DORA: un enfoque para su implantación

Celedonio Villamayor Pozo
24 de enero de 2023

FIDES

Pilares clave y requisitos de DORA

Gobernanza y gestión de riesgos de las TIC

- Las entidades financieras establecerán un sistema sólido, completo y bien documentado como marco de gestión de riesgos TIC.
- Los requisitos incluyen sistemas, protocolos y herramientas de TIC actuales, identificar y documentar las funciones comerciales de TIC y los activos relacionados, monitorear, controlar y detectar actividades anómalas dentro del sistema de TIC, establecer recuperación ante desastres, continuidad comercial y planes de respaldo.

Incidentes TIC e intercambio de información

- Las entidades financieras deberán definir e implementar un proceso de gestión de incidentes TIC para detectar, gestionar, clasificar y notificar los incidentes.
- Las entidades financieras también comunicarán las incidencias a la autoridad competente mediante una plantilla predefinida y común.
- DORA proporciona lineamientos para apoyar el intercambio de información relacionada con ciberamenazas e incidentes entre entidades financieras.

Gestión del Riesgo TIC de Terceros

- Las entidades financieras evaluarán, administrarán y monitorearán los riesgos relacionados con los proveedores de servicios de terceros de TIC y los derechos y obligaciones del tercero deben establecerse en un acuerdo contractual.
- Incluye proveedores externos críticos de TIC (CTPP) y proveedores de servicios en la nube (CSP).

Pruebas de resiliencia operativa

- Como parte de su marco de gestión de riesgos de TIC, las entidades financieras establecerán un programa sólido y completo de prueba de resiliencia operativa digital que incluya una variedad de evaluaciones, pruebas, metodologías, prácticas y herramientas para evaluar su sistema de TIC e identificar las debilidades.

Alcanzar la resiliencia no es un lineal recta, es un proceso aditivo

Los ocho pasos hacia la resiliencia

Cuando las cosas van mal, van mal rápido y durante tiempo

0. Empezar con el cliente

- La resiliencia consiste en poder mantener el nivel de servicio incluso en situaciones de estrés. Idealmente, una organización debería ser capaz de mantener sus actividades comerciales habituales en cualquier momento, sin embargo, todos entendemos que eso no es realista.
- Como es de esperar, el primer paso para desarrollar la resiliencia debe ser identificar los productos y servicios que son realmente clave para los clientes. Pero antes de que se pueda juzgar eso, hay una pregunta más fundamental que hacer: ¿quiénes son los clientes de una organización? ¿Cuáles son sus principales clientes?
- Las organizaciones pueden considerar que todos los clientes son igualmente importantes.
- Pero se puede considerar la posibilidad de que ciertos grupos o tipos de clientes sean “más importantes” para el negocio debido al tipo de ofertas, productos o nivel de servicios prestados. En una situación en la que la capacidad de servicio es limitada, es posible que desee priorizar el enfoque en ciertos tipos o grupos de clients.

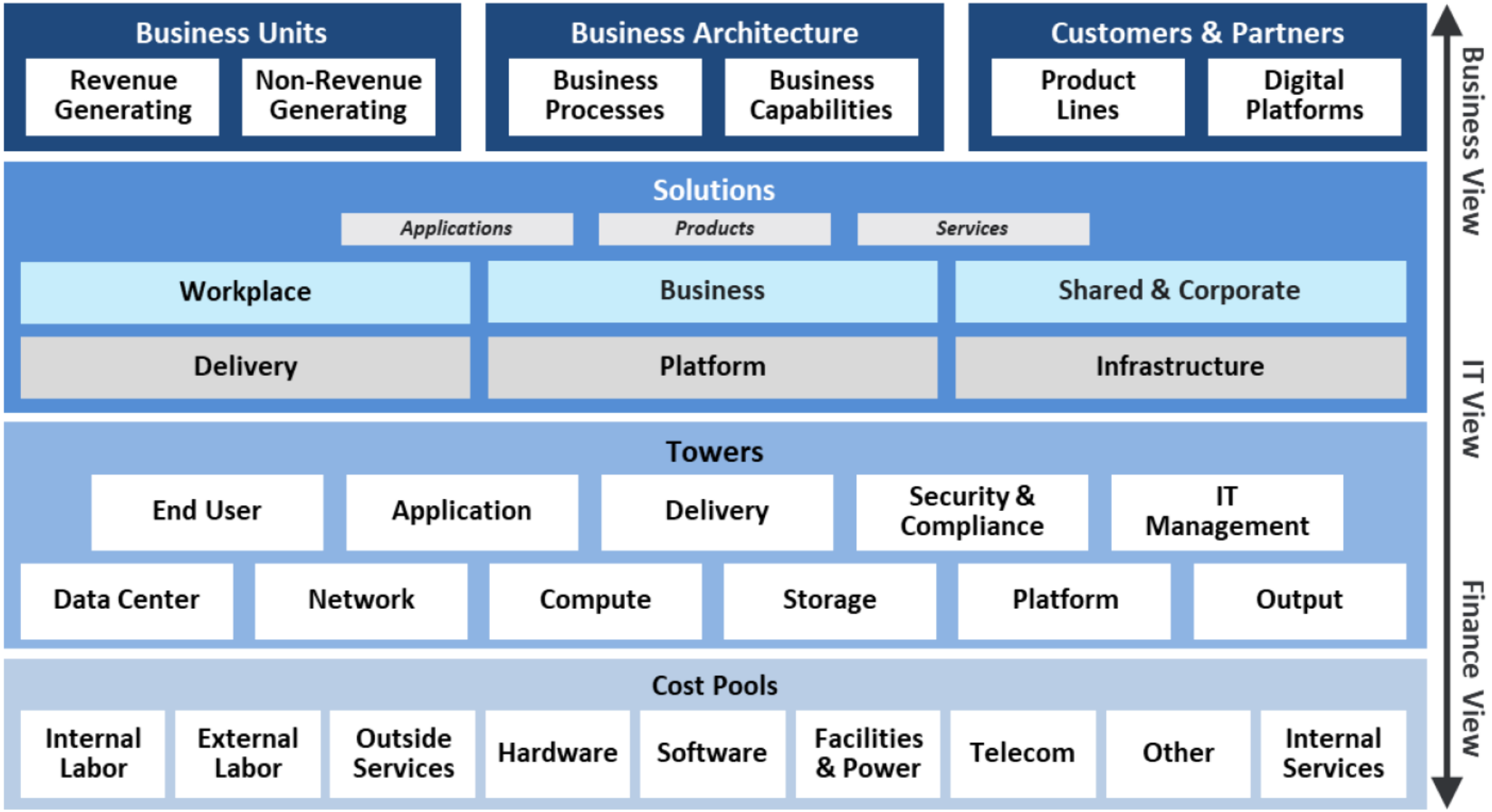
1. ¿Qué es lo que realmente necesitan tus clientes de ti?

- Ya sea que haya decidido segmentar su población de clientes o no, hay otra pregunta importante que hacer: **¿qué debe mantenerse "sin importar qué" para sus clientes (clave)?.**
- Si su organización es un banco, estos productos pueden incluir banca electrónica y comercio on line, mientras que una compañía de seguros puede querer garantizar soporte telefónico 24/7 a los clientes que han tenido accidentes.
- Tenga en cuenta que este paso **debe realizarse una vez para todos los productos y servicios existentes**, mientras que debería convertirse en una pregunta estándar al definir nuevos productos y servicios o cuando se planifican cambios dentro de la cadena de valor (gestión del cambio y cambios en la estrategia comercial).
- La organización debe entrar en una etapa en la que **considere la "resiliencia operativa" como una condición por defecto para cualquier producto o servicio que sea clave** para sus clientes.

2. Aplicar ingeniería inversa a los productos y servicios clave

- Una vez que haya identificado los productos y servicios clave, hay que **centrarse en la cadena de valor** que los creó.
- Primero, debe identificar los procesos clave que contribuyen a ese resultado.
- Tenga en cuenta que aquí también hablamos de procesos clave: cualquier producto en organizaciones complejas es, naturalmente, el resultado de una serie de procesos e interacciones. La pregunta aquí es: ¿qué es clave (en términos de procesos y personal) para mantener, inalterable, la oferta de tal producto?

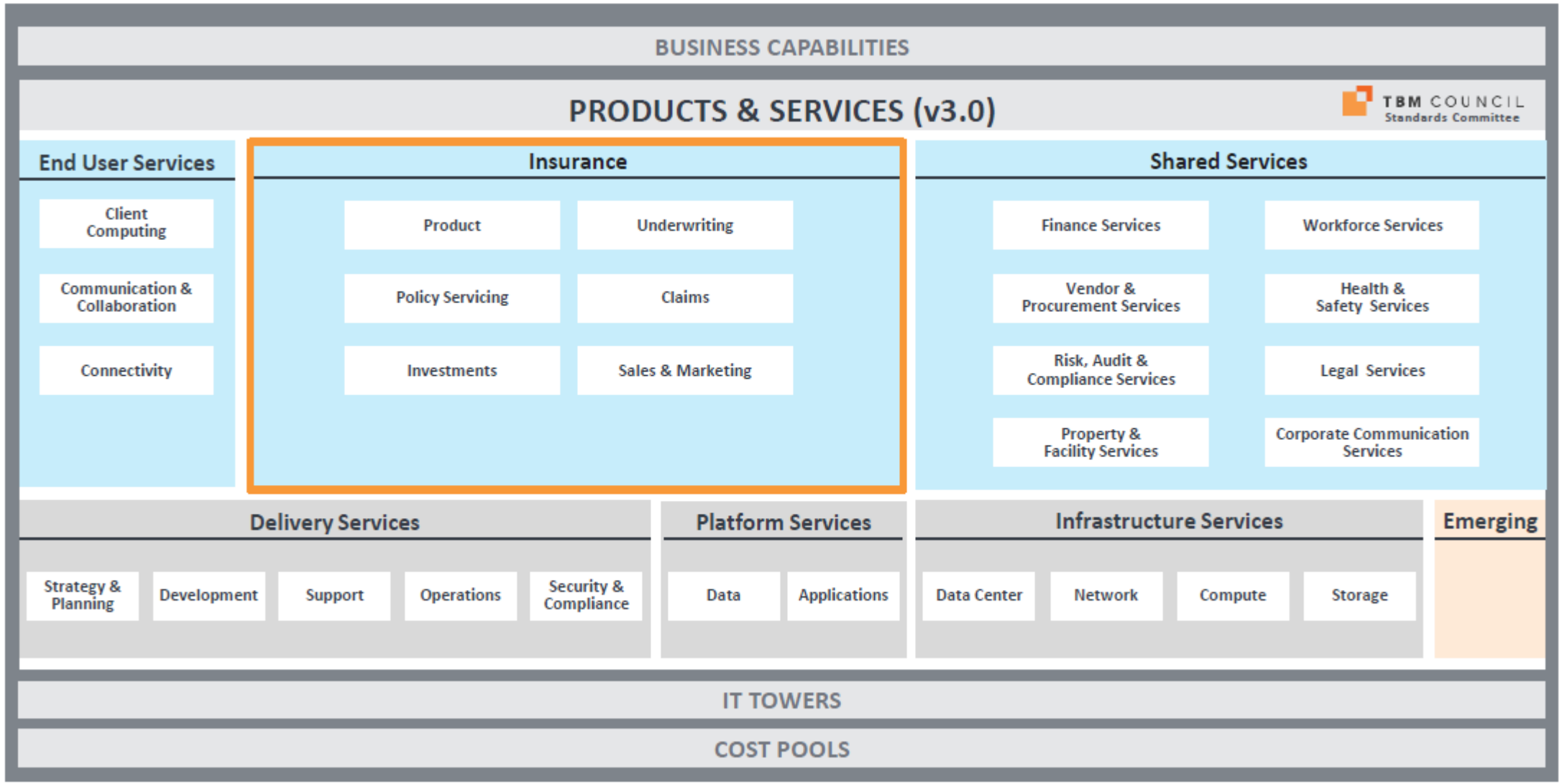
2. Aplicar ingeniería inversa a los productos y servicios clave



