50 MOST IMPORTANT DISASTER RECOVERY SOFTWARE QUESTIONS

Neighborly Software

TABLE OF CONTENTS

USER EXPERIENCE 4

KEY FEATURES 6

COMMUNICATIONS 9

BUDGETS, DRAWS AND PAYMENTS 11

FRAUD DETECTION 13

COMPLIANCE 15

DATA ACCESS AND REPORTING 17

SYSTEM ARCHITECTURE AND SECURITY 19

SOFTWARE SUPPORT & SERVICES 22

Howdy neighbor!

It’s great that you’re taking the time to carefully consider the software solution for your Disaster Recovery (DR) program. It’s crucial to have the right system of record in place to ensure the success and sustainability of your efforts. You’re right—there’s a lot to think about, and making the wrong decision could impact your program’s efficiency and effectiveness.

Don’t worry! While the world of software solutions might feel overwhelming, asking the right questions is the key to making a confident decision. In this guide, we’ve gathered the top 50 questions that will help you navigate through the process. Whether you’re evaluating must-have functionalities like financial system integration or advanced features like automated DRGR reporting, these questions are designed to give you a comprehensive understanding of what a DR software system of record can offer.

By becoming familiar with these questions and their underlying importance, you’ll have a solid foundation choosing the right partner. And remember, we’re always here to help if you need expert advice from our CDBG-DR team—just a click away!

USER EXPERIENCE

1. Is the software modern and intuitive to use?

The online experience often serves as the face of a disaster recovery program, shaping how people perceive its quality, accessibility, and overall effectiveness. A modern, intuitive software solution ensures that users, whether applicants, administrators, subrecipients and contractors, can easily navigate the system without extensive training. A well-designed, user-friendly interface enhances accessibility, reducing the likelihood of errors and inefficiencies. This is especially important for disaster recovery programs, where timely and accurate processing is essential.

2. Does the solution provide access in languages spoken by your constituents?

Providing access to a government software solution in constituent languages is essential for fostering inclusivity, ensuring equal opportunities, and promoting effective communication.
This approach empowers citizens to engage with your organization, regardless of their language proficiency, and removes barriers to participation.

3. Is the system 508 Compliant and are they willing to provide their most recent VPAT?

A system that is 508 compliant helps organizations meet legal accessibility requirements and avoid potential penalties. Additionally, the provider should be willing to provide their most recent Voluntary Product Accessibility Template (VPAT), which outlines the system's compliance status. This demonstrates the organization's ethical commitment to inclusivity and reflects a responsible approach toward accessibility and security.

4. Is the software mobile friendly?

The system must be fully mobile-responsive, ensuring a seamless experience for applicants using phones or tablets. This is especially important, as many survivor applications will be submitted through mobile devices. One key feature is the ability for applicants to upload required documentation directly from their smartphone camera, eliminating the need for a scanner. This functionality significantly enhances the efficiency of the application process while improving accessibility for individuals who may not have access to traditional desktop resources.

5. Is the software application a comprehensive Disaster Recovery System of Record?

A comprehensive Disaster Recovery System of Record consolidates all essential functions into a single platform, avoiding the complexity of multiple systems and manual workarounds. It must support diverse programs—Public Infrastructure, Housing Rehab, Rental Assistance, Home Buyout, and Economic Assistance—and include key features like construction management and loan administration. A unified solution improves efficiency, reduces errors, and provides a complete view for faster, more effective decision-making.

KEY FEATURES

6. Does the system provide reviewer checklists based on best practices?

Reviewer checklists based on best practices are crucial for maintaining consistency, fairness, and transparency in the evaluation/underwriting process. These checklists provide standardized guidelines, ensuring that reviewers assess grant applications according to established criteria and benchmarks. This leads to more objective, informed decision-making and helps streamline the review process, ensuring that all applications are evaluated fairly and efficiently.

7. Does the system render documents based on templates?

The system should include a document rendering engine that allows users to generate custom documents directly from the platform, without the need for external software or technical expertise. By using stored data, the system can automatically merge fields into templates, enabling users to easily create documents such as grant award letters, project status reports, financial statements, compliance reports, and impact assessments. This streamlines document generation, saving time and improving efficiency while ensuring accuracy and consistency across all generated documents.

8. Does the solution have FEMA and SBA duplication of benefits validation?

The system should have the capability to validate duplication of benefits by identifying prior FEMA and SBA payments. This ensures that applicants do not receive funding for the same expenses from multiple sources. By adjusting award amount calculations based on this validation, the system helps maintain compliance and prevents overpayment. It is also essential that the system can refresh FEMA and SBA data regularly to ensure that the most up-to-date information is used for duplication of benefits calculations. This feature safeguards the integrity of the funding process and helps protect against fraudulent or incorrect claims.

9. Does the system originate and track deferred, forgivable and amortizing loans?

The ability to track both grants and loans, including deferred, forgivable, and amortizing loans, in a single system is crucial for efficiency and accuracy. Managing both types of financial assistance within one system eliminates the need for separate systems and the associated reconciliation efforts, reducing administrative burden and the risk of errors. This unified approach ensures that both loans and grants are accurately reflected and tracked, providing a clear and comprehensive view of all financial assistance provided to applicants.

10. Does the system enable inspectors to complete inspections and work write-ups in the field, including access to a specification library for consistent project scoping and contractor bidding?

It is essential for inspectors to conduct and record inspections while in the field, allowing for immediate documentation of findings and recommendations. Additionally, the system should include a standardized specification library for work write-ups, ensuring consistency across projects and providing clear, detailed scopes of work. This consistency is critical for creating project bids that contractors can accurately and fairly respond to. By capturing inspection results, generating work write-ups, and facilitating bidding within the same platform, the system reduces administrative complexity, improves transparency, and speeds up the process from inspection to contractor selection and project completion.

11. Does the solution allow contractors to register, update documents, bid on projects, and request funding draws?

Providing contractors with direct access to the system streamlines communication and simplifies contractor management. Contractors should be able to upload insurance and license documents, submit construction bids, and request draws, all within a centralized platform. This improves efficiency, enhances collaboration, and helps ensure better outcomes in quality, cost control, and timely project completion.

12. Does the system allow applicants to submit online appeals, and are those appeals tracked within the system for compliance purposes?

Allowing applicants to submit online appeals is essential for regulatory compliance and ensures fairness and transparency in the disaster recovery process. An integrated appeals process provides applicants with a structured and accessible way to contest decisions, meeting compliance requirements while minimizing administrative burden. Ideally, the system should capture all appeal-related actions, communications, and documentation in the System of Record. This ensures a complete audit trail for reporting, reduces the risk of missed or mishandled appeals, and helps agencies respond efficiently while maintaining accountability and adherence to program guidelines.

COMMUNICATIONS

13. Does the system include SMS messaging?

SMS messaging provides a convenient and efficient communication channel for quick and direct interaction with grant applicants, subrecipients, and contractors. SMS texting ensures broader accessibility as it doesn’t require internet access or a smartphone, making it an inclusive option for individuals with limited access to technology. This feature enhances communication and ensures that important notifications, updates, or reminders can reach users in a timely and accessible manner.

14. Does the system include configurable email templates that can be sent in the stakeholders preferred language?

Configurable email templates in stakeholders’ preferred languages ensure accessibility, improve efficiency by automating communication, and maintain consistent messaging. This promotes inclusivity, reduces errors, and builds trust, especially in diverse programs with varied stakeholders.

15. Does the system integrate with Power BI to publish constituent-facing dashboards?

The ability to share progress with the public is essential for transparency and accountability. By integrating with tools like Power BI, the system should produce interactive dashboards that highlight key disaster recovery metrics and milestones. These dashboards allow stakeholders to explore program progress, filter data, and visualize achievements in a clear and engaging format, showcasing the impact of government efforts and building public trust.

BUDGETS, DRAWS AND PAYMENTS

16. Does the system allow for the tracking of budgeted, encumbered and disbursed funds?

The ability to track budgeted, encumbered, and disbursed funds is critical for effective budget management and compliance with funding requirements. This feature enables grant managers to monitor fund allocation and utilization, ensuring spending aligns with the approved budget and grant guidelines. It also helps identify discrepancies or potential overspending early, allowing for proactive measures to mitigate risks, maintain financial accountability, and ensure timely spending.

17. Does the system have adequate controls to ensure separation of duties when creating and approving budgets and payments?

The system should have robust controls in place to ensure separation of duties when creating and approving payments. This is crucial for maintaining integrity and reducing the risk of fraud or errors. A well-designed system enforces this separation by restricting permissions, ensuring that no single individual has the authority to both create and approve payments. Built-in system controls, such as role-based access and approval workflows, prevent conflicts of interest. Additionally, audit logging should track every action, providing a detailed history of who initiated and approved payments. This level of oversight not only ensures compliance with financial policies but also strengthens accountability and transparency, safeguarding the payment process from potential abuse.

18. Does the system support multiple draw approval processes?

Automatic routing for the draw approval process is essential for ensuring timely disbursement of funds, especially in disaster recovery scenarios where speed is critical. This functionality streamlines the approval workflow, reducing administrative burden and minimizing delays in processing payments. By automating approvals, the system enhances efficiency, ensuring that survivors, contractors, and other stakeholders receive financial assistance as quickly as possible, supporting recovery efforts and providing essential aid when it is most needed.

19. What options does the system have to support payments?

Different jurisdictions have different needs for payment support. Do you want a fully integrated payment solution (ACH, Check, reloadable debit card)? Do you need a NACHA file? Do you need a payment file for import into a third-party financial system? It's important to choose a provider that can meet your specific payment requirements, ensuring seamless and efficient financial transactions for your organization.

20. Does the system validate check payment addresses and ACH numbers prior to payment?

The system should validate check payment addresses and ACH numbers prior to payment to prevent costly errors. Validating addresses against the USPS database ensures that checks are sent to the correct destination and arrive on time. Similarly, validating ACH numbers helps avoid complications like payment recapture and additional due diligence, reducing the workload for staff and streamlining payment processing.

21. Does the system have functionality supporting accounting/finance functions such as payment batching, invoicing and reconciliation?

The back end of the payment process is often overlooked, but a system that handles these critical functions—batching, submission, and reconciliation—can drastically reduce manual efforts and minimize the need for emailing spreadsheets. This not only cuts down on errors and inefficiencies but also alleviates frustration for both users and finance teams, streamlining the entire payment process and ensuring better financial oversight.

FRAUD DETECTION

22. Does the system identify and flag duplicate applications?

The system should identify, and flag duplicate applications based on phone numbers, SSNs, and email addresses. This functionality helps maintain data integrity, prevents fraudulent activities, and safeguards the organization against potential financial losses by ensuring that each application is unique and legitimate.

23. Can the system track application completion time and flag unusually fast submissions?

The time it takes to complete an application can be a strong indicator of fraudulent activity. The system can track and flag applications that are submitted unusually quickly, as this may signal suspicious behavior. By monitoring the completion speed and identifying applications that deviate from typical processing times, the system helps detect potential fraud and enhances overall security, ensuring a more reliable and protected process.

24. Does the solution identify and track IP addresses?

This feature is crucial for detecting and preventing unauthorized access or suspicious behavior. By monitoring IP addresses, the system can enhance security, flag unusual activities, and help protect both the system and its users from potential threats or fraud.

25. Does the system refuse IPs outside the United States?

The ability to identify and block IP addresses outside the United States, enhances security by preventing unauthorized access from foreign sources. Additionally, the system should be able to whitelist specific IP addresses, allowing trusted users or systems from outside the U.S. to gain access as needed. This flexibility ensures that access remains secure while accommodating legitimate, authorized use.

26. Does the system flag suspicious documents that have been altered by 3rd party software?

The system must be able to flag suspicious documents that may have been altered or manipulated, such as those modified in third-party solutions like Adobe Photoshop. By checking the meta-data of uploaded documents, the system can identify signs of tampering or changes made outside the original source. This feature is essential for detecting fraudulent claims, as altered documents are a common indicator of suspicious activity and ensures the integrity of submitted materials.

COMPLIANCE

27. Does the system include a full audit log of activities and data field changes?

An audit log provides a clear record of all actions and modifications made within the system, detailing who performed each task and when. This is essential for maintaining data integrity, detecting unauthorized or suspicious activities, and facilitating accurate reporting and auditing processes. It also serves as a valuable tool for organizations to track user interactions and ensure the security and accuracy of their data.

28. Does the system allow for configurable roles and permissions?

The system must support both role-based and user-based permissions to ensure access is granted based on least privilege and need-to-know principles. Role-based permissions define access levels for specific job functions, while user-based permissions allow customization for individual users. This segmentation enhances workflow management, accountability, and collaboration, while also reducing the risk of unauthorized data manipulation or leakage by restricting access to sensitive information.

29. Does the system include monitoring reports for contractors and subrecipients?

Managing large sums of disaster recovery (DR) funding requires robust compliance reporting to ensure transparency, accountability, and adherence to regulatory requirements. The system should provide tools to generate and manage a wide range of compliance reports, such as Davis-Bacon wage compliance, financial control audits, Section 3 reporting, and accomplishment reporting. A comprehensive monitoring solution should create a schedule of required reports, track report completion, and enable users to submit, review, and share reports directly within the system. It should also support both desktop and onsite audits, capturing real-time data and documentation to ensure accurate reporting and audit preparedness.Centralizing compliance monitoring within a single system not only reduces administrative burden but also improves oversight, mitigates risks, and ensures faster, more efficient responses during audits. This all-in-one approach strengthens overall program integrity and facilitates seamless collaboration with contractors, subrecipients, and regulatory bodies.

DATA ACCESS AND REPORTING

30. How "real time" is the data available through the system for external reporting to key stakeholders and constituents?

Access to real-time data is critical for effective decision-making and timely reporting. Disaster recovery programs move quickly, and stakeholders need up-to-date information to monitor progress, assess performance, and address potential issues as they arise. A platform that provides real-time data ensures that dashboards and visualizations reflect the most current program status, allowing for transparent communication with the public and key stakeholders.

31. Does the system create reports for upload into DRGR?

The system should generate reports in formats compatible with HUD's Disaster Recovery Grant Reporting (DRGR) system, particularly by producing Excel files that can be directly uploaded. This capability ensures a seamless integration between your reporting processes and DRGR, enabling efficient submission of performance accomplishments and financial data related to grant-funded activities. Being able to automate this reporting step reduces manual effort, minimizes the risk of errors, and ensures that all required data is accurately and timely submitted. This integration is essential for maintaining compliance with HUD reporting requirements and supports transparent tracking of grant progress, helping to keep stakeholders informed and improving overall grant management.

32. Are you provided with a Data Dictionary for all relevant data tables?

A Data Dictionary is essential for ensuring that your data team can quickly and accurately understand the structure of the system's data. It provides clear definitions for all relevant data tables and fields, helping your team navigate the datasets efficiently. By offering a comprehensive guide to data relationships, naming conventions, and field descriptions, a Data Dictionary enhances data accuracy and integrity. It also supports seamless data extraction, integration, and reporting, ensuring that everyone is on the same page regarding the meaning and use of the data. This transparency is crucial for data-driven decision-making, maintaining consistency across teams, and minimizing confusion or errors when handling data.

