数据平安方案

一．数据平安概念

数据平安存在着多个层次，如：制度平安、技术平安、运算平安、存储平安、传输平安、产品和效劳平安等。对于计算机数据平安来说：制度平安治标，技术平安治本，其他平安也是必不可少的环节。数据平安是计算机以及网络等学科的重要研究课题之一。它不仅关系到个人隐私、企业商业隐私；而且数据平安技术直接影响国家平安。

二．公司概况

目前公司对于数据平安方面根本只是依赖于托管的机房和阿里云的根本平安保护，并没有我们自己的平安保护措施，或者只有根本的平安保护措施。

托管机房效劳器众多，不会有特别完全的数据平安保护措施。另外，即便其提供系统的平安保护措施，其内部众多效劳器不能保障全部没有病毒或者黑客程序，其内部病毒依然需要防护。

至于阿里云，我们只是享有其根本的平安保护，其他比拟有针对性或者高级的平安防护措施或者手段都跟效劳器一样，需要我们每年缴纳相应的费用才会享有较高级的平安保护。

三．实际统计

宕机时间统计：

过去的一年里，济阳机房因硬件维护、网络维护及软件和系统维护等原因，总宕机时间大概在 24 小时以内，也就是说宕机率小于 0.27%，效劳器的可靠性是大于 99.73%，这样的宕机率虽说不是很低了，但是在对数据平安方面就没有可靠性的保障了，这仅仅是建立在没有被恶意攻击的情况下。

对业务影响统计：

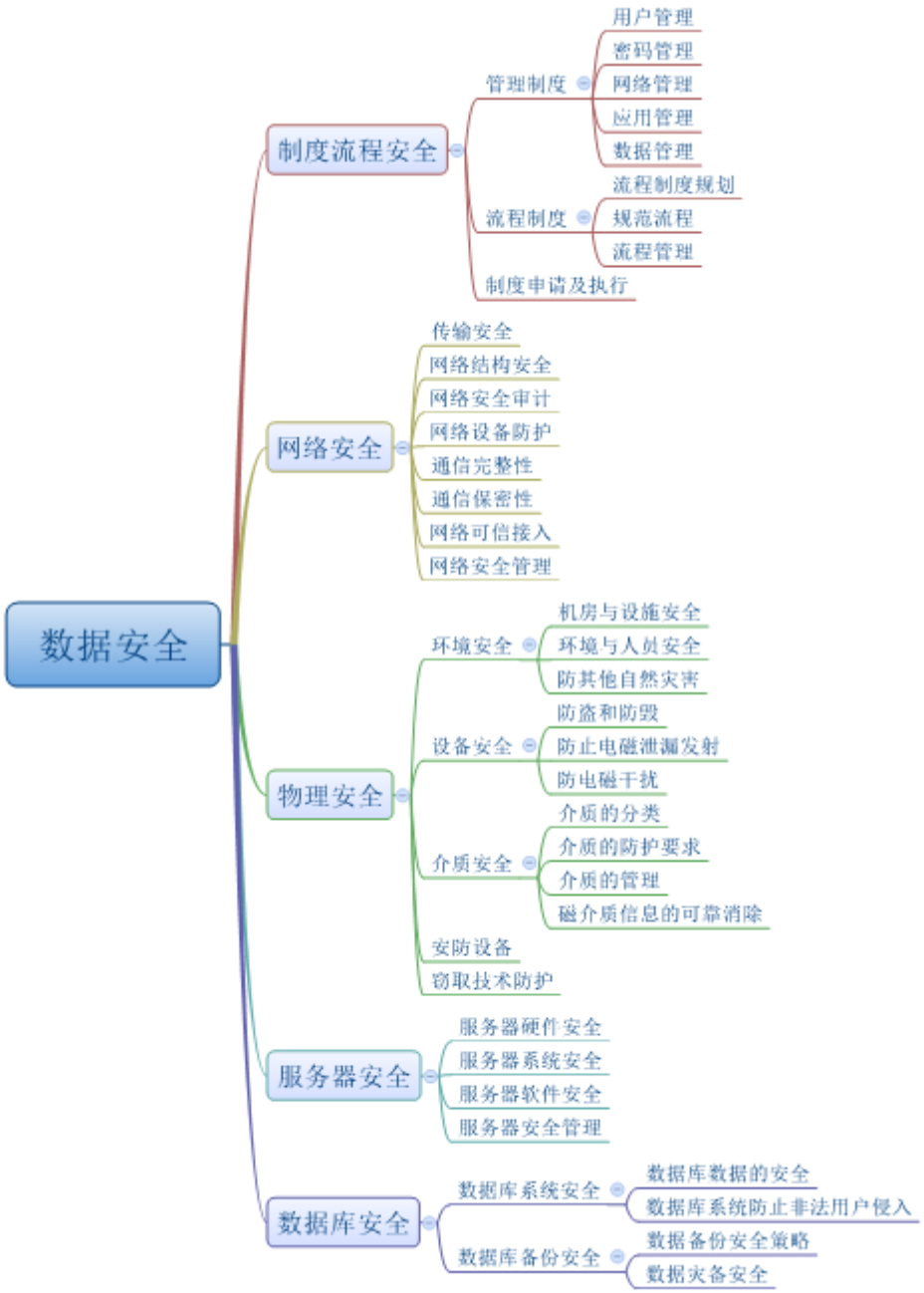
上面简单记述了一下宕机率，但是宕机或者软硬件维护等原因造成的对业务的影响就不是和宕机率一致了，下面我们来简单分析一下：