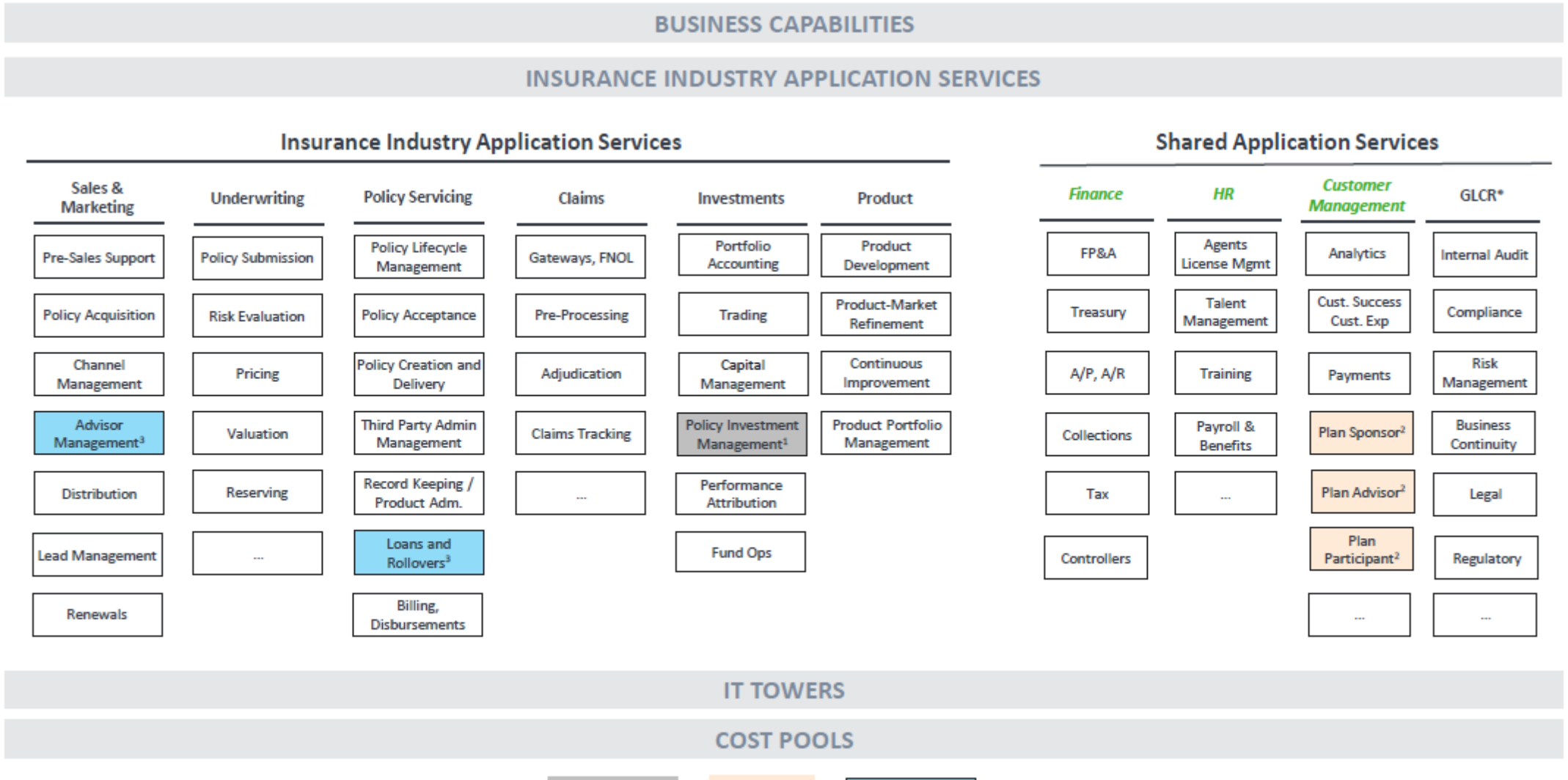
2. Aplicar ingeniería inversa a los productos y servicios clave

