UNIVERSITAS MULIA

IT RISK MANAGEMENT
M. Zulfariansyah, S.Kom., M.TI

IT RISK PORTFOLIO

SESSION 2

Contents

1. Introducing the IT risk portfolio
2. Implementing an IT risk management capability
3. Health check
4. Case study: European fleet management services provider

UNIVERSITAS MULIA

The need for the IT risk portfolio

Dunia bisnis mulai melihat nilai dari pendekatan terintegrasi untuk mengidentifikasi dan mengelola risiko bisnis; waktu yang tepat untuk bidang SI untuk mulai mengembangkan pendekatan terpadu untuk mengidentifikasi dan mengelola risiko terkait TI. Tidak hanya pendekatan seperti itu akan bermanfaat bagi bisnis dalam upaya mereka untuk mendapatkan nilai maksimum dari investasi TI mereka, itu juga akan membantu menyatukan sebagian besar literatur SI di bawah payung konseptual yang umum.

Dengan melihat pengembangan dan pemeliharaan sistem bersama dengan akuisisi paket dan outsourcing sebagai bagian dari proses investasi TI bisnis, manajemen risiko menjadi pusat perhatian. Dengan melihat kegagalan pengembangan sistem, pelanggaran keamanan dan ancaman persaingan sebagai jenis berbeda dari fenomena kesatuan risiko TI yang terkait, menjadi mungkin untuk membuat keputusan tradeoff end to end yang cerdas di sepanjang siklus hidup sistem dalam organisasi. (Markus, 2000, hlm. 176)

UNIVERSITAS MULIA

First : seek to manage IT risks like other business risks

An IT risk is something that can go wrong with IT and cause a negative impact on the business.

***an IT opportunity is something that can go right with IT and cause a positive impact on the business*.**

UNIVERSITAS MULIA

Classes of IT Risk (Portofolio)

1. Projects – failing to deliver;
2. IT service continuity – when business operations go off the air;
3. Information assets – failing to protect and preserve;
4. Service providers and vendors – breaks in the IT value chain;
5. Applications – flaky systems;
6. Infrastructure – shaky foundations; and
7. Strategic and emergent – disabled by IT.

UNIVERSITAS MULIA

1. Projects – failing to deliver

Suatu proyek dapat gagal dalam berbagai cara lain dan pada tingkat yang lebih besar atau lebih kecil.

Tiga kegagalan kinerja utama adalah dalam hal waktu, kualitas, dan ruang lingkup.

Daftar contoh Project yang Kurang Baik :

1. menyelesaikan terlambat,
2. mengkonsumsi lebih banyak sumber daya dan dana dari yang direncanakan,
3. memberikan fungsionalitas yang lebih sedikit kepada pengguna daripada yang direncanakan, memberikan produk di bawah standar, mengganggu bisnis selama implementasi, dan sebagainya.

UNIVERSITAS MULIA

2. IT service continuity

Kelas risiko ini berkaitan dengan pemadaman layanan TI dan tidak dapat diandalkan yang menyebabkan gangguan pada bisnis.

Ini berkaitan dengan sistem operasional atau produksi dan kemampuan mereka untuk terus berjalan dengan andal untuk mendukung kebutuhan pengguna.

UNIVERSITAS MULIA

3. Information assets

Kelas risiko TI ini secara khusus berkaitan dengan kerusakan, kehilangan, atau eksploitasi aset informasi yang disimpan di dalam dan dibawa oleh sistem TI.

Dampak risiko aset informasi dapat sangat bervariasi. Sebagai contoh, informasi penting dapat bocor ke pesaing bisnis, rincian kartu kredit pelanggan dapat dicuri dan digunakan untuk tujuan penipuan, atau hanya dipublikasikan - merusak hubungan pelanggan dan reputasi perusahaan. Proses bisnis inti yang bergantung pada informasi penting dapat sangat terdegradasi, seperti ketika cek saldo bank ternyata saldo yang ditampilkan tidak akurat.

UNIVERSITAS MULIA

4. Service providers and vendors

Saat ini penyedia layanan dan vendor memainkan peran penting dalam pengiriman proyek TI dan kegiatan sehari-hari.

