KCM GRC

2021 SIG Core and SIG Lite: Questions with N/A Answers

KnowBe4

2021 SIG Core and SIG Lite: Questions with N/A Answers

We have added the following two questionnaire templates to your Vendor Risk Management module: **2021 SIG Core** and **2021 SIG Lite**.

The KCM GRC system pre-defines the "correct" answer for each question in a questionnaire template. For some of the questions in the **2021 SIG Core** and **2021 SIG Lite** templates, the KCM GRC system has defined **N/A** as the correct answer. The questions with **N/A** answers are subjective to your third-party vendor's environment and these questions may or may not impact your organization's risk assessment for the third party. For the most part, this means that the questions with **N/A** answers are for informational purposes and they do not affect your organization's risk assessment.

If you send the **2021 SIG Core** or **2021 SIG Lite** questionnaire templates to your vendors and they select either **"Yes"** or **"No"** for the applicable questions, their response will be marked as "incorrect". Incorrect doesn't mean that the response is "wrong", but rather that the user didn't select **"N/A"** as their response.

When you're creating and reviewing these questionnaires, it may be helpful for you to refer to the **2021 SIG Core** and **2021 SIG Lite** tables below that outline the questions that the KCM system has defined **"N/A"** to be the "correct" answer. The tables include the category and subcategory where you will find the questions in your questionnaire template.

2021 SIG Core: Template Questions With "N/A" Answers

Question	Category	Subcategory
Is scoped data sent or received via physical media?	Physical Media Transmission	Physical Media Transmission
Is scoped data sent or received electronically?	Data Transmission	Data Transmission
Are scoped systems or data stored or transferred in cloud-based public file sharing solutions? If yes, please explain in the Additional Information field.	Data Transmission	Cloud File Sharing Access Controls
Is regulated or confidential scoped data stored electronically?	Encryption	Scoping
Is regulated or confidential scoped data stored in a database?	Encryption	Database Encryption
Is regulated or confidential scoped data stored in files?	Encryption	File/Folder Encryption
Is there a loading dock at the facility?	Loading Dock Controls	Secure Workspace Perimeter
Do other tenants use the data center?	Data Center Controls	Secure Workspace Perimeter
Are applications used to transmit, process or store scoped data?	Application Security	Scoping
Is application development performed?	SDLC	Scoping

2021 SIG Core: Template Questions With "N/A" Answers Cont.

Question	Category	Subcategory
Is a web site supported, hosted or maintained that has access to scoped systems and data?	Web Server Security	Scoping
Are Web Servers used for transmitting, processing or storing scoped data?	Web Server Security	Scoping
Are mobile applications that access scoped systems and data developed?	Mobile Application Security	Scoping
Will this engagement include any call center related services?	Call Center Controls	Governance
Is the call support team physically segregated from teams servicing other clients?	Call Center Controls	Personnel
Are marketing or selling activities conducted directly to Client's customers?	Consumer Protection	Marketing and Sales Practices
Are calls for telemarketing purposes recorded and retained? If yes, please provide the retention period in the additional information field.	Consumer Protection	Marketing and Sales Practices
Are collections activities conducted directly to Client's customers?	Consumer Protection	Collections Practices
Are calls for collections' purposes recorded and retained? If yes, please provide the retention period in the additional information field.	Consumer Protection	Collections Practices

2021 SIG Core: Template Questions With "N/A" Answers Cont.

Question	Category	Subcategory
Are there direct interactions with your client's customers?	Consumer Protection	Complaint Management
Are accounts opened, financial transactions initiated or other account maintenance activity (e.g., applying payments, address changes, receiving payments, transferring funds, etc.) through either electronic, telephonic, written or in-person requests made on behalf of your clients' customers?	Payments Compliance	Governance
Are electronic commerce web sites or applications used to transmit, process or store Scoped systems and data?	Payments Compliance	eCommerce Security
Do the services require receiving or processing credit or debit card data? If yes, indicate the PCI Level in the additional information field (Level 1, 2, 3 or 4).	Payments Compliance	Payment Card Processing
Are End User Devices (desktops, laptops, tablets, smartphones) used for transmitting, processing or storing Scoped data?	End User Device Security	Scoping
Are Baseboard Management Controllers (BMCs) enabled on any servers or other devices?	Remote System Access	Baseboard Management Controllers
For client scoped data, is personal information provided to the organization directly by the client?	Collection	Types of Personal Information Collection and Methods of Collection

