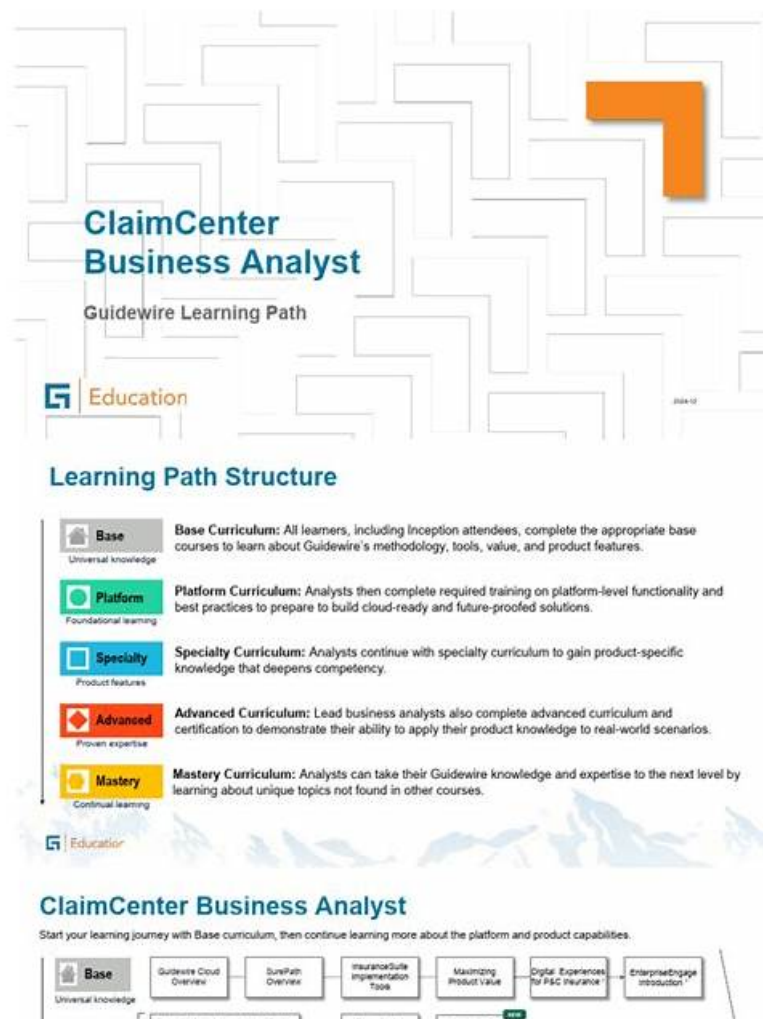


ClaimCenter-Business-Analysts試験準備資料、 ClaimCenter-Business-Analysts試験出題傾向、 ClaimCenter-Business-Analysts試験練習問題



さらに、Pass4Test ClaimCenter-Business-Analystsダンプの一部が現在無料で提供されています：
<https://drive.google.com/open?id=1uEllbPnUJOZUXgZI51rXTWFCzg4pml2>

弊社のClaimCenter-Business-Analysts問題集は大勢の専門家たちの努力で開発される成果です。初心者といい、数年IT仕事を従事した人といい、我々Pass4TestのGuidewire ClaimCenter-Business-Analysts問題集は最良の選択であると考えられます。なぜならば、弊社は高品質かつ改革によってすぐに更新できるClaimCenter-Business-Analysts問題集を提供できるからです。

Guidewire ClaimCenter-Business-Analysts 認定試験の出題範囲：

トピック	出題範囲
トピック 1	<ul style="list-style-type: none"> Guidewire における動作駆動開発: このセクションでは、共同開発アプローチと、BDD 原則を使用した明確でテスト可能な要件の記述に焦点を当て、BDD 方法論と Guidewire 実装でのその適用について説明します。
トピック 2	<ul style="list-style-type: none"> 品質アナリストの基礎: このドメインでは、開発全体を通じての品質の推進、開始時からの品質の統合、リスクの評価と軽減、テスト戦略の選択、および欠陥管理プロセスを含む品質保証の基礎をカバーします。

トピック 3	<ul style="list-style-type: none"> ClaimCenter のデータ モデルと判定: このドメインでは、ClaimCenter のデータ モデル アーキテクチャ、請求の設定、判定プロセス、財務用語と概念、および支払い作成手順について説明します。
トピック 4	<ul style="list-style-type: none"> InsuranceSuite アナリストの基礎: このドメインでは、ユーザー インターフェイス、データ モデル、アプリケーション ロジック、統合メカニズム、実際のアプリケーションのための実践的なワークショップ演習など、InsuranceSuite プラットフォームの基礎をカバーします。
トピック 5	<ul style="list-style-type: none"> クレーム センターの財務トランザクション: このセクションでは、支払いの承認と保留、連絡先とベンダーの管理、サービス リクエストの処理、権限とアクセス制御リストを使用したセキュリティ フレームワークなどの財務管理について説明します。

>> ClaimCenter-Business-Analysts資格講座 <<

ClaimCenter-Business-Analysts関連資料 & ClaimCenter-Business-Analysts 受験資格

今の社会はますます激しく変化しているから、私たちはいつまでも危機意識を強化します。キャンパス内の IT 知識を学ぶ学生なり、IT 職人なり、ClaimCenter-Business-Analysts 試験資格認証証明書を取得して、社会需要に応じて自分の能力を高めます。我々社は最高の Guidewire ClaimCenter-Business-Analysts 試験問題集を開発し提供して、一番なサービスを与えて努力しています。業界で有名な Guidewire ClaimCenter-Business-Analysts 問題集販売会社として、購入意向があると、我々の商品を選んでくださいませんか。

Guidewire ClaimCenter Business Analyst - Mammoth Proctored Exam 認定 ClaimCenter-Business-Analysts 試験問題 (Q26-Q31):

質問 # 26

Which set of three objects is required to create a liability exposure?

- A. Claimant, Coverage (type and subtype), Reserve Line
- B. Claimant, Incident, Reserve Line
- C. Coverage (type and subtype), Incident, Reserve Line
- **D. Claimant, Coverage (type and subtype), Incident**

正解: D

解説:

In the Guidewire ClaimCenter object model, a Liability Exposure represents a specific potential financial obligation to a third party. To successfully instantiate (create) a new exposure record, the system requires three fundamental data associations to define "Who, What, and How":

* **Claimant:** The specific person or entity seeking compensation (the "Who"). Every exposure must be linked to a contact designated as the claimant.

* **Coverage (Type and Subtype):** The specific contractual provision from the policy that applies to the loss (the "How"). The exposure must link back to a valid coverage on the verified policy to confirm the insurer is liable.

* **Incident:** The specific details of the event or damage (the "What"). In ClaimCenter, an Incident is a distinct object (e.g., Vehicle Incident, Injury Incident) that captures the facts of the loss. Multiple exposures can link to the same incident (e.g., Bodily Injury and Property Damage exposures both linking to the same Vehicle Incident), but every exposure requires one underlying incident to define the scope of the damage.

Why other options are incorrect:

* **Reserve Line (A, C, D):** A Reserve Line is a financial accounting object created after the exposure exists to set aside funds. It is a child object of the exposure, not a prerequisite for creating the exposure itself.

質問 # 27

To help manage new user setup, Succeed Insurance would like all manager-level employees to be able to add new users to

ClaimCenter. Some managers are already assigned the Community Admin role, which has a set of permissions for the administration of the ClaimCenter community model that includes the permission to create new users.

Where are two places the Business Analyst (BA) can go to view the permissions assigned to manager-level users? (Choose two.)

- A. Go to c:\GW10\ClaimCenter\build\dictionary\security\index.html to view the Security Dictionary
- B. Go to c:\GW10\ClaimCenter\build\dictionary\data\index.html to view the Data Dictionary
- C. Go to the Administration menu > Users & Security > Users
- D. Go to the Administration menu > Users & Security > Authority Limits
- E. Go to the Administration menu > Users & Security > Roles

正解: A、E

解説:

To view the detailed System Permissions (such as usercreate, claimview, etc.) associated with a specific user role (like "Manager" or "Community Admin"), a Business Analyst has two primary methods: one within the application UI and one via generated documentation.

* Administration Menu > Users & Security > Roles (Option E): This is the direct User Interface method. By navigating to the Roles page in the Administration tab, the BA can select a specific role (e.g., "Manager").

The detailed view of that role lists every system permission currently granted to it. This allows the BA to verify if the "usercreate" permission is present.

* Security Dictionary (Option B): For a comprehensive, searchable, and offline reference, the BA can access the Security Dictionary. This is a set of HTML files generated from the application's configuration (found in the build directory). It provides a complete matrix of all Roles, the Permissions assigned to them, and the Access Profiles configured in the system.

Why other options are incorrect:

* Data Dictionary (A): This documents the Data Model (Entities and Typelists), not the security configuration.

* Users (C): While this screen lists users and their assigned roles, it does not display the definitions (the specific list of permissions) of those roles.

* Authority Limits (D): This screen manages Financial limits (dollar amounts for reserves/payments), not system access permissions.

質問 # 28

Succeed Insurance had an embarrassing event last month that had potential legal ramifications. One of their Customer Service Representatives (CSR) shared details of a celebrity's personal auto claim on social media.

Fortunately for Succeed, the celebrity decided not to pursue legal actions as long as Succeed agreed to resolve the potential for future occurrences within the next 30 days.