每次宕机都会直接影响业务的连贯性，所以宕机时间会直接影响全部的业务系统，也就是说过去的一年里对业务的影响最少也是在 24 小时内，这仅仅是宕机造成的影响。再加上软件更新，系统维护，数据库，网络维护等造成的影响，这个时间远远大于 24 小时。经过仔细统计，预估业务影响将大于 7 天：宕机影响 1 天；网络维护 1 天；系统遭受攻击维护 3 天以上，主要原因是在虚拟化平台上各种效劳器众多，网络监控机制较差造成；数据库系统等维护大于 2 天，原因数据库局部参数等更新重启，效劳器系统监控机制较差，局部系统不能时时监控到位等。以上众多原因致使对各种业务影响总加起来的影响将大于 7 天。这样统计下来，我们系统的业务影响率将会大于 1.9%，这样可以看到我们系统应用的稳定性，可靠性都很低。

所有的业务平台都需要一个可靠稳定的后台来支撑，没有可靠稳定的后台，会对我们前台的业务开展产生很严重的影响。

四. 平安结构框架

近期一直在考虑关于数据平安方面的各种事项，在数据平安方面，我们欠缺的还很多很多。从近一年的情况来看，我们最重要的是欠缺一个整体的平安管理体系，当然只是对于我们软件及效劳器等运维方面来说的。近期我整合了一个关于数据平安的体系结构，下面我们来简单看一下，如下列图就是我能想到的关于平安的一个体系结构的框架图。



上图是我根据一些资料以及我个人的想法建立的一个关于数据平安的一个框架图。数据平安从大面来分我能想到的有这几个方面：制度平安、网络平安、物理平安、效劳器平安、数据库平安以及产品和效劳平安 这几个大面，也许每一个大面单独拿出来都可以从专业的角度去书写一本书，这里我就单独结合我们公司的情况简单说明一下每一个方面的事项。

4.1 制度平安

制度平安指计算机拥有单位，为了保证其计算机以及计算机内存储的数据平安而制定的一套约束各工作人员和非工作的规章制度。

在运维中，平安的管理制度也是重中之重，没有统一平安的管理制度，我们在所谓的平安架构平安体系都没有得到实际意义上的平安保障。拥有平安的制度，我们才能去管理和维护一个相对平安的系统。

平安管理制度

建立平安的管理制度是所有平安意义上的一个重要的环节，拥有平安的管理制度，是其他平安的重要保障。

4.1.1.1 用户管理

用户管理分为使用用户、系统用户、应用用户、数据用户等的管理，按照各种用户的不同身份不同等级清晰划分用户的各种使用权限及访问范围，通过各个用户的需求不一，使用不同的权限来限制用户的访问范围。