SYSTEM ARCHITECTURE AND SECURITY

33. Is the system cloud based?

A cloud-based solution eliminates the need for maintaining or securing software on local servers or end-user computers. A fully cloud-based solution ensures access to the latest security protocols, modern access controls, and seamless updates, reducing IT overhead and enhancing system reliability.

34. Is the solution hosted in a FedRAMP certified data center?

A FedRAMP data center ensures that the hosting environment meets stringent federal security standards and complies with government regulations. It signifies that the data center has undergone thorough security assessments and has implemented robust security controls, providing a high level of protection for sensitive data.

35. Does the solution provide geo-redundancy?

Geo-redundancy is critical for ensuring high availability and minimizing downtime. By maintaining data in geographically dispersed locations, the solution protects against localized outages, natural disasters, and other disruptions. This approach enhances business continuity, data resilience, and reliable access to services, ensuring uninterrupted operations and compliance with disaster recovery best practices.

36. Does the solution have point in time restore?

Having the ability to perform point-in-time restores within a specified window, such as the last month, is essential for ensuring data integrity and security. This capability allows users to recover from data loss, system errors, or any unintended modifications by reverting the system to a known, stable state. In the event of accidental data deletion, corruption, or errors during processing, point-in-time restore provides a safety net to minimize disruption and maintain operational continuity. It is also a critical feature for compliance purposes, as it ensures that historical data can be accurately restored and audited, meeting regulatory requirements for data retention and reporting.

37. Does the system have two-factor authentication?

Two-factor authentication (2FA) is a crucial security measure that significantly reduces the risk of unauthorized access. By requiring an additional verification step beyond a password, it provides an extra layer of protection against phishing, credential theft, and other cyberattacks. This ensures that only authorized users can access the system, helping safeguard sensitive data and maintain the integrity of user accounts.

38. Does the database logically isolate client data?

Logical isolation of client data is crucial for ensuring data privacy, security, and system stability. It prevents unauthorized access by separating client data within the database, significantly reducing the risk of data breaches. This separation also facilitates efficient management, allowing for easier backups, migrations, and rollbacks without impacting other clients. By enhancing scalability and data integrity, logical isolation ensures the software remains reliable while safeguarding the confidentiality and integrity of each client’s data.

39. Is all the data encrypted at rest and in transit?

Encrypting data at rest and in transit ensures that sensitive information is protected by rendering it unreadable to unauthorized parties without the proper decryption key. This provides a strong layer of security, safeguarding personal and proprietary business data, even in the event of physical device theft, database breaches, or network interception. It helps organizations comply with security standards and reduces the risk of data exposure.

40. Does the system time out after inactivity?

A configurable system timeout after periods of inactivity is an essential security measure to prevent unauthorized access. It reduces the risk of sensitive information being exposed if a user leaves their session unattended, ensuring that the system remains secure and compliant with security best practices.

41. Does the system integrate with 3rd party systems?

The system should feature a modern architecture that supports seamless connections to third-party systems via API integrations and flat file uploads. This enables real-time data synchronization, reducing manual effort and minimizing the risk of errors, while improving overall efficiency. API integration ensures that the system can adapt to evolving needs, enabling better collaboration across platforms.Key use cases for API integration include Single Sign-On (SSO) to simplify user access and enhance security, financial system integration to automate transactions and financial reporting, and USPS database integration to validate addresses and ensure accurate mailings. These integrations ensure data consistency, streamline workflows, and increase scalability, making the system more effective and adaptable to future demands.

SOFTWARE SUPPORT & SERVICES

42. Is the vendor Soc 2 Type 2 certified?

SOC 2 Type 2 certification ensures a vendor has implemented and consistently maintains robust controls for security, availability, processing integrity, confidentiality, and privacy. It verifies that these controls have been tested over time, providing assurance that sensitive data is protected, systems are reliable, and processes meet industry best practices. This certification reduces risk, enhances regulatory compliance, and builds trust by demonstrating the vendor's commitment to safeguarding data and ensuring operational integrity.