- Tomemos nuestro ejemplo de una línea de ayuda telefónica de seguros 24/7.
- Múltiples procesos contribuyen a dicho servicio, incluida una etapa de clasificación para asignar la llamada a la persona más experta disponible y un proceso para grabar la conversación con fines de cumplimiento.
- Lo más importante para que el servicio esté disponible es que la organización disponga de personas que respondan a la llamada.
- ¿Qué es realmente clave en todo esto? Los clientes que llaman a la línea buscan apoyo inmediato, por lo que no aceptarán una “no respuesta”, aunque pueden estar dispuestos a aceptar que la llamada no se grabe si tal proceso falla. Del mismo modo, es posible que acepten no poder hablar con un experto de inmediato (si el proceso de clasificación falla), siempre que alguien más los apoye mientras tanto.
- Entonces, ¿qué es realmente clave? En este caso, es un número mínimo de personas capaces de contestar las llamadas y poder permanecer con los clientes hasta que un experto esté disponible para ellos

2. Aplicar ingeniería inversa a los productos y servicios clave



2. Aplicar ingeniería inversa a los productos y servicios clave



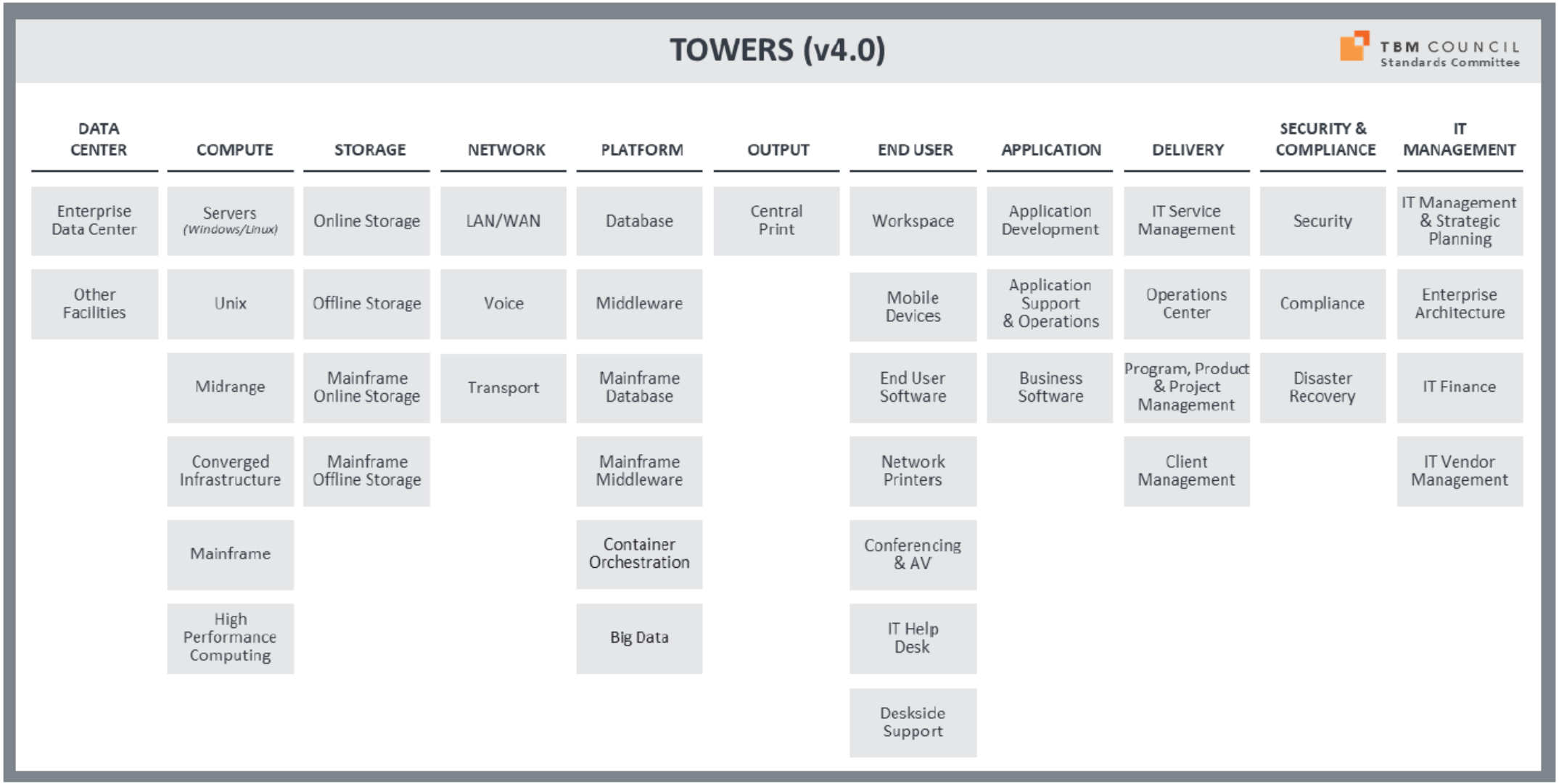
Note: abbreviations used in graphic; taxonomy uses full names

This is a conceptual view of services simplified for display purposes.
It does not represent a best-practice service hierarchy for modeling service costs.

3. Identificar dependencias digitales

- Uno de los resultados de la ingeniería inversa debería ser la lista de sistemas de TI (y sus respectivos datos) y dependencias que son clave para entregar los productos y servicios (resiliencia digital y operaciones de servicios, y resiliencia de datos).
- ¿Qué software se utiliza? ¿Qué redes se aprovechan? ¿Qué infraestructura digital se utiliza? Un servicio prestado a través de una red móvil necesitará consideraciones diferentes a un servicio prestado a través de un teléfono fijo. Qué bases de datos se utilizan, dónde están ubicados los servidores, etc.
- La cantidad de preguntas al respecto es bastante variada y cubre más o menos todo lo que asegura que un producto se entrega a un cliente, procesos, personas y terceros.
- Volviendo al ejemplo: un requisito clave de TI es mantener una línea abierta para que se pueda llamar al personal disponible. Esto incluye tener una conexión que funcione (ya sea LAN o Wi-Fi), un software que funcione para recibir llamadas y un hardware que funcione para permitir que el personal escuche y hable con los clientes.

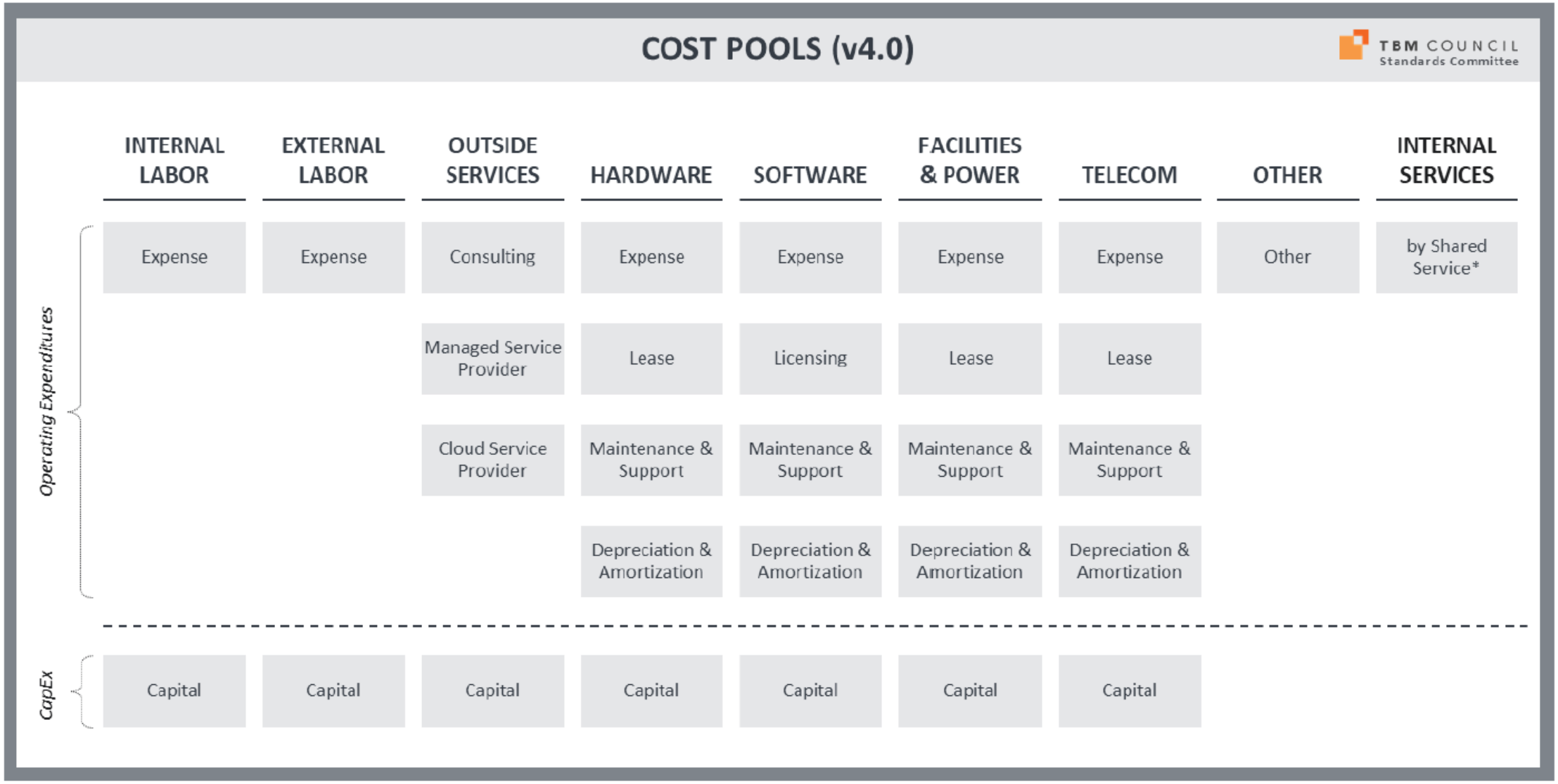
3. Identificar dependencias digitales



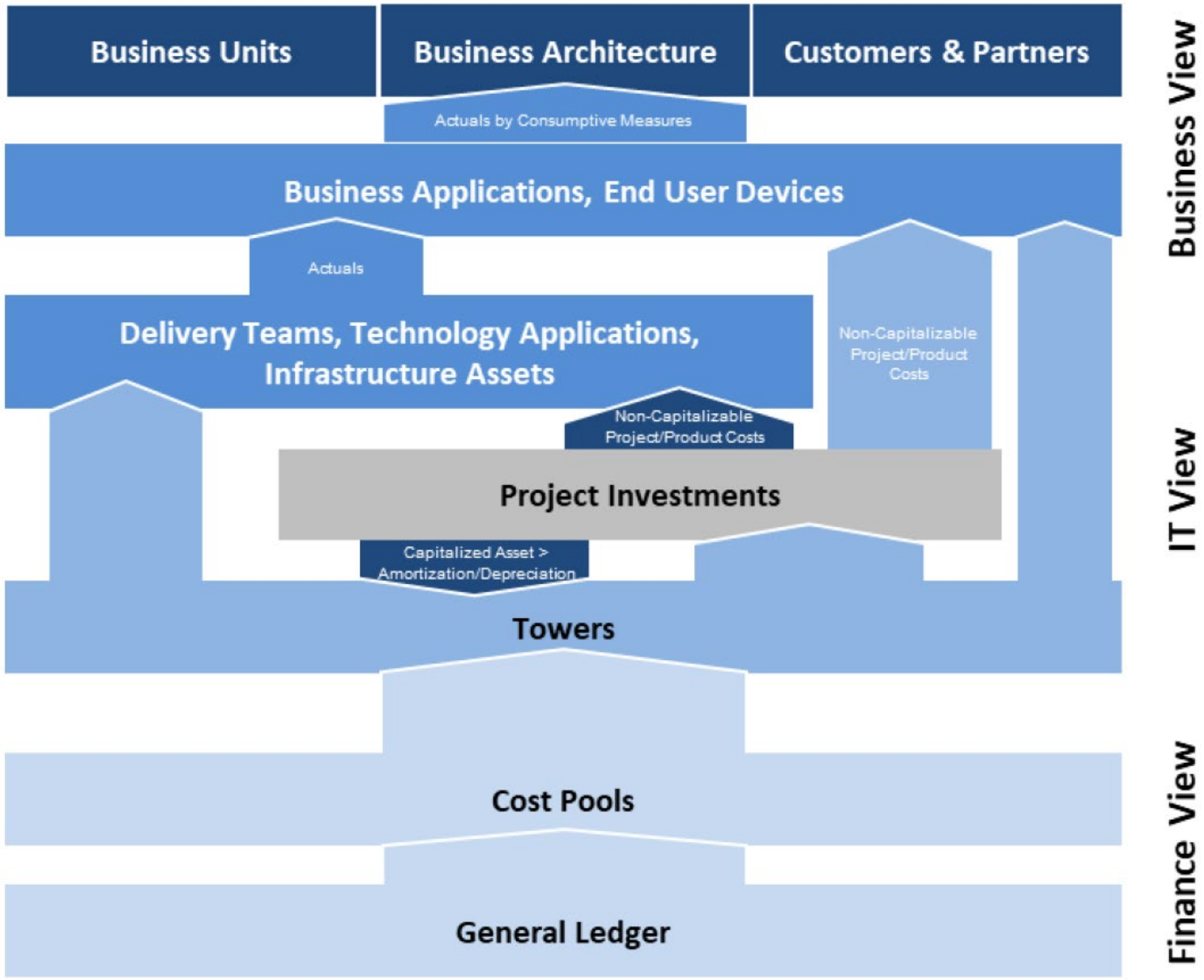
4. Asignar dependencias de terceros

- Es fundamental saber quiénes son los terceros críticos en los procesos e infraestructura identificados (sourcing y dependencias externas). Ya sea que estén en la organización que proporciona la conexión a Internet o en la empresa que le alquila el edificio donde se encuentra su personal: debe comprender con qué terceros “no puede vivir”. Cuando se trata de terceros, también es importante comprender cualquier interdependencia con otros procesos: ¿es el mismo tercero una parte interesada clave en la entrega de una cantidad de productos que aparentemente están desconectados entre sí?
- Volviendo al ejemplo, un tercero puede proporcionarte la infraestructura de TI en la que confías para atender las llamadas, o puedes confiar aún más en terceros para que te proporcionen el personal necesario para cubrir el servicio 24/7.
- Trate de analizar este punto en detalle: es posible que esté confiando en terceros sin darse cuenta, por ejemplo, si una función interna que le proporciona un servicio en realidad depende completamente de un tercero para este proceso

4. Asignar dependencias de terceros



4. Asignar dependencias de terceros



5. Definir posibles escenarios de amenazas

- Llegados a este punto, debería tener una idea clara de qué servicios y productos necesita para poder mantener en condiciones de estrés y qué procesos clave/personas/sistemas de TI/terceros realmente entregan esos productos y servicios críticos.
- Si bien la resiliencia debería significar ser capaz de soportar cualquier tipo de escenario de estrés, uno debe ser pragmático y comenzar con una pregunta bastante simple: ¿qué puede salir mal con los componentes identificados de la cadena de valor? Tenga en cuenta que partimos del supuesto de que la organización ya cuenta con controles para garantizar que cada proceso individual funcione en todo momento, por lo que ahora es el momento de olvidarse del enfoque aislado y tratar de ver la cuestión desde una perspectiva holística.
- Es necesario identificar escenarios de riesgo potenciales que impacten en toda la cadena de valor, en lugar de eventos únicos y aislados que ya están abordados por el marco estándar de gestión de riesgos. Además, es esencial que considere escenarios que amenazan físicamente el negocio (seguridad física y gestión de instalaciones), así como como escenarios que amenazan la viabilidad del negocio en general(gestión de la continuidad).