使用用户是指对应用、系统、数据等的使用者，或者对效劳器、交换机等的使用者，这类用户需要根据其对这类事物的应用范围或者用量等合理安排其权利并作详细的使用记录或者留有操作日志等。

系统用户指操作系统的各个管理用户，在操作系统中，一般 linux 以 root 用户权限最大来管理其他全部用户及文件数据等。Root 用户只有运维管理人员或者系统管理员才可以使用这个用户，其他人员的使用可以根据需求来创立适合需求的用户来管理其用户的数据信息等。

应用用户指应用程序的使用用户，这里需要开发人员做好相应的程序控制，不同用户在我们应用程序中所接触的数据不一样。

数据用户我这里主要针对于数据库的操作用户。 数据库的各个用户根据不同的数据需求赋予其相应的角色或者用户权限，以到达对不同系统数据的保护和保密作用。

所有用户按照其特点统一管理，根据不同用户的属性划分使用者范围及用户管理人员。其他人员需要使用用户需要跟相关的管理人员作出申请，申请审核过后，经过登记以前方可使用其申请的用户权限，其他人员在未经授权的情况下不得随意使用或者在有可使用权限以后不能直接告诉其他未经授权使用的人员。

.2 密码管理

用户密码和用户一致，都需要进行统一的管理。用户及密码的获取均需要提出相应申请经过审核通过后，由管理人员登记给出用户及密码。对于密码的安保性，管理人员更需要时刻注意防止密码的外泄，在需要的情况下，可以对秘密进行加密等手段进行保密处理。

.3 网络管理

网络管理包括网络设备及网络监控等的管理，要保障网络设备平安可靠稳定的运行，例如防毒墙、防火墙等软硬件，合理管理网络设备的 IP 地址，账号密码等不被泄漏，合理设置防毒墙、防火墙等软硬件的过滤规那么和防护等级，合理划分管理区域层次，例如平安管理区域，办公区域，网络接入区，核心交换区，中心效劳区，数据管理区等。

对于高平安性的数据保护措施还需要划分区域边界的平安，主要包括：边界访问控制、边界完整性检测、边界入侵防范以及边界平安审计等方面。

平安管理平台应实现对网络设备的集中管理，实现网络设备的升级、网络设备工作状态监管、网络流量监管、网络设备漏洞分析与加固等功能，同时具备对网络设备访问日志的统一收集和分析。

4.1.1.4 应用管理

应用管理需要加强应用开发，应用代码，应用效劳等的平安管理。

应用开发过程中需要有相应的代码描述和注释，统一的代码书写标准及命名标准等。对于应用代码需要保证代码的平安性，例如防止代码丧失，代码外泄，代码混淆等问题一般比拟常见，一般可以通过 svn 等工具可以从一定程度上提高平安性，但是并不是一定的，也需要从制度上和习惯上的严格要求。应用效劳需要控制好平安数据的私密性，个人隐私数据及保密数据需要做加密及解密措施，以防止隐私数据的透漏。