Succeed executives immediately reacted to the situation by establishing new guidelines regarding claim security. The Business Analyst (BA) assigned to the project researched ClaimCenter base product capabilities and held several requirements gathering sessions designed to document their strategy. The new requirements indicate that only authorized users should be looking at celebrity claims.

Which two features should be used to meet the new requirements? (Choose two.)

- A. Create a rule that tracks who has viewed secure claims
- B. Hide secure claim information fields
- C. Create an access profile for each claim security level
- D. Assign authority profiles to authorized users
- E. Specify the claim security types

正解: C、E

解説:

To restrict access to sensitive claims (such as those involving celebrities) so that "only authorized users" can view them, a Business Analyst must utilize the Claim Security features in Guidewire.

* Specify Claim Security Types (Option A): The first step is to define the classification of the claim.

The system uses the ClaimSecurityType typelist. The BA would add a new typekey (e.g., "Celebrity" or "High Profile") or use an existing one (e.g., "Sensitive") to flag these specific claims.

* Create/Assign Access Profiles (Option E): Access control in Guidewire is managed through Access Profiles (sometimes referred to within Role configurations). An Access Profile maps specific Security Levels (like the "Celebrity" type defined above) to permissions. To meet the requirement, the BA defines an Access Profile that grants "View" permission for the "Celebrity" security type and assigns this profile only to the authorized users (or roles). Users without this specific Access Profile will be unable to search for or view the claim.

Why other options are incorrect:

- * Authority Profiles (B): In Guidewire terminology, "Authority" refers strictly to Financial Authority (limits on reserves and payments), not data access visibility.
- * Hide secure fields (C): This refers to Field Level Security (masking specific data like a Tax ID). The requirement is to restrict access to the entire claim, not just specific fields.
- * Tracking rules (D): While "Claim Access Auditing" (tracking history) is often enabled for sensitive claims, it is a detective control, not a preventive one. The requirement specifies that unauthorized users should not be looking at the claim at all, which requires the Access Profiles (preventive control).

質問 # 29

Succeed Insurance requires that all vehicles involved in collisions be evaluated to determine if the vehicle is a total loss. A vehicle claim is deemed a total loss using a calculation based on points earned for selecting specific vehicle information.

What are two examples of acceptance criteria for this business requirement? (Choose two.)

- A. Create a business rule to calculate total loss points.
- **B. Ensure that the business rule generates the Review for Salvage Activity.**
- C. Add a question to the Total Loss Calculator that identifies the relevant damage.
- **D. Validate the assignment to the Salvage Group when calculated points are 25 or greater.**

正解: B、D

解説:

Acceptance Criteria (AC) are specific conditions that the software must satisfy to be accepted by the user. In the context of a User Story, AC must be written as testable outcomes or verification steps (pass/fail conditions), not as implementation tasks for the developer.

* Option D (Testable Outcome): "Validate the assignment to the Salvage Group when calculated points are 25 or greater." This is a perfect example of AC. It describes a specific scenario (Points \geq 25) and the expected system behavior (Assign to Salvage Group). A tester can run this scenario and objectively determine if the system passes or fails.

* Option A (Testable Outcome): "Ensure that the business rule generates the Review for Salvage Activity." Similarly, this describes the expected result of the logic. It does not tell the developer how to write the code, but it tells the QA team what to look for (the creation of a specific Activity) to confirm the requirement is met.

Why other options are incorrect:

* Option B ("Add a question..."): This is an Implementation Task. It describes work the developer must do ("Add a question"), but it is not a criterion for verifying the end-to-end business value.

* Option C ("Create a business rule..."): This is also an Implementation Task. A user cannot "test" that a rule was created; they test the effect of that rule (which is described in A and D). Acceptance criteria focus on the "What" (behavior), while tasks focus on the "How" (configuration).

Here are the 100% verified answers for Question 16 and Question 17, formatted as requested.

質問 # 30

An Adjuster at Succeed Insurance increases the reserve on a claim's exposure from \$1,000 to \$1,500 to account for inflation in repair costs. A week later, a Supervisor reviews the claim and wants to know specifically who made this change, the exact date and time it was made, and what the previous value was.

The Supervisor needs a chronological audit trail of changes to the claim file without navigating through complex financial ledgers.

Which screen in the ClaimCenter user interface should the Supervisor access to find this information?

- A. Loss Details > Status
- B. Notes
- **C. History**
- D. Financials > Transactions

正解: C

質問 # 31

.....

ClaimCenter-Business-Analysts学習教材の試用版を無料でダウンロードできます。ClaimCenter-Business-Analysts学習教材の試用版を使用した後、ClaimCenter-Business-Analystsトレーニングエンジンの利点をより深く理解できると

さらに、Pass4Test ClamCenter-Business-Analystsダンプの一部が現在無料で提供されています: <https://drive.google.com/open?id=1uEllbPnUJOZUXgZ151rXTWFCczg4pm2>