概要

このドキュメントでは、Coupa Spendプラットフォームを介して、本サービス製品としての本ソフトウェアを生産するために、Coupa Softwareが管理するビジネス継続性プログラムの概要を説明します。このプログラムは、セキュリティとコンプライアンスのVPによって監督され、最高レベルのエグゼクティブリーダーシップによってサポートされています。

Coupa 内のビジネス継続性管理 (BCM) は、重要なビジネス プロセスと業務を維持するために必要な主要なスタッフ、リソース、サービス、およびアクションをカバーします。この計画は、ビジネスの中断の拡大に対処することを目的としており、以下のポリシーおよびプロセスに含まれる情報に基づいています。

1. ビジネス継続性ポリシー
2. ビジネス・インパクト評価
3. ビジネス継続性計画
4. データセンターのリカバリ – 支出プラットフォーム
5. インシデント対応計画
6. アクティビティ回復計画
7. コンティンジェンシーテスト – 支出プラットフォーム
8. ビジネス継続性:アクティビティ・リカバリ・テスト
9. インシデント対応テストと卓上演習
10. 年間ビジネス継続性とインシデント対応トレーニング

目標

BCM の目的は、次の目的を達成するための明確な行動方針を提示することです。

1. 人命を守り、クーパの従業員、請負業者、訪問者の安全と幸福を提供します。
2. 会社の財産、資産、記録、財務資産や商業資産を含む情報、およびCoupaの競争力、評判、およびのれんなどの無形資産を保護することにより、物理的資産の不必要な損失の大きさを制限します。
3. 危機の結果としての紛争、混乱、優柔不断を、重大なビジネス中断を引き起こすイベントに対するCoupaの対応方法に関する継続的な準備と教育を通じて、削減します。危機への対応は、クーパの人や事業運営に対する中断の影響を減らすことを目標に、組織化され、効果的で、専門的でなければならない。
4. 重要なビジネス プロセスとコンポーネントに関する優先順位を設定します。
5. 株主、従業員、顧客の信頼を維持する。
6. 適用される法律や規制を遵守することにより、法執行機関、規制、その他の政府機関との生産的な関係を維持します。
7. できるだけ早く通常の業務に戻ります。

ビジネス継続性プランニング

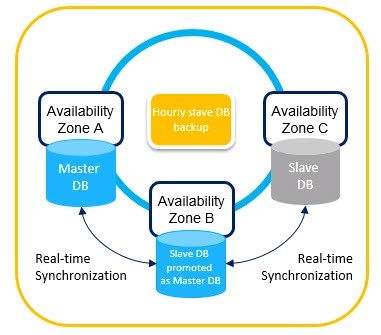
Coupa は、すべての重要なビジネス活動のアクティビティ回復計画を含むビジネス継続性プランを維持しています。ビジネス継続性戦略は、毎年見直され、重要なプロセスとリカバリ戦略を決定します。ビジネス継続性プランは、2019年10月31日に更新/レビューされました。年次レビューと計画の一環として、各アクティビティはビジネス・インパクト評価を完了して、変更や変更が必要かどうかを判断します。これらの影響評価は、年間プラットフォームリスク評価に組み込まれます。Coupaエンタープライズリスク管理(ERM)チームは、リスクを特定、評価、および修復するために設立されました。このチームは組織の断面であり、すべての部門で代表を持っています。毎月、ERMのリーダーシップは、リスク環境における容認できない変化の解決を監視し、優先順位を付けます。

事業継続計画や災害復旧活動を支援するため、BCMチームはリカバリ戦略を支援するために作成され、危機管理チームとしても機能します。このチームは、組織の収益性、評判、および運用能力への損害を回避または最小限に抑えることを目的として、危機や災害に対するCoupaの対応の全体的な調整を効果的かつタイムリーに管理します。

BCM のコンポーネントは、特定されたチーム メンバーによって確認および更新されます。さらに、Coupa では、ビジネス継続性とインシデント対応計画の年次トレーニングとテストが必要です。その後、特定された調査結果は、リスクが許容可能なレベルに緩和されるまで文書化され、追跡されます。

データセンターの復旧

Coupa は、世界クラスのデータセンターを備えたインフラストラクチャ プロバイダー (IaaS) を選択し、クライアントに高レベルの中断のないサービスを提供できるようにします。ほとんどのクーパのお客様は、アマゾン ウェブ サービス (AWS) のグローバルインフラストラクチャーでホストされています。AWS は、信頼性が高く、拡張性が高く、安全な環境を提供します。Coupa は、AWS グローバルインフラストラクチャー内で実行されるプロセスとスケーラビリティーのセーフガードを継承します。Coupa は、AWS アーキテクトと定期的に連携して、セキュリティ、可用性、整合性に関する AWS のベストプラクティスとのアライメントを検証します。図 1 に示すように、Coupa の運用バックアップ構成は、2 つの異なる地域にまたがる 3 つの異なる個別のデータセンターにまたがって、マスタ、スレーブ、および第 3 スレーブ アーキテクチャで実行されます。データセンターのリカバリ計画プロセスは、当社のインフラストラクチャプロバイダーとサブプロセッサによって管理されます。運用環境をサポートする各プロバイダーは、セキュリティと回復の戦略を確認するためにリスク評価を受けます。



内部年次レビューの一環として、回復時間目標 (RTO) および最大許容ダウンタイム (MTD) が計算され、更新されます。データ・センターの復旧計画によりダウンタイムが発生することは少ないですが、災害が発生した場合、RTOは60分です。

|  |  |  |
| --- | --- | --- |
| 重要なプロセス | Rto | Mtd |
| 顧客への Coupa アプリケーションの可用性 | 1時間 | 24時間 |
| Coupa 顧客へのサポートの可用性 (コール センターおよびポータル) | 4時間 | 24時間 |
| 運用担当者の可用性 (サイト信頼性エンジニアリング) | 1時間 | 24時間 |
| 開発担当者の可用性 | 2時間 | 24時間 |
| 主要なドキュメントと手順へのアクセスと可用性 | 1時間 | 24時間 |

テスト、演習、トレーニング

危機管理の計画とテスト - 支出プラットフォーム

クラウドオペレーションチームは、危機管理計画の開始、管理、および実施を担当します。クラウドオペレーションチームは、インシデント対応や予防的なメンテナンスなど、日常業務に対する責任も負います。Coupa はアマゾン ウェブ サービス (AWS) でホストされており、AWS は世界中の複数のデータセンターや地域でかなりの容量と冗長性を持っているため、これらの要素は Coupa と顧客にとって低いリスクです。現在、Coupa はホット サイトと呼ばれる障害復旧サイト戦略で実行されています。

Coupaデータセンターのコンティンジェンシーテストは、少なくとも毎年、リカバリプロセスと手順が成功することを保証するために実施されます。最新のテストは、以下の目的で2019年10月25日に完了しました。

* システム回復に関連するドキュメントとプロセスの改善の機会を特定する
* システムの有効性を評価する
* 自動システム回復の有効性を評価する
* 通知手順の有効性を評価する
* 危機的状況の発生時にシステムの機能とパフォーマンスを評価する
* 回復チーム間の連携の有効性を評価する

最新の危機管理計画テストが正常に完了し、ドキュメントが更新されました。大きな所見や不備はなかった。期待される RTO パラメータ内で復旧されたサービス。さらに、データの回復が必要なテスト ケース シナリオでは、データへの影響 (損失) が発生しないため、RPO が達成されました。1 つのマイナーな発見があった: リージョンのバケットアクセスを持つ S3 IAM ポリシーを更新します。これは、閉鎖されるまで発券システムを介して監視されます。

ビジネス継続性とアクティビティのリカバリテスト

効果的なビジネス継続性計画と手順を実行するクーパ機能を検証するために、Coupaビジネス継続性計画、活動に関連するプロセスと手順を分析するためのチェックリストとレビュー演習を実施します。復旧計画、およびインシデント対応計画。

各アクティビティには、完了のためのチェックリストとビジネス継続性目標のレビューが提示されます。チェックリスト テストには、アクティビティとコンプライアンス マネージャーの回復のための技術のレビュー、監査、検証、検証が含まれます。これらのチェックリストは、以下の方法で、クーパのビジネス継続性の成熟を支援する社内の議論やチームトレーニングを容易にするために使用されます。

* 特定された手順がBCPの目的を満たしていることを確認し、
* BCPが組織のニーズを満たしていることを確認し、
* クーパの担当者に必要なトレーニングを特定し、
* BCP と手順の欠点を特定する。