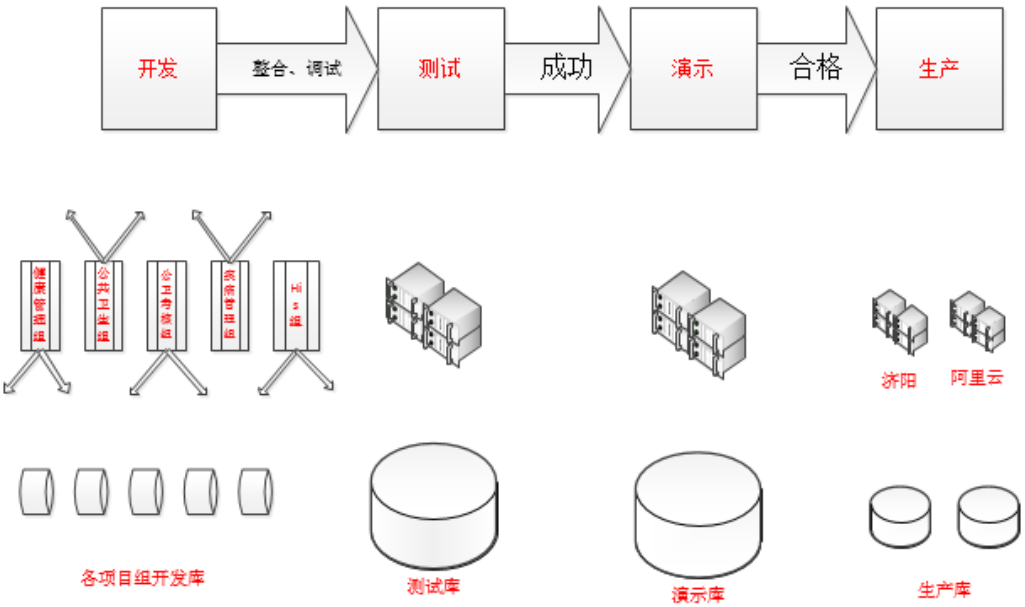
4.1.1.5 数据管理

数据管理主要针对数据库内存储的数据管理，包括数据库用户，密码，数据表空间及表的管理。根据应用系统及存储数据的性质来分配应用使用的用户及密码，划分相应的数据库表结构及表空间。做到数据同一规划，数据存储形式一致，这样既可以保证存储数据的平安性，也可以使我们数据的存储有条理性。现状是数据存储较混乱，A 用户的数据存在于 B 用户的表空间中，这样很容易使用户的数据轻易泄露。而且在数据库中这样也很容易造成各个应用之间对数据的读取消耗很多资源，更严重的就是耗时较高，应用性能的整体降低。

4.1.2 流程制度

4.1.2.1 流程制度规划

下面我们来简单看一下下面的一个流程规划



上图我们可以看到将我们的整体环境划分为四个大的环境，这四个大环境分别有各自的作用：

开发环境：

这个环境严格标准在公司的内部环境，在这里有开发人员做主，开发人员在这个环中可以做日常的开发测试。一般情况下开发人员的代码程序都是在其本地的电脑上，而开发环境中目前只有开发测试数据库。这个环境只作为开发人员开发测试程序使用。

测试环境：

测试环境的要求就相对的要较高一些了。这里的测试环境不是开发测试，这里测试环境是专门用来给测试人员进行各种功能测试及性能测试的环境。环境要求至少需要生产环境减半的配置，或者最少是符合生产要求的独立环境。这个环境不涉及其他任何，只做为测试使用，这样至少保障测试环境的测试结果符合生产环境的要求。只有经过严格测试的应用，排除了大量的 bug 和性能问题的应用，才能说是较稳定的应用。这样这个应用才能上线。

演示环境

这个环境可以适当的降低配置，但是需要保障环境的稳定运行。这个环境的主要作用是公司领导可以在公司内外跟客户做程序的演示时使用。其次测试后的正式应用一定要先都部署在这个环境中，经过领导演示，客户认可，领导审核通过以后，应用产品才可以正式上线。未审核通过的应用经过提出问题或者变更以后，由开发修正测试通过后，再次在演示环境中由领导检验审核。最后全部通过的程序，才能在正式的生产环境中上线。

生产环境

这个环境要求一定是能够承载 5 年业务数据增长量的一个可靠稳定的应用环境。并且环境的要求及软硬件的配置都需要有可靠稳定的保障。在之前的平安架构中的规划只是针对与这个环境的初步规划。生产环境的可靠稳定主要依靠前面的流程严格保障，另外就是环境软硬件的合理标准化配置。通过稳定可靠的软硬件支持及相应的技术保障生产环境的平安可靠及稳定。