2021 SIG Core: Template Questions With "N/A" Answers Cont.

Question	Category	Subcategory
If required, has the organization registered as a telemarketer under any state regulation? If yes, identify the stake and link to the registration in the Additional Information field.	State Privacy Regulations	Use of Personal Information
Has the organization self-certified to the EU-U.S. Privacy Shield Framework and/or Swiss-U.S. Privacy Shield Framework? If, yes, please provide a link to the publicly available filing.	Monitoring and Enforcement	Compliance Review
Do you deliver software, firmware, and/or BIOS updates to clients through automatic downloads (e.g., Windows Update, LiveUpdate)?	Vulnerability Management	Automatic Software Update Mechanisms
Are Servers used for transmitting, processing or storing scoped data?	Server Security Configuration Management	Governance
Is Unix or Linux used as part of the scoped services?	Unix/Linux Security	Scoping
Are AS/400s used as part of the scoped services?	AS/400 Security	Scoping
Are Mainframes used as part of the scoped services?	Mainframe Security	Scoping
Are Hypervisors used to manage systems used to transmit, process or store Scoped data?	Hypervisor and Virtualization Security	Hypervisor Security

2021 SIG Core: Template Questions With "N/A" Answers Cont.

Question	Category	Subcategory
Are Containers used to process or store Scoped data e.g., Docker, Kubernetes, OpenShift?	Container Security	Scoping
Are Cloud Hosting services (IaaS) provided?	Cloud Hosting	Cloud Service Model
Are Cloud Hosting services subcontracted?	Cloud Hosting Organization	Subcontracted Cloud Services

2021 SIG Lite: Template Questions With "N/A" Answers

Question	Category	Subcategory
Is scoped data sent or received via physical media?	Physical Media Transmission	Physical Media Transport Integrity
Is scoped data sent or received electronically?	Data Transmission	Data Transmission Security Policy
Is regulated or confidential scoped data stored electronically?	Encryption	Scoping
Are applications used to transmit, process or store scoped data?	Application Security	Scoping
Is application development performed?	SDLC	Scoping
Is a web site supported, hosted or maintained that has access to scoped systems and data?	Web Server Security	Scoping
Are mobile applications that access scoped systems and data developed?	Mobile Application Security	Scoping
Will this engagement include any call center related services?	Call Center Controls	Governance
Are marketing or selling activities conducted directly to Client's customers?	Consumer Protection	Marketing and Sales Practices
Are collections activities conducted directly to Client's customers?	Consumer Protection	Collections Practices

2021 SIG Lite: Template Questions With "N/A" Answers Cont.

Question	Category	Subcategory
Are there direct interactions with your client's customers?	Consumer Protection	Complaint Management
Are accounts opened, financial transactions initiated or other account maintenance activity (e.g., applying payments, address changes, receiving payments, transferring funds, etc.) through either electronic, telephonic, written or in-person requests made on behalf of your clients' customers?	Payments Compliance	Governance
Are End User Devices (desktops, laptops, tablets, smartphones) used for transmitting, processing or storing Scoped data?	End User Device Security	Scoping
Are Baseboard Management Controllers (BMCs) enabled on any servers or other devices?	Remote System Access	Baseboard Management Controllers
For client scoped data, is personal information provided to the organization directly by the client?	Collection	Types of Personal Information Collection and Methods of Collection
If required, has the organization registered as a telemarketer under any state regulation? If yes, identify the stake and link to the registration in the Additional Information field.	State Privacy Regulations	Use of Personal Information
Do you deliver software, firmware, and/or BIOS updates to clients through automatic downloads (e.g., Windows Update, LiveUpdate)?	Vulnerability Management	Automatic Software Update Mechanisms

2021 SIG Lite: Template Questions With "N/A" Answers Cont.

Question	Category	Subcategory
Is Unix or Linux used as part of the scoped services?	Unix/Linux Security	Scoping
Are AS/400s used as part of the scoped services?	AS/400 Security	Scoping
Are Mainframes used as part of the scoped services?	Mainframe Security	Scoping
Are Hypervisors used to manage systems used to transmit, process or store Scoped data?	Hypervisor and Virtualization Security	Hypervisor Security
Are Cloud Hosting services (IaaS) provided?	Cloud Hosting	Cloud Service Model
Are Cloud Hosting services subcontracted?	Cloud Hosting Organization	Subcontracted Cloud Services

KCM GRC

2021 SIG Core and SIG Lite: Questions with N/A Answers

KnowBe4