43. Is the solution delivered by a vendor who builds software as their core competency?

It's important to choose a solution delivered by a software company that specializes in building software, rather than a service provider. Service providers often focus more on the service component, with less emphasis on the software itself, which can result in suboptimal solutions for specialized programs like CDBG-DR. By separating services from software, you ensure access to a best-of-breed, optimized solution specifically designed for CDBG-DR programs, providing greater efficiency, flexibility, and scalability for grantees. Additionally, choosing a separate software vendor ensures you're not tied to the same service provider for future disasters, allowing the software to grow with your needs and adapt to changing requirements.

44. Was the solution specifically built for state and local governments?

State and local governments have unique requirements, processes, and regulations that are specific to their jurisdictions. A software solution built for state and local governments can offer tailored functionality that addresses these specific needs. Generic platforms will need to be customized at a heavy cost, in terms of dollars, time and staffing in order provide the necessary functionality.

45. Does the provider regularly update the software and are they willing to share features added in the last three years to show ongoing improvement?

It's important to ensure that the software solution remains up to date with evolving requirements and continues to improve over time. A provider who regularly adds new features demonstrates a commitment to innovation and adapting to user needs. Requesting a list of features added in the past few years gives insight into their development history and helps assess how actively the solution is evolving to meet the needs of its users.

46. Does the provider have a software roadmap that they are willing to share with you?

A clear product roadmap ensures that the solution is continuously developed and enhanced to meet the evolving needs of your programs, incorporating new features, addressing emerging challenges, and staying aligned with industry trends. This transparency provides confidence that the solution will remain effective and adaptable over time.

47. Who is responsible for system maintenance and enhancements?

Customized software is not only expensive to build, but it also requires significant subject matter expertise from the client to determine "what to build." Furthermore, maintenance and support of customized code are often the responsibility of the client and/or expensive third-party support contracts. Custom builds also require an ongoing investment in time and resources to keep them up-to-date and functional. Without regular maintenance, these custom solutions can quickly become obsolete, leading to increased costs and inefficiencies. By contrast, adopting a standardized, regularly updated platform ensures that maintenance and enhancements are handled by the software provider, keeping the system current and minimizing the need for constant reinvestment.

48. Does the solution provider include a dedicated Client Success Manager to handle all your requests?

Having a dedicated Client Success Manager (CSM) post-sale is essential for ongoing support and success. Implementing a new solution involves more than just the initial setup; you need ongoing assistance as your needs evolve. A CSM provides a personalized point of contact who understands the intricacies of your account and is available to address any questions, training need, or configuration requests. This ensures smooth operations, quick resolution of issues, and continuous alignment of the solution with your evolving requirements, enhancing your overall experience and success with the software.

49. Does the solution provider provide training for the system whenever required throughout the contract for not just internal administrators but for applicants, contractors, and subrecipients?

Training at the initial implementation stage is important, but ongoing support is equally critical. Your provider should offer training on demand whenever you need it, ensuring that your team stays up to date with any new features or updates. It's essential that training is accessible to all stakeholders involved (e.g. administrators, applicants, contractors, subrecipients, etc.). This ensures that everyone using the system is well-equipped to maximize its value, leading to better outcomes and continued efficiency across the organization.

50. Is technical support based in the United States and available from 8am to 8pm EST?

Tier I and Tier II technical support should be based in the United States and available from 8am to 8pm EST, ensuring that you and all third-party stakeholders, such as contractors, applicants, and subrecipients, can get the help you need during your normal operating hours. Timely access to support is crucial for addressing issues that may arise.

Neighborly Software

neighborlysoftware.com

Speak to one of our experts