4.1.2.2 标准流程

有了相应的管理，就需要去标准其管理流程，包括之前提到的用户管理，密码管理

，网络管理，应用管理以及数据管理等，需要哪些资源或者权限，需要相关人员给与书面或者文字性的申请审核流程，经过审核前方可确认使用。

通过流程的标准包括从开发环境到生产环境的流程，都必须按照流程来标准我们的应用程序的开发及上线，这样我们的后台环境才能有一个稳定平安的根底。

流程管理

确定了流程的事项，就要严格的管理流程，相关的负责人或者部门经理要做到流程管理者的带头和监督的作用。定制了流程就要安装流程来进行，除非某种特殊的情况出现。当然，我们并不希望特殊情况的出现，毕竟无规那么不成方圆。只有规那么制度起了作用我们才能拥有一个健康的管理后台。

4.1.3 制度申请及执行

制度的制定需要向制度监管人或者部门提出申请，审核通过前方可执行。由于之前这一块儿的欠缺，致使这局部的管理松散，也造成我们后台的各种不必要的麻烦，甚至导致影响平安的生产环境。后台的平安管理必须要有相关的平安制度的建立。

4.2 网络平安

在整个数据平安体系中，网络平安是最重要的一环，也是平安的第一个重要关卡大门，所有的数据信息都是通过网络来传输交互的，网络的平安是平安体系中的最重要的一环。

4.2.1 传输平安

网络分区

根据应用部署要求和新一代数据中心建设的原那么，考虑网络平安的实施，数据中心内划分为如下几个区域：

1、数据管理区：集中存储、管理所有应用系统的数据。

2、业务应用区：部署总局端的业务应用系统。

3、支撑平台应用区：部署平台支撑应用系统〔集中认证平台、电子效劳平台、客户端升级系统、Session 集中系统、分布式缓存系统、分布式任务调度系统〕。

4、数据交换区：部署电子业务平台，以供各外挂系统接口使用。

5、公共效劳区：部署公共效劳、WEB 效劳和平安管理所需要的各种设置和应用系统。

6、平安接入区：用于实现与互联网的平安连接和逻辑隔离，包括各种平安保障设施，以及直接向互联网用户提供效劳的应用系统。

7、IT 管控区：用于实现对 ECIQ 主干系统的网络管理、平安管理、运维管理，包括各种平安保障设施和管控平台。

平安接入区域、数据管理区域、应用效劳区域、IT 管控区域，采用身份鉴别：主机身份鉴别和应用身份鉴别；访问控制；系统平安审计；入侵防范；主机恶意代码防范；软件容错；

数据完整性与保密性、 备份与恢复等平安保护措施。 详细见下列图：

计算机环境	保护措施
平安接入区域	操作系统、应用平安加固
	CA 认证系统
	内控运维管理系统
	入侵防御系统 IPS
	入侵检测系统 IDS
	漏洞扫描系统
	补丁管理系统
	网络防病毒系统
	平安管理平台
	数据备份系统
数据管理区域	操作系统、数据库、应用平安加固
	CA 认证系统
	内控运维管理系统
	入侵防御系统 IPS
	入侵检测系统 IDS
	数据库审计系统
	漏洞扫描系统
	补丁管理系统
	网络防病毒系统
	平安管理平台
	数据备份系统备份
应用效劳区域	操作系统、数据库、应用平安加固
	CA 认证系统
	内控运维管理系统
	入侵防御系统 IPS
	入侵检测系统 IDS
	漏洞扫描系统
	补丁管理系统
	网络防病毒系统
	平安管理平台
	数据备份系统
IT 管控区域	操作系统、数据库、应用平安加固
	内控运维管理系统
	漏洞扫描系统
	补丁管理系统
	网络防病毒系统
	平安管理平台

对平安接入区域边界、数据管理区域边界、应用效劳区域边界、IT 管控区域边界采用以下平安措施：边界访问控制、边界完整性检查、边界入侵防范、边界平安审计、外部边界恶意代码防范等。

4.2.1.2 网络可靠性

网络高可靠性方面需要采用构建具备高可靠性的网络结构，我们需要建设的网络要可以对业务流量实现分流，也可以互为灾备，因此

需要构建可靠的硬件冗余以及网络协议冗余，在网络出现单点故障时能够自动侦测到网络的可达性，并对全网络进行宣告，通过硬件切换或软件切换实现网络的可达性，保证网络正常运行。

4.2.1.3 网络负载均衡

负载均衡运行，在网络层面，需要将日常的业务流量均衡至整个数据中心。数据中心内采用负载均衡设备对网络数据流量进行负载分担。

对于业务流量，采用全局负载均衡设备对用户访问数据中心分流，根据策略或负载情况不同用户访问不同的数据中心，分散网络流量，减少网络拥塞，提高访问和效劳质量。

对于数据中心内部效劳器数据流量，采用本地负载均衡把数据流量合理分配给效劳器群内的效劳器共同负担。

4.2.2 网络结构平安

网络结构的平安是网络平安的前提和根底，对于北京双中心主干系统核心路由和网络设备需要进行冗余部署，防止单点故障，并考虑业务处理能力的顶峰数据流量，因此需要冗余空间满足业务顶峰期需要；网络各个局部的带宽要保证接入网络和核心网络满足业务顶峰期需要。

按照业务系统效劳的重要次序定义带宽分配的优先级，在网络拥堵时优先保障重要业务效劳器，合理规划路由，业务效劳器之间建立平安路径绘制与当前运行情况相符的网络拓扑结构图：根据所涉及信息的重要程度等因素，划分不同的网段或 VLAN。

重要业务系统及数据的重要网段不能直接与外部系统连接，需要和其他网段隔离，单独划分平安区域。

4.2.3 网络平安审计

网络平安审计系统主要用于监视并记录网络中的各类操作，侦察系统中存在的现有和潜在的威胁，实时地综合分析出网络中发生的平安事件，包括各种外部事件和内部事件，通过网络监控功能及启用网络设备日志审计，并纳入平安管理平台统一监控管理实现。

4.2.4 网络设备防护

为提高网络设备的自身平安性，保障各种网络应用的正常运行，对网络设备需要进行一系列的平安加固措施，包括：

1、对登录网络设备的用户进行身份鉴别，用户名必须唯一；

2、对网络设备的管理员登录地址进行限制；

3、身份鉴别信息具有不易被冒用的特点，口令设置需 3 种以上字符、长度不少于 8 位，并定期更换；

4、具有登录失败处理功能，失败后采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；

5、启用 SSH 等管理方式，加密管理数据，防止被网络窃听。

同时需要部署内控运维管理系统对设备管理用户登录认证和审计，确保经过授权的管理员通过可靠

路径才能登录设备进行管理操作，并对所有操作过程进行审计、控制、记录，防止

授权用户非法操作或误操作，保证对网络设备进行管理维护的合法性。

4.2.5 通信完整性

信息的完整性设计包括信息传输的完整性校验以及信息存储的完整性校验。

对于信息传输和存储的完整性校验可以采用的技术包括校验码技术、消息鉴别码、密码校验函数、散列函数、数字签名等。

对于信息传输的完整性校验应由传输加密系统完成，对于信息存储的完整性校验应由应用系统和数据库系统完成。

4.2.6 通信保密性

应用层的通信保密性主要由应用系统完成。在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证；并对通信过程中的敏感信息字段进行加密。对于信息传输的通信保密性由应用系统和数据库系统传输加密系统完成。

4.2.7 网络可信接入

为保证网络边界的完整性，不仅需要进行非法外联行为，同时对非法接入进行监控与阻断，形成网络可信接入，共同维护边界完整性。可以将效劳器的 IP 和 MAC 地址绑定，并禁止修改自身的 IP 和 MAC 地址。

4.2.8 网络平安管理

通信网络应当有网络平安监控、网络审计、网络备份／冗余与故障恢复、网络应急处理、网络数据传输平安性保护以及可信网络设备接入，在本工程分别通过网络平安监测、网络平安审计、网络结构优化、设备加固、以及内控运维管理系统来完成。

主干系统按照根本要求保护级别设计信息系统的保护环境模型，依据《信息系统等级保护平安设计技术要求》，按照平安计算环境、平安区域边界、平安通信网络和平安管理中心等进行设计，结合管理要求，形成如下列图所示的保护环境模型：