Ketika penyedia layanan TI gagal memberikan ada potensi dampak langsung dan signifikan pada sistem dan layanan TI.

Dampak lain dapat dirasakan dalam jangka panjang; seperti kelemahan dalam kepemimpinan teknologi mitra IT Services delivery, yang diam-diam mengikis efektivitas TI secara keseluruhan.

UNIVERSITAS MULIA

5. Applications

Kelas risiko ini berkaitan dengan kegagalan dalam aplikasi TI. Aplikasi biasanya adalah sistem yang berinteraksi dengan pengguna dan di sebagian besar organisasi akan merupakan kombinasi perangkat lunak paket dan perangkat lunak khusus yang pada tingkat tertentu akan diintegrasikan bersama.

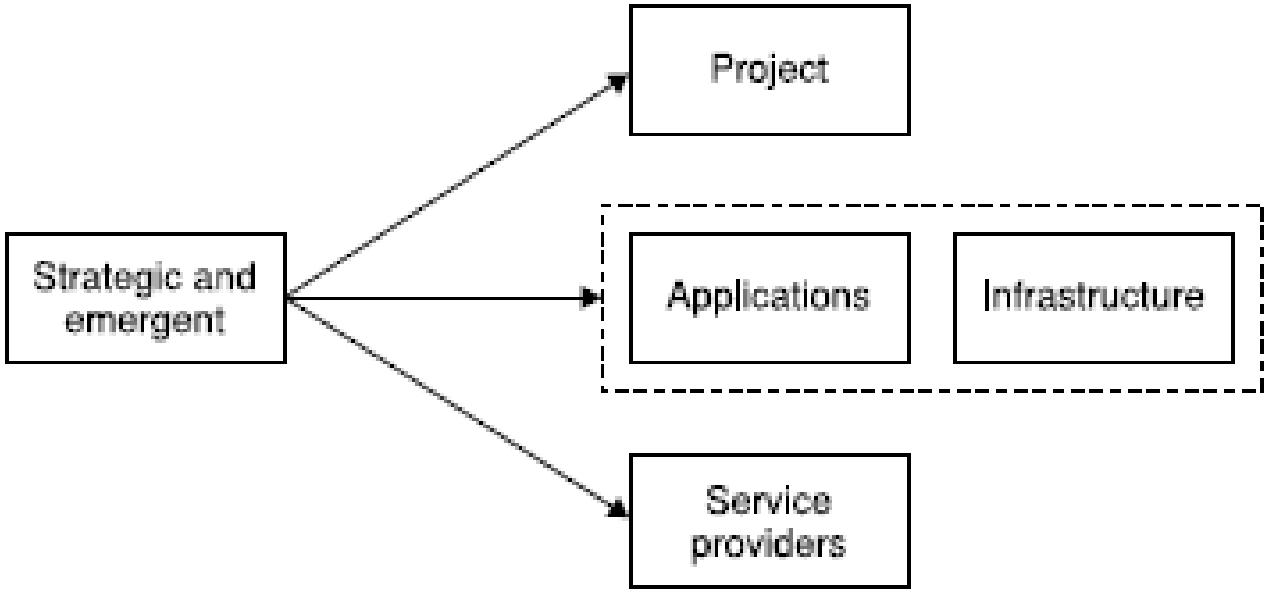
UNIVERSITAS MULIA

6. Infrastructure

Kelas risiko ini berkaitan dengan kegagalan dalam infrastruktur TI. Infrastruktur adalah nama umum untuk berbagai sumber daya komputer dan jaringan yang terpusat dan didistribusikan tempat aplikasi di-host dan dijalankan. Juga termasuk dalam definisi infrastruktur adalah perangkat lunak platform seperti sistem operasi dan sistem manajemen basis data.

