BAB I PENDAHULUAN

I.1 Latar Belakang

Dalam era modern yang digerakkan oleh kemajuan teknologi, transformasi digital telah menjadi pendorong utama perubahan dalam berbagai sektor industri, perusahaan dipaksa untuk dapat mengadopsi transformasi digital tersebut ke dalam setiap proses bisnisnya agar tidak kehilangan pangsa pasar dengan cepat serta dapat bersaing dengan perusahaan baru yang muncul dan langsung mengadopsi transformasi digital dalam proses bisnisnya (Warner & Wäger, 2019). Transformasi digital (TD) didefinisikan sebagai "*perubahan mendasar yang dapat terjadi dalam penerapan dan pemanfaatan teknologi digital ke dalaman sumber daya suatu organisasi dengan tujuan utamanya untuk meningkatkan kinerja dari suatu organisasi serta dapat meningkatkan perbaikan bagi organisasi*" (Gong & Ribiere, 2021 hal-01). Transformasi digital tidak hanya sekadar proses implementasi teknologi, tetapi juga melibatkan perubahan pada proses, struktur, strategi, serta model bisnis, guna meningkatkan layanan kepada pelanggan (Gurbaxani & Dunkle, 2019).

Penelitian sebelumnya mengidentifikasi 28 mekanisme tata kelola teknologi informasi yang mempengaruhi transformasi digital, terdiri dari 6 struktur, 17 proses, dan 5 mekanisme relasional, dengan keamanan informasi dan manajemen data sebagai komponen penting di dalamnya (Mulyana dkk., 2021). Fungsi Teknologi Informasi (TI) dalam bisnis juga dituntut untuk mampu meningkatkan efektivitas, efisiensi, dan keamanan data pelanggan dalam setiap layanan yang diberikan. (Rinanty dkk., 2017). Saat ini, banyak perusahaan di berbagai industri, termasuk industri perbankan terdorong untuk menerapkan TI dalam upaya transformasi digital mereka untuk menjaga keutuhan data (Mulyana dkk., 2022). Pada literatur lainnya menyatakan bahwa, transformasi digital juga berpotensi mempengaruhi kinerja organisasi (Mulyana dkk., 2023). Hal ini juga berlaku bagi perusahaan berskala UMKM dalam industri keuangan, seperti Bank Perkreditan Rakyat (BPR). Meskipun TI menawarkan potensi besar dalam mendukung TD, terdapat pula risiko signifikan, terutama terkait keamanan informasi. (Utami dkk., 2021). Keamanan Informasi memiliki peranan yang sangat signifikan dalam

berjalannya layanan suatu perusahaan, karena melibatkan banyak aspek seperti privasi, integritas, serta kerahasiaan pelanggan (Antunes dkk., 2021). Untuk itu, perusahaan perlu mengambil langkah strategis guna menghindari dampak yang ditimbulkan dari risiko yang akan muncul. Pada suatu perusahaan, bentuk keberhasilan transformasi digital yang terjadi tidak hanya dilihat dari penerapan teknologi terkini, tetapi juga bergantung pada kemampuan perusahaan dalam mencegah dan mengatasi ancaman siber yang semakin canggih dan beragam. Temuan pada penelitian sebelumnya menunjukkan bahwa empat mekanisme SMKI yang bersifat *ambidextrous* (dewan dan eksekutif, strategi dan arsitektur, data dan informasi, serta kolaborasi internal dan eksternal) sangat memengaruhi kinerja organisasi, yang di mediasi oleh transformasi digital (Mulyana dkk., 2024a). Potensi penerapan sistem manajemen keamanan informasi (SMKI) *ambidextrous* yang strategis dalam sektor perbankan, dengan menyeimbangkan eksplorasi dan eksploitasi inisiatif digital, dapat meningkatkan kinerja dan daya saing organisasi di era digital yang terus berkembang. (Mulyana dkk., 2024b).

Menurut (Panjaitan dkk., 2021 hal-2814)“ *SMKI merupakan suatu proses yang disusun berdasar pendekatan risiko bisnis untuk merencanakan, mengimplementasikan, meninjau ulang dan memonitor, dan memelihara atas keamanan informasi perusahaan*”. SMKI yang baik tentu disertai dengan pengelolaan sistem yang baik pula, di mana sistem tersebut harus dianggap sebagai komponen penting dalam proses bisnis yang terjadi dan merupakan tanggung jawab bersama bagi semua pihak di perusahaan. Dalam hal ini, SMKI tidak cukup jika hanya dilakukan dari segi teknis saja, namun juga memerlukan analisis dan pengelolaan risiko untuk mendapatkan gambaran terhadap berbagai risiko yang mungkin timbul di dalam organisasi (Putri dkk., 2022). UMKM berpotensi untuk dapat mengadopsi keamanan sistem informasi dalam jalannya bisnisnya.

Terdapat 90% Perusahaan yang terdapat di negara berkembang adalah UMKM, sehingga membuat posisi UMKM menjadi penting di dalam proses menaikkan ekonomi negara (Saah, 2021). Oleh karena itu, penting bagi UMKM untuk dapat meningkatkan produktivitas serta efisiensinya agar dapat bertahan di era revolusi industri 4.0 ini dengan melakukan transformasi digital (Classen dkk., 2021).

Penerapan teknologi digital pada UMKM, harus disertai dengan tanggung jawab mereka dalam melakukan perlindungan data (Telukdarie dkk., 2022). Penerapan teknologi pada UMKM dapat membuka peluang baru bagi mereka sehingga memberikan banyak keuntungan salah satunya dari retensi pelanggan yang sangat penting untuk keberlanjutan bisnis, namun penerapan teknologi ini juga dapat mengakibatkan UMKM terkena dampak dari ancaman kejahatan siber, maka dari itu diperlukannya strategi ataupun manajemen keamanan informasi, jika tidak terdapatnya hal tersebut, UMKM akan berada dalam risiko siber (Varachia dkk., 2022). Peningkatan penerapan teknologi digital oleh perusahaan telah menyebabkan meningkatnya serangan siber di seluruh sektor. UKM (Usaha Kecil dan Menengah) cenderung lebih rentan dibandingkan perusahaan besar karena terbatasnