**概览**

本文档提供了 Coupa Software 通过 Coupa its 平台将其生产软件作为服务产品维护的业务连续性程序的摘要。该项目由安全和合规副总裁负责监督，并得到最高层行政领导的支持。

Coupa 中的业务连续性管理（BCM）涵盖了维护关键业务流程和操作所需的关键人员、资源、服务和操作。此计划旨在解决扩展的业务中断，并基于以下政策和流程中包含的信息：

1. 业务连续性政策
2. 商业影响评估
3. 业务连续性计划
4. 数据中心恢复 - 花费平台
5. 事故响应计划
6. 活动恢复计划
7. 应急测试 - 开销平台
8. 业务连续性 —活动恢复测试
9. 事故反应测试和桌面演习
10. 年度业务连续性及事故应对培训

**目的**

BCM 的目标是提出明确的行动方针，以完成下列工作：

1. 保护人类生命，保障 Coupa 员工、承包商和访客的安全和福利。
2. 通过保护公司财产、资产、记录和信息（包括金融和商业资产），以及 Coupa 的竞争优势、声誉和商誉等无形资产，限制不必要的物质资产损失的规模。
3. 通过不断的准备和教育，减少因危机而产生的冲突、困惑和优柔寡断，让 Coupa 如何应对造成严重业务中断的事件。应对危机必须是有组织的、有效的和专业的，目的是减少中断对 Coupa 人员和业务运作的影响。
4. 建立关键业务流程和组件的优先级。
5. 维护股东、员工和客户的信心。
6. 遵守适用的法律法规，保持与执法、监管和其他政府机构的生产关系。
7. 尽快恢复正常的业务运作。

**业务连续性规划**

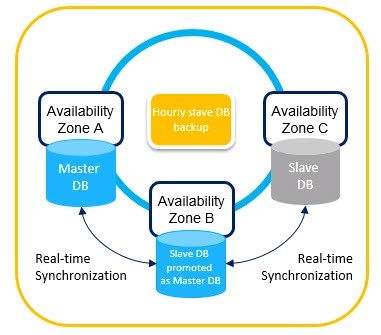
Coupa 维护一个业务连续性计划，包括所有关键业务活动的活动恢复计划。业务连续性战略每年审查一次，以确定关键的恢复过程和战略。业务连续性计划最后一次更新/复核是在 2019 年 10 月 31 日。作为年度评审和计划的一部分，每个活动都完成一个业务影响评估，以确定是否需要进行任何更改或修改。这些影响评估将被纳入年度平台风险评估。建立了 Coupa 企业风险管理（ERM）团队，用于识别、评估和修复风险。这个团队是组织的一个横截面，在所有部门都有代表。每个月，ERM领导层都会对风险环境中任何不可接受的变化进行监控和优先处理。

为了支持业务连续性规划和灾难恢复活动，已经创建了一个 BCM 团队来支持恢复策略，并将作为危机管理团队发挥作用。该团队将以有效、及时的方式管理 Coupa 应对危机或灾难的总体协调，其目标是避免或尽量减少对组织盈利能力、声誉和运作能力的损害。

每年至少有一次，由确定的团队成员对 BCM 的组件进行评审和更新。此外，Coupa还需要对业务连续性和事故响应计划进行年度培训和测试。然后记录和跟踪任何已确认的发现，直到风险降低到可接受的水平。

**数据中心恢复**

Coupa 选择拥有世界级数据中心的基础设施提供商（IaaS），允许 Coupa 为其客户提供高水平的不间断服务。大多数 Coupa 客户托管在 Amazon Web Services（AWS）全球基础设施中。 AWS 提供了一个高度可靠、可扩展和安全的环境。 Coupa 继承了在 AWS 全局基础结构中运行的几个流程和可伸缩性保障。 Coupa 定期与 AWS 架构师合作，以验证 AWS 在安全性、可用性和完整性方面的最佳实践。如图 1 所示，Coupa production backup configuration 运行在一个主、从和三级从体系结构中，跨越两个不同地理区域的三个不同的独特数据中心。数据中心恢复计划过程由基础设施提供商和子处理器管理。支持生产环境的每个供应商都要进行风险评估，以评估其安全性和恢复策略。



作为内部年度评审的一部分，计算和更新恢复时间目标（RTO）和最大允许停机时间（MTD）。由于我们的数据中心恢复计划，预计停机时间很少，但如果发生灾难，则 RTO 为 60 分钟。

| **关键工序** | **回授** | **MTD** |
| --- | --- | --- |
| Coupa 应用程序对客户的可用性 | 1 小时 | 24 小时 |
| 对 Coupa 客户的支持（呼叫中心和门户） | 4 小时 | 24 小时 |
| 操作人员的可用性（现场可靠性工程） | 1 小时 | 24 小时 |
| 开发人员的可得性 | 2 小时 | 24 小时 |
| 获取和提供关键文件和程序 | 1 小时 | 24 小时 |

**测试、练习、训练**

**应急计划与测试 - 开销平台**

云运营团队负责应急计划的启动、管理和实施。云运营团队还负责日常运营，包括事故响应和主动维护。由于 Coupa 托管在 Amazon Web Services（AWS）上，而 AWS 在世界各地的多个数据中心和地理区域拥有巨大的容量和冗余，因此这些元素对 Coupa 和客户来说风险较低。 Coupa 目前运行一个灾难恢复站点策略，称为热点站点。

Coupa 数据中心的应急测试至少每年进行一次，以确保恢复过程和程序是成功的。最近一次测试于 2019 年 10 月 25 日完成，目标如下：

* 确定改进与系统恢复相关的文档和过程的机会
* 评估系统的有效性
* 评估自动化系统恢复的有效性
* 评估通知程序的有效性
* 在突发事件中评估系统功能和性能
* 评估恢复团队间协调的有效性

最当前的应急计划测试成功地完成了，文档也更新了。没有重大的发现或缺陷；服务是在预期的 RTO 参数范围内恢复的。此外，在任何需要数据恢复的测试用例场景中，都不会对我们的数据产生影响（损失），从而实现了我们的 RPO 。有一个小的发现：更新 S3 IAM 策略以获得区域桶访问。这将通过我们的售票系统进行监控，直到关闭为止。

**业务连续性和活动恢复测试**

为了验证 Coupa 执行有效业务连续性计划和程序的能力，将进行检查表和评审工作，以分析与 Coupa 业务连续性计划、活动恢复计划和事件响应计划相关的过程和程序。

每个活动都将提供一份清单，用于完成和审查业务连续性目标。检查表测试将涉及活动和合规经理对恢复技术的审查、审计、验证和验证。然后，将这些检查表用于促进内部讨论和团队培训，以帮助实现 Coupa 业务的连续性，方法如下：

* 确保所确定的程序符合 BCP 的目标，
* 确保 BCP 满足组织的需要，
* 确定 Coupa 人员所需的任何培训，以及
* 识别 BCP 和过程中的任何缺陷。

检查表包括检查计划是否准确的任务和提供的资源：为每个活动执行恢复计划，检查负责恢复的员工是否熟悉计划细节，检查计划中规定的所有步骤的执行情况，在预定的截止日期内完成所有义务，启动替代程序（如果需要），确保所有必要的资源（包括恢复数据），使个人团队成员之间的沟通和警告程序，对其他恢复团队、危机管理团队和其他相关方，实现与其他活动的恢复计划的协调，并创建评论或建议以改进计划。

**事故应对演习与测试**

使用上面描述的相同方法，为事故响应团队使用了一个检查表练习。此外，对于这个检查表方法，还进行了桌面练习。桌面练习是一种基于讨论的活动，参与者在一个 “教室”环境中开会，讨论他们将采取的应对事件的行动。桌面是人员讨论与危机场景相关的所有问题的有效的初始步骤。这些练习提供了一个极好的论坛来审查角色和责任，发掘相互依赖，评估计划。

本次演习的参与者将看到影响事故应对计划的情景。主持人将帮助指导讨论，提出的问题，旨在解决演习的目标。主持人可以选择对场景进行修改，以进一步刺激讨论。大会亦鼓励参加者互相提问。

以下是这项工作的目标：

* 验证团队识别事件的能力。
* 验证团队对已确认的事件做出反应的能力。
* 确定需要进行的任何额外培训，以确保所有负有事故反应职责的人员都能熟练地完成所分配的职责。
* 确定事故响应计划中的任何缺陷。

目标将通过在所述场景中讨论事件处理阶段（准备；识别；遏制；根除；恢复；后续行动）来实现。事件反应小组成员回答调解人向小组提出的关于他们在事件反应过程中的作用的问题。事件响应计划已提供给所有团队成员作为测试的参考。请记住，这不是一个测试，而是一个工具，Coupa将使用它来衡量我们目前对事件的反应能力。对于事件响应团队成员来说，这既是一种学习机制，也是运动促进者的学习机制。这些演习的数据将有助于 Coupa 制定经验教训，并将这些发现纳入管理我们的事故反应能力的政策和程序中。这些练习还将帮助小组成员了解他们在 IR 过程中职责范围以外的所有作用，以便全面了解这些过程和程序将有助于对今后发生的事件作出顺利的反应。

**业务连续性、活动恢复和事件响应测试结果**

对业务连续性和事件响应测试/练习的结果进行审查，并将其合并为一份企业报告。这份报告将提交给领导和 ERM 团队进行审查和采取行动。任何不符合项或发现项都将记录在 ERM 售票队列中，以便进行纠正和关闭。合规经理负责完成报告并跟踪不合格情况。在最近的测试和锻炼期间，没有发现主要的结果。所有次要的发现都已记录在案，并将被跟踪，直到它们被解决为止。

**激活/通知**

Coupa 为客户制定了灾难恢复通信计划。已经建立了与客户沟通的过程，以便在灾难发生时通过各种渠道与客户沟通。客户和涉众可以通过 Coupa 支持门户或 Coupa 网站查看 Coupa 花费平台的状态。

**业务连续性和事故应对培训**

在基于 CoupaU 计算机的培训图书馆中增加了业务连续性和事件响应培训。对业务连续性和事件响应至关重要的团队成员每年都要修这门课。

**课程内容：**

* 目的
* 业务连续性
  + 概览
  + 程序部件
  + 资料和文件
  + 当前状态
  + 资源
  + 关键活动
* 恢复优先级和恢复时间目标
* BCP 角色和职责
* 事件
  + 管理概述
  + 角色与责任
  + 例子
  + 响应计划
  + 处理
  + 通讯
* 小测验

所有 BCP 和 IR 团队成员都必须每年接受此培训。