UNIVERSITAS MULIA

7. Strategic and emergent risk relationships



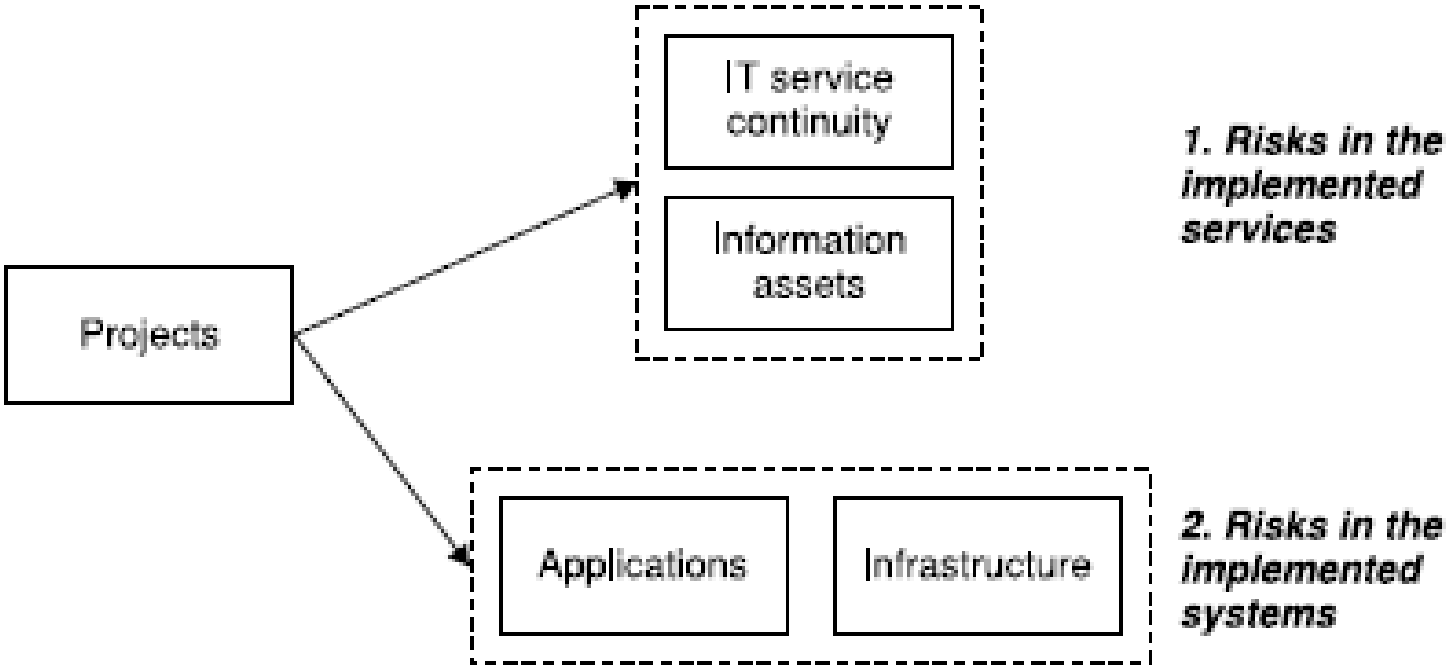
1. Risks in project selection and direction

