexure- I: Technical Requirement	The solution should integrate with DLP, encryption, Information right management (IRM) and Digital rights management (DRM) solution.	Pls specify existing tools for integration support. Suggested Point: The solution can integrate with full fledged DLP tools and not tools like Trend Micro DLP	Bidder have to provide the list of 3rd party solution which can be integrated with the proposed solution
49		Annexure- I: Technical Requirement	The solution should provide the ability to attach metadata to information objects, which can be leveraged by e-discovery solutions.	Needs to be under discovery section	As per RFP, Bidder to update the remarks in response
50		Annexure- I: Technical Requirement	The solution must have ability to assign classification level to discovered data elements according to customer policy	Needs to be under discovery section	As per RFP, Bidder to update the remarks in response

51		Annexure- I: Technical Requirement	The solution must have the capability to do analysis (discovering sensitive data) Based on Compliance requirement (PII, PHI, etc.)	These points are applicable under discovery section. Remediation actions are not taken on user endpoints.	Treat this requirement under as technical specification of "Data Discovery"
52		Annexure- I: Technical Requirement	The solution must have the capability to do analysis (discovering sensitive data) Based on file types (MS-office, pdf's, TXT files, XML, HTML, JPEG, Compressed file's etc.)	These points are applicable under discovery section. Remediation actions are not taken on user endpoints.	Treat this requirement under as technical specification of "Data Discovery"
53		Annexure- I: Technical Requirement	The solution must have the capability to do analysis (discovering sensitive data) along with host details.	These points are applicable under discovery section. Remediation actions are not taken on user endpoints.	Treat this requirement under as technical specification of "Data Discovery"
54		Annexure- I: Technical Requirement	The solution must have the capability to do analysis (discovering sensitive data) based on Current Classification Level and to suggest classification.	These points are applicable under discovery section. Remediation actions are not taken on user endpoints.	Treat this requirement under as technical specification of "Data Discovery"
55		Annexure- I: Technical Requirement	The solution must have the capability to do analysis (discovering sensitive data) along with the User Permission on the sensitive data.	These points are applicable under discovery section. Remediation actions are not taken on user endpoints.	Treat this requirement under as technical specification of "Data Discovery"
56		Annexure- I: Technical Requirement	The solution must have the capability to Delete the sensitive data as a Remediation action if required.	These points are applicable under discovery section. Remediation actions are not taken on user endpoints.	Treat this requirement under as technical specification of "Data Discovery"
57		Annexure- I: Technical Requirement	The solution must have the capability to move the sensitive data as a Remediation action if required.	These points are applicable under discovery section. Remediation actions are not taken on user endpoints.	Treat this requirement under as technical specification of "Data Discovery"
58		Annexure- I: Technical Requirement	The solution must have the capability to replace the sensitive data as a Remediation action if required.	These points are applicable under discovery section. Remediation actions are not taken on user endpoints.	Treat this requirement under as technical specification of "Data Discovery"
59		Annexure- I: Technical Requirement	The solution must have ability to connect to windows share drive and discover data sets	Scanning tool needs to cover various repositories of un-structured data Suggested Point: The solution should have the ability to scan Windows file shares, SharePoint, SharePoint Online, OneDrive, Dropbox, Box and enforce classification based on content, file attributes, file location	As per RFP, Bidder to propose the best practices in the RFP response

60		Annexure- I: Technical Requirement	The solution must have ability to identify and apply multiple business rules (e.g., GDPR PII rules)	Pls clarify business rules. Does this refer to protection	No
61		Annexure- I: Technical Requirement	The solution must have ability to find unique identities by a data subject's key attributes across all data sources	The solution should provide the ability to run scheduled scans to discovery, gather inventory of files and automatically classify files based on several factors, including the file properties/attributes, owner, content, and/or metadata.	As per RFP, Bidder to propose the best practices in the RFP response
62		Annexure- I: Technical Requirement	The solution must have ability to see all identifiers on a data subject by conducting a search using either a name or other key attributes	The solution should provide the ability to run scheduled scans to discovery, gather inventory of files and automatically classify files based on several factors, including the file properties/attributes, owner, content, and/or metadata.	As per RFP, Bidder to propose the best practices in the RFP response
63		Annexure- I: Technical Requirement	The solution must have ability to develop an inventory of discovered identities	The solution should provide the ability to run scheduled scans to discovery, gather inventory of files and automatically classify files based on several factors, including the file properties/attributes, owner, content, and/or metadata.	As per RFP, Bidder to propose the best practices in the RFP response
64		Annexure- I: Technical Requirement	The solution must have ability to identify what objects within a system contain personal information about a data subject before retrieving the data	The solution should provide the ability to run scheduled scans to discovery, gather inventory of files and automatically classify files based on several factors, including the file properties/attributes, owner, content, and/or metadata.	As per RFP, Bidder to propose the best practices in the RFP response
65		Annexure- I: Technical Requirement	The solution must have ability to control the amount of personal information retrieved in response to a data subject access request to manage volume of data	Not in scope of classification solution. Pls clarify controlling amount of personal data	The is not a core feature of Data Discovery and will be treated as Optional Specification
66		Annexure- I: Technical Requirement	Recognize data sources of systems, schemas, tables, data elements	Not in scope of classification solution. This probably refers to structured data like databases.	Requirement is under "Data Discovery" technical specification