チェックリストには、計画が正確であるかどうかを確認するタスクと提供されるリソースが含まれます:各アクティビティの復旧計画を実装する、回復を担当する従業員が計画の詳細に精通しているかどうかを確認する、指定されたすべてのステップの実装を確認する計画によって、事前に定義された期限内のすべての義務を完了し、代替手続き(必要な場合)を開始し、必要なすべてのリソース(回復データを含む)を確保し、個々のチームメンバー間のコミュニケーションと警告手順を可能にし、他の回復チーム、危機管理チーム、その他の利害関係者は、他の活動の回復計画との調和を達成し、計画を改善するためにコメントや提案を作成します。

インシデント対応演習とテスト

上記と同じ方法を使用して、インシデント対応チームにチェックリストの練習を使用しました。また、このチェックリスト方式では、卓上運動も行った。卓上演習は、参加者が「教室」の設定で会い、インシデントに対応するアクションに対処するディスカッションベースのイベントです。卓上は、人員が危機シナリオに関連する問題の全範囲を議論するための効果的な初期ステップです。これらの演習は、役割と責任を検討し、相互依存性を発掘し、計画を評価するための優れたフォーラムを提供します。

この演習の参加者には、インシデント対応計画に影響を与えるシナリオが提示されます。ファシリテーターは、演習の目的に対処するために設計された質問をすることによって議論を導くのに役立ちます。ファシリテーターは、議論をさらに刺激するためにシナリオに変更を注入することを選択することができます。参加者はまた、お互いに質問することをお勧めします。

この演習の目的は次のとおりです。

* チームがインシデントを識別する能力を検証します。
* 確認されたインシデントに対応するチームの能力を検証します。
* インシデント対応の職務を担うすべての担当者が、割り当てられた役割に熟練していることを確認するために、追加のトレーニングを実施する必要がある場合は、そのトレーニングを特定します。
* インシデント対応計画の欠点を特定します。

この目標は、提示されたシナリオにおけるインシデント対応処理段階(準備、識別、封じ込め、根絶、回復、フォローアップ)の議論を通じて達成されます。インシデント対応チームのメンバは、ファシリテーターがインシデント対応プロセスにおける自分の役割についてグループに対して提起した質問に答えます。インシデント対応計画は、テストのリファレンスとしてすべてのチーム メンバーに提供されています。これはテストではなく、事故に対応するための現在のキャパシティを測定するために Coupa が使用するツールです。これは、運動ファシリテーターと同じくらい、インシデント対応チームのメンバーにとっての学習メカニズムです。これらの演習のデータは、Coupaが学んだ教訓を策定し、それらの調査結果をインシデント対応能力を管理するポリシーと手順に組み込むのに役立ちます。これらの演習は、IR プロセス内の責任の領域外のすべての役割をチーム メンバーが理解するのにも役立ちます。

ビジネス継続性、アクティビティの回復、インシデント対応のテスト結果

ビジネス継続性およびインシデント対応テスト/演習の結果は、レビューされ、1 つのエンタープライズ レポートにまとめられます。このレポートは、リーダーシップとERMチームにレビューと行動のために提出されます。不適合または調査結果は、修復および閉鎖のためにERM発券キューに記載されます。コンプライアンス マネージャは、レポートの完了と不適合の追跡を担当します。最新のテストと運動期間中、主要な知見はありませんでした。すべてのマイナーな調査結果は文書化されており、解決されるまで追跡されます。

アクティベーション/通知

Coupaは、お客様向けの災害復旧通信計画を立てております。災害時に様々な店舗を通じて、お客様とのコミュニケーションを図るプロセスが確立されています。お客様および利害関係者は、Coupa サポート ポータルまたは Coupa Web サイトを通じて、クーパ の支出プラットフォームの状態を確認できます。

ビジネス継続性とインシデント対応トレーニング

ビジネス継続性とインシデント対応トレーニングが、CoupaU コンピュータベースのトレーニングライブラリに追加されました。ビジネス継続性とインシデント対応に不可欠なチーム メンバーは、毎年このコースを受講する必要があります。

コースコンテンツ:

* 目標
* ビジネス継続性
  + 概要
  + プログラム コンポーネント
  + 情報とドキュメント
  + 現在の状態
  + リソース
  + 重要な活動
* リカバリの優先度と目標復旧時間
* BCPの役割と責任
* 事件
  + 管理の概要
  + 役割と責任
  + 例
  + 対応計画
  + 処理
  + 通信
* クイズ

BCPおよびIRチームメンバー全員が毎年このトレーニングを受ける必要があります。