2. Risks in system architecture and component selection

3. Risks in service provider selection

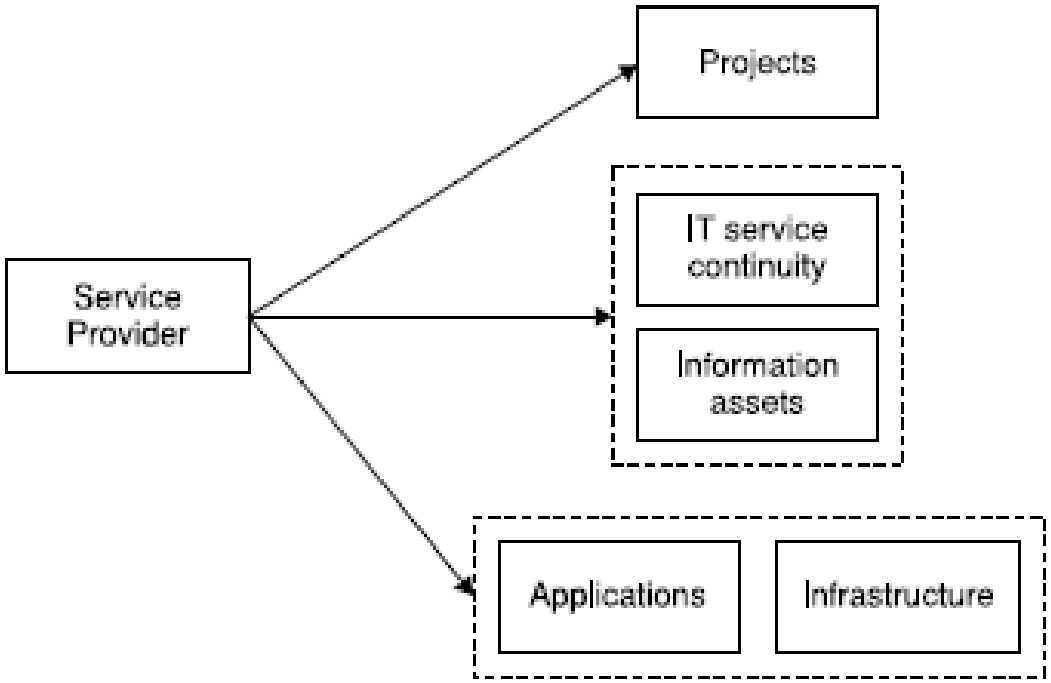
UNIVERSITAS MULIA

Project risk relationships



UNIVERSITAS MULIA

Service provider and vendor risk relationships



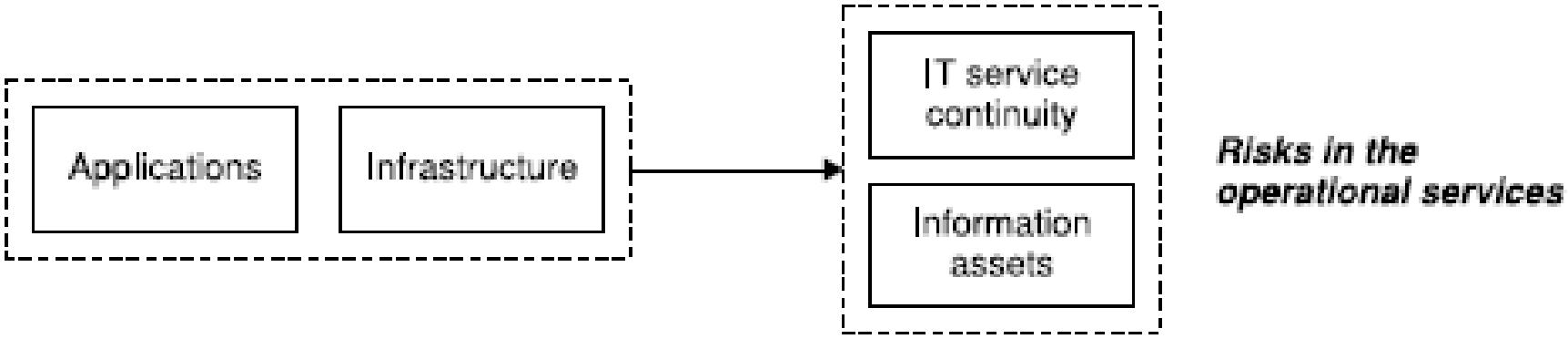
1. Risks in the delivered project services

2. Risks in the delivered operational services

3. Risks in the supported systems

UNIVERSITAS MULIA

Applications and infrastructure risk relationships



UNIVERSITAS MULIA

Wider impacts of your IT failures

An IT risk is something that can go wrong with IT and cause a negative impact on the business.

UNIVERSITAS MULIA

Table 3.1—Business impact examples attributable to IT risk causes

Impact	*IT risk cause and examples*
Financial	A costly IT project fails to deliver and the investment is written off. Example: Sydney Water spent A$60 million on a customer information and billing system project that was cancelled in late 2002 (NSW Auditor-General, 2003). A major outsourcing deal blows out. Example: UK magistrates court Libra contract costs have nearly doubled (*IntoIT*, 2003). Misuse of systems to perpetrate crime or fraud. Example: Kidder Peabody suffered significant loss with the illicit trading activities of Joseph Jett who fabricated profits of approximately US$339 million, perpetrated through insider abuse of trading and accounting systems (Dhillon and Moores, 2001).
Reputational	Major business processes visible to the public grind to a halt because of an IT service outage. Example: Extensive Bank of America ATM outages in January 2003 caused by corruption of their database servers by the SQL Slammer worm (*Infosecurity*, 2004). Sensitive customer information is disclosed resulting in fraudulent misuse. Example: Softbank in Japan reported the leakage of 4.5 million customer records in February 2004 and attempted extortion (Softbank, 2004).
Regulatory or legal	Integrity of information resulting in a penalty for breach of legislation Example: AT&T incorrect billing resulting in successful legal action by the State of Florida in 2004. Failure to comply with legislation. Example: 14 years after legislation required the coastguard to develop a vessel identification system, no such system exists (GAO, 2002).
Customer	Customer service is significantly impaired. Example: *Cigna HealthCare's $1 billion IT overhaul and CRM initiative went live in a big way, with 3.5 million members of the health insurance company moved from 15 legacy systems to two new platforms in a matter of minutes. The migration did not go smoothly. In fact, there were glitches in customer service so significant that millions of dissatisfied customers walked away, causing the nation's fourth largest insurer to lose 6 percent of its health-care membership in 2002.—CIO*, 2003 Closing for business. Example: Early in 2004 the SCO Group was the target of the MyDoom virus that pointed infected computers at the SCO Group corporate website in a massive denial of service attack. Their site couldn't cope and was soon closed for business. Business could be restarted only at a new Internet address (*AFR*, 2004b).* Failing to deliver what the customer needs. Example: The UK eUniversity flopped after having attracted only 900 students (*Times*, 2004).
Competition	Being outstripped by a rival with a better service. Example: In a press release relating to Google's IPO, Standard & Poor's reveal that more than six out of ten Google users would switch search engines if a better service came along (Standard & Poor's, 2004).

UNIVERSITAS MULIA

Implementing an IT risk management capability

Kemampuan manajemen risiko TI yang efektif adalah yang memenuhi kebutuhan bisnis Anda, dengan mempertimbangkan elemen desain utama berikut:

- Strategi dan kebijakan;
- Peran dan tanggung jawab;
- Proses dan pendekatan;
- Orang/Pegawai dan kinerja.

UNIVERSITAS MULIA

Strategy and policy

- **Bagaimana manajemen risiko TI terintegrasi dengan kegiatan manajemen risiko bisnis yang lebih luas?**
- **Sejauh mana pengambilan keputusan sehubungan dengan risiko TI didelegasikan dan apa otoritas di berbagai tingkat manajemen?**
- **Apa kelas risiko TI Anda dan bagaimana masing-masing kelas risiko dikelola?**

(Jelas sangat direkomendasikan agar portofolio risiko TI ke tujuh sebagai titik awal Anda!)

- **Apa selera risiko keseluruhan perusahaan dan bagaimana seharusnya semua karyawan menginterpretasikan hal ini ketika berhadapan dengan risiko TI?**
- **Apa dampak potensial kritis terhadap bisnis dari risiko TI yang menjadi fokus utama upaya manajemen risiko?**
- **Bagaimana dana dan sumber daya dialokasikan untuk kegiatan manajemen risiko TI?**
- **Apa yang merupakan risiko material yang, jika diidentifikasi, harus dilaporkan dan jika demikian, kepada siapa harus dilaporkan?**
- **Risiko mana yang dikelola secara proaktif - yaitu, sebelum peristiwa yang tidak diinginkan dan tidak diinginkan yang ditentukan - dan risiko mana yang dikelola secara reaktif, setelah terjadinya satu atau lebih peristiwa yang tidak diinginkan dan tidak diinginkan?**

UNIVERSITAS MULIA

Roles and responsibilities

Some important considerations include:

- Pemisahan tugas - memastikan bahwa untuk setiap kelas risiko, peran independen melakukan kegiatan pemantauan dan peninjauan;
- Menyeimbangkan kebutuhan akan input spesialis - menyumbangkan pemahaman tentang suatu proses, sistem atau risiko spesifik, dan pengambilan keputusan manajerial - menimbang semua faktor dan menentukan arah tindakan;
- Memasukkan peran manajemen risiko TI ke dalam struktur yang ada di mana ada kecocokan alami. Sebagai contoh, tindakan perlakuan manajemen risiko akan secara alami selaras dengan manajer proyek untuk risiko proyek;
- Menciptakan peran manajemen risiko TI baru ketika diperlukan, misalnya, peran koordinasi kesinambungan bisnis lintas fungsi; dan
- Mengalokasikan tanggung jawab bersama bila perlu dan memastikan semua slot diambil.

UNIVERSITAS MULIA

Processes and approach

1. Identifikasi / penemuan - mendapatkan risiko TI di radar manajemen;

2. Penilaian / analisis - memahami risiko TI dalam konteks seluruh portofolio risiko TI dan menilai kemungkinan terjadinya dan dampak potensial pada bisnis;

3. Perawatan - menentukan pilihan terbaik dari berbagai tindakan yang mungkin dilakukan untuk menangani risiko, merencanakan dan menyelesaikan tindakan yang diperlukan; dan

4. Pemantauan dan peninjauan - menindaklanjuti untuk memastikan apa yang direncanakan benar-benar dilakukan dan untuk memahami setiap perubahan lebih lanjut dalam portofolio risiko TI.

UNIVERSITAS MULIA

People and performance

Manajemen risiko TI juga tentang orang dan kinerja mereka.

Keterampilan dan pengetahuan masyarakat dalam manajemen risiko TI perlu dikembangkan dan dipelihara.

Ini membutuhkan beberapa kombinasi antara pendidikan dan pelatihan yang berhubungan dengan risiko IT, sesuai untuk peran dan tanggung jawab yang dipegang.

UNIVERSITAS MULIA

Health check:
Is IT risk management important to your business?

- Banyak jenis risiko TI berpotensi berdampak pada bisnis.
- Ada berbagai pandangan tentang bagaimana risiko TI harus dikelola.
- Memperoleh airtime manajemen dan pendanaan untuk kegiatan terkait risiko TI sulit.

If you agree with two or more of the three statements, then IT risk management is important to your business.

Health check:
Is IT risk management important to your business?

- **Risiko TI ditinjau secara berkala.**
- **Proses untuk identifikasi dan analisis risiko TI dapat diulang, terstruktur, dan konsisten.**
- **Alokasi biaya dan upaya untuk mengelola risiko TI menerima pertimbangan formal.**
- **Semua pemangku kepentingan terlibat dalam menentukan prioritas relatif dan strategi perawatan risiko TI.**
- **Pendanaan risiko TI yang sedang berjalan mencakup aspek teknis dan aspek manajemen / manusia.**
- **Jelas bagaimana berbagai jenis risiko TI ditangani dan dikelola.**
- **Manajemen risiko TI secara efektif terkait dengan proses manajemen risiko perusahaan yang lebih luas.**
- **TI dikelola secara proaktif.**
- **Kegagalan TI diperiksa sehingga perubahan kebijakan, prosedur dan pendekatan yang diperlukan dapat dilakukan sebagai proses pembelajaran berkelanjutan.**

If you agree with these statements, then you are doing the right things in your organization. If you disagree with three or more of the nine statements, then there is significant room for improvement in your IT risk management capability

UNIVERSITAS MULIA

Health check:
Do you have a good track record?

- Bisnis telah terhindar dari dampak negatif dari sebagian besar jenis risiko TI.
- Penilaian dan pendapat TI dipercaya dan dihargai oleh bisnis.
- Ketika tindakan mendesak telah diperlukan untuk memperbaiki krisis TI, jawabannya telah telah efektif (juga jawab ya jika Anda belum mengalami krisis TI yang signifikan).
- Kerugian nyata yang dialami dari kegagalan TI di masa lalu telah dapat diterima.

If you agree with these statements, then you have a good track record of managing IT risks. If you disagree with two or more of the four statements, then there is evidence of the need to improve IT risk management capability.

UNIVERSITAS MULIA

Open Now