67		Annexure- I: Technical Requirement	The solution must have ability to scan structured, semi-structured and unstructured data	Classification solutions are designed to identify and classify un-structured data. Structured data in databases need different set of controls like Anonymization and not classification.	Requirement is under "Data Discovery" technical specification. Will be treated as Optional Specification
68		Annexure- I: Technical Requirement	Search data sets by facets, keywords or business terms	Classification solutions are designed to identify and classify un-structured data. Structured data in databases need different set of controls like Anonymization and not classification.	Solution must support data search by facets, keywords OR business terms
69		Annexure- I: Technical Requirement	The solution must have ability to present data in masking format.	Masking is a irreversible process which is typically used to minimize data exposure on UAT, business analytics environment that too for structured data like databases. Redaction applies to unstructured data. Suggested Point: The solution should provide the ability to highlight sensitive information within an MS outlook email and redact the sensitive content so that users can remediate any policy violations before the email leaves the desktop.	As per RFP
70		Annexure- I: Technical Requirement	The solution must have ability to encrypt data elements of interest	Encryption is a separate technology and tools like IRM apply her which should not be in scope if IFTAS is just looking data identification and classification.	IRM/DRM deployment will be done in later phase and The Solution must integrate with the IRM/DRM
71		Annexure- I: Technical Requirement	The solution must have the capability to do analysis (discovering sensitive data) based on Current Classification Level and to suggest classification.	Suggestions are given to users while they are creating, saving, sending data and does not apply to data at rest in file servers	As per RFP, Bidder to propose the best practices in the RFP response

72		New Point	Suggestion to include new point in Technical Requirement	The solution should support automatic classification of files like reports generated from CRM, HRMS, tools when its downloaded and saved to on user endpoint folders like desktop, downloads, my documents. The classification should be based on file content, file type, file size, file name and combination of any of these parameters.	As per RFP, Bidder to propose the additional feature in the RFP response
73		New Point	Suggestion to include new point in Technical Requirement	The solution should support the ability to set the classification automatically based on a series of questions presented to the user via the classification dialog.	As per RFP, Bidder to propose the additional feature in the RFP response
74		New Point	Suggestion to include new point in Technical Requirement	The solution should support metadata remediation and prioritization when multiple sources of metadata are available on a file. For example, a user-applied classification may be most critical and trustworthy, while in other cases, a automatic classification tag is treated as a preferred value.	As per RFP, Bidder to propose the additional feature in the RFP response
75		New Point	Suggestion to include new point in Technical Requirement	The solution should support the ability to evaluate multiple email and document attributes to determine the appropriate markings.	As per RFP, Bidder to propose the additional feature in the RFP response
76		New Point	Suggestion to include new point in Technical Requirement	The solution should support the discovery and identification of large volumes of data, stored both on premise and in the cloud. This includes the scanning of network file shares, SharePoint (on premise and Online), as well as Cloud storage providers.	As per RFP, Bidder to propose the additional feature in the RFP response
77		New Point	Suggestion to include new point in Technical Requirement	The solution should provide the ability to warn users when opening sensitive MS Office documents natively.	As per RFP, Bidder to propose the additional feature in the RFP response

78		New Point	Suggestion to include new point in Technical Requirement	The solution should support the use of task panel alerts, which can be applied at all times or only under certain conditions. For example, the task panel can be configured to appear when handling an Excel spreadsheet containing PII (Personnel Identity Information) data.	As per RFP, Bidder to propose the additional feature in the RFP response
79		New Point	Suggestion to include new point in Technical Requirement	The solution should provide the ability to present the user with a checklist of blocked attachments when a policy violation occurs, and allows the user to manually select the attachments that are allowed to bypass the policy violation. For example, the user can be shown all "Confidential" attachments and asked to confirm individual attachments before sending the email.	As per RFP, Bidder to propose the additional feature in the RFP response
80		New Point	Suggestion to include new point in Technical Requirement	The solution should provide the ability to secure SharePoint content based on document metadata.	As per RFP, Bidder to propose the additional feature in the RFP response
81		New Point	Suggestion to include new point in Technical Requirement	The solution should support multiple classification types (i.e. dropdowns, multi-selects, date fields, and user type-in).	As per RFP, Bidder to propose the additional feature in the RFP response
82		New Point	Suggestion to include new point in Technical Requirement	The solution should support the mapping of old classification values to new ones, and seamlessly update previously classified information if required.	As per RFP, Bidder to propose the additional feature in the RFP response
83		New Point	Suggestion to include new point in Technical Requirement	The solution should enable users to assign classification values via a one click classification user interface.	As per RFP, Bidder to propose the additional feature in the RFP response
84		New Point	Suggestion to include new point in Technical Requirement	The solution should enable users to save type-in fields as Favourites so that the information needs to be typed in only once.	As per RFP, Bidder to propose the additional feature in the RFP response
85		New Point	Suggestion to include new point in Technical Requirement	The solution should provide the ability to prevent printing of sensitive email and Office documents based on classification to specific printers natively.	As per RFP, Bidder to propose the additional feature in the RFP response

86		New Point	Suggestion to include new point in Technical Requirement	The solution should provide advanced control over email attachments via policies that evaluate content, recipients, sender, classification, filename, file size, and other attributes.	As per RFP, Bidder to propose the additional feature in the RFP response
87		New Point	Suggestion to include new point in Technical Requirement	The solution should support the ability to restrict email based on sender. For example, one user may be authorized to send sensitive information externally, but others are not allowed to do this. The policy decision may be based on the sender's email, name, or AD attributes or group membership.	As per RFP, Bidder to propose the additional feature in the RFP response
88		New Point	Suggestion to include new point in Technical Requirement	The solution should provide the ability to present the user with a checklist of blocked recipients when a policy violation occurs, and allows the user to manually select the recipients that are allowed to bypass the policy violation. For example, the user can be shown all external recipients and asked to confirm individual recipients before sending the email.	As per RFP, Bidder to propose the additional feature in the RFP response
89		New Point	Suggestion to include new point in Technical Requirement	The solution should support policy combinations to enable more advanced use cases, such as checking whether a document is having regulatory data, and then blocking an unauthorized user from sending the document as an attachment.	As per RFP, Bidder to propose the additional feature in the RFP response
90		Annexure- I: Technical Requirement	The solution should have the capability to deploy, upgrade, uninstall the component without the use of any 3rd party software.	This option you require in the application which we provide?	Yes
91		Annexure- I: Technical Requirement	The solution should be able to send policy to further changes to the clients without any need or intervention of a 3rd party software	your requirement is to update remotely Client side features?	This is policy update
92		Annexure- I: Technical Requirement	The unavailability of a management component/ server in no way shall impact the functioning of a client	Require offline mode?	As per RFP

93		Annexure- I: Technical Requirement	The solution should work on MS Windows environment	solution should run on other OS? Like Linux / MAC / Ubuntu?	As per RFP
94		Annexure- I: Technical Requirement	The Solution should have capability to integrate with SIEM and can send logs	Which SIEM application you are looking for	Logrhythm
95		Annexure- I: Technical Requirement	The solution should support the ability to quarantine files stored inappropriately, flag files for follow-up, or act based on results of the scan. This may include quarantine, delete, encrypt through 3rd party encryption tools, etc	Want to understand 3rd party encryption tool? We need more clarity	Bidder have to provide the list of 3rd party solution which can be integrated with the proposed solution
96		Annexure- I: Technical Requirement	The solution must have the capability to do analysis (discovering sensitive data) along with host details	Need more clarity in requirement	Data Discovery shall provide Host detail where data are located
97		Annexure- I: Technical Requirement	Recognize data sources of systems, schemas, tables, data elements and The solution must have ability to scan structured, semi-structured and unstructured data	Which database schemas? MSSQL	Bidder have to provide the list of supported database