5. Definir posibles escenarios de amenazas

- Consideremos nuestro ejemplo: en lugar de centrarnos en escenarios de riesgo aislados que afectan a un componente de la cadena de valor (p. ej., todos los empleados de una oficina que se enferman por intoxicación alimentaria), deberíamos ver cómo un evento podría afectar a toda la cadena de valor.
- Digamos que en Asia la compañía de seguros confía en un tercero tanto para proporcionar personal para atender las llamadas como para brindar soporte de TI. Esta empresa pertenece a una organización más grande, que también le proporciona la conexión a Internet necesaria para contestar las llamadas de sus clientes. ¿Qué pasaría si tal organización fuera objeto de una huelga general mañana?

6. Mapear los riesgos de la cadena de valor

- Lo más probable es que su organización cuente con un marco de trabajo de gestión de riesgos (incluida la gestión de riesgos operativos).
- Sin embargo, incluso en este caso, los riesgos a menudo se consideran de forma aislada. TI habrá considerado ciertos riesgos, mientras que el negocio tiene otros riesgos en su radar. Ahora es el momento de considerar todos los riesgos identificados y enumerar aquellos riesgos que están vinculados a la cadena de valor de sus productos y servicios clave. ¿Cuáles son esos riesgos? ¿Están interrelacionados? ¿Qué regulaciones impactan mis procesos clave y cómo se refleja esto en el perfil de riesgo de toda la cadena de valor?
- Al identificar riesgos, se debe prestar especial atención a los riesgos cibernéticos, ya que la resiliencia cibernética es un pilar clave para cualquier organización moderna que intente desarrollar resiliencia operativa.
- Cuando consideramos en nuestro ejemplo la amenaza de una huelga en la empresa de terceros que presta servicios en la ubicación asiática, pueden materializarse diferentes mismo tiempo y afectando toda su cadena de valor en un servicio tan fundamental? Al definir las medidas de mitigación, debe asegurarse de considerar las interdependencias de las amenazas y los riesgos para su cadena de valor

6. Mapear los riesgos de la cadena de valor

- Es importante que identifique todos estos riesgos antes de que se materialicen, para que pueda implementar las medidas de mitigación adecuadas en sus procesos
- Por ejemplo, diferenciar más los riesgos o incluir redundancias internas para los procesos donde los riesgos no se pueden diferenciar.

6. Mapear los riesgos de la cadena de valor

ALCANCE PREVIO AL CONTRATO

¿Es este un proveedor existente o nuevo?
¿Cuál es la naturaleza del producto/Servicio?
- Todos los proveedores/servicios/ubicaciones/instalaciones no son iguales
¿Cómo de esencial/crítico es el producto/servicio?

ALCANCE DURANTE EL CONTRATO

¿Cuál es el nivel de riesgo de la relación?
¿Cuál es el nivel de riesgo inherente/residual del proveedor?
¿Ha habido cambios desde la última evaluación?
¿La evaluación está impulsada por una renovación o modificación del contrato?

6. Mapear los riesgos de la cadena de valor

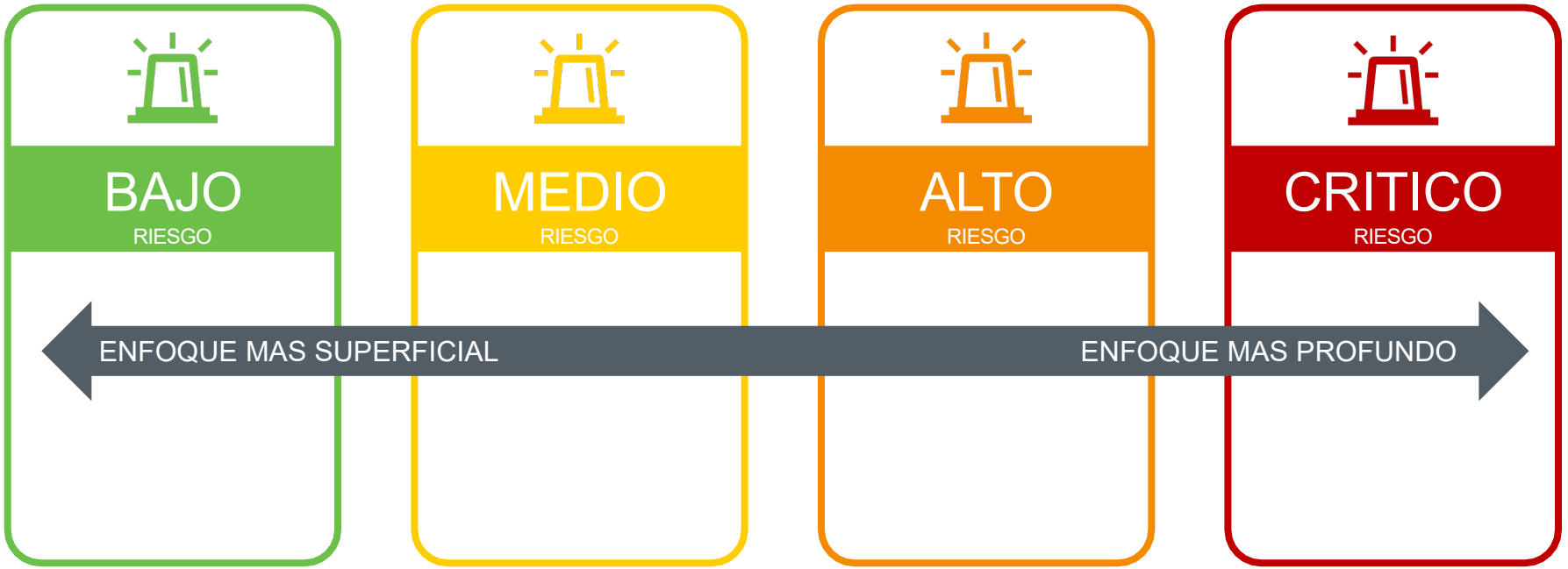
Dominios de Riesgo

Continuidad de negocio	Cumplimiento	Cibersecurida d
Financiero	Cuartas partes	Geografía
Seguridad de la Información	Legal	Seguridad Física

6. Mapear los riesgos de la cadena de valor

Enfoque y Frecuencia de las revisiones

NO TODOS LOS VENDORS REQUIEREN EL MISMO NIVEL DE ATENCION



7. Aprender del pasado

- Incluso cuando haya ejecutado todos los pasos anteriores, es posible que aún se encuentre en una situación en la que un servicio clave experimente una interrupción debido a un evento impredecible (cisne negro) o a interdependencias no identificadas dentro de su organización (puntos negros). . De cualquier manera, debe asegurarse de que las lecciones aprendidas como parte de sus procesos de gestión de incidentes y gestión de crisis se utilicen para definir mejores controles o medidas de mitigación para sus procesos e infraestructura clave.
- En nuestro ejemplo, puede tener dos ubicaciones diferentes que dependen de diferentes proveedores de Internet para garantizar la cobertura (cuando una ubicación no funciona, la otra lo cubre). No podría saberlo, pero ambas compañías confían en los mismos servidores: cuando uno de estos servidores sufre una interrupción, ambas ubicaciones no pueden conectarse a Internet, incluso si intentó diferenciar el riesgo de una interrupción utilizando dos diferentes proveedores. Una vez que haya resuelto el incidente, debe agregar esta información a su evaluación de amenazas y riesgos.

8. Controle su exposición al riesgo

- Cada gran organización tiene KRI (indicadores clave de riesgo) en su lugar. Idealmente, la exposición al riesgo de su organización se mantendrá relativamente baja en lo que respecta a la gestión de riesgos. Sin embargo, en el contexto de la resiliencia operativa, debe asegurarse de que su organización siempre mantenga las luces encendidas y que los procesos y sistemas que forman la cadena de valor de sus productos y servicios clave estén siempre disponibles.
- Si hay indicios de que su servicio puede no brindarse de manera continua y efectiva, pero esto no se refleja en sus KRI, es posible que deba reconsiderar esos indicadores. ¿Está midiendo los parámetros correctos? ¿Está aplicando los umbrales correctos?
- En otras palabras, los KRI deben reflejar la exposición y las debilidades de sus capacidades de resiliencia, que incluyen medidas protectoras y reactivas. Comprender y cuantificar la exposición de sus procesos clave y monitorearlos de manera efectiva es esencial para remediar las brechas de resiliencia y las interdependencias. Este enfoque ayuda a impulsar las decisiones de resiliencia y las inversiones para las discusiones a nivel del Consejo.

En resumen

- En el enfoque propuesto, la resiliencia operativa se materializa cuando hace un buen uso de las capacidades que ya tiene en sus manos y cuando comienza a seguir un enfoque holístico de la cadena de valor relacionada con los productos y servicios que son clave para sus clientes.
- Debería poder hacerlo para los procesos y sistemas existentes, y tratar de incorporar este pensamiento como parte de su estrategia y marco de gestión de cambios, para construir una cultura "resistente por defecto" en su organización cuando se trata de a productos y servicios clave.
- Una vez que haya construido este nivel básico de resiliencia operativa, puede considerar avanzar más en la curva de madurez de "resiliencia" hacia "resiliencia estratégica" (donde le da aún más espacio a las consideraciones sobre sus clientes, quiénes son, qué comentarios están proporcionando , cómo está cambiando su demografía

Marco del programa de resiliencia operativa

El primer nivel del programa está compuesto por líderes sénior que tienen responsabilidad y responsabilidad general por las decisiones estratégicas relacionadas con el programa de resiliencia operativa.

El segundo nivel está compuesto por los Gestores para cada una de las disciplinas clave de las partes interesadas. Estos deben colaborar y coordinar sus respectivos programas y compartir objetivos y métricas conjuntas. Cada uno lidera sus respectivos equipos en el tercer nivel para apoyar el programa de resiliencia.

El tercer nivel está compuesto por representantes de cada uno de los programas. Cada uno de ellos es responsable de la ejecución e implementación de sus planes o programas individuales en relación con el programa de resiliencia y dirigidos por el gestor respectivo.

Individuos asignados que tienen propiedad para desarrollar, ejercer y mantener sus planes y actividades de continuidad comercial según lo guíe el BC PM.

Miembros del equipo de TI que tienen la responsabilidad directa de recuperar la infraestructura y las aplicaciones requeridas según lo indique el DR PM.

Individuos que tienen la responsabilidad directa de garantizar que los activos de seguridad de la organización se mantengan seguros y protegidos. Las actividades son dirigidas por elseguridad cibernéticaPM.

Individuos que tienen responsabilidad directa sobre la cadena de suministro crítica y/o terceros. Actividades dirigidas por el Tercero.

Personas que tienen la responsabilidad directa de la gestión de crisis en toda la empresa. Actividades dirigidas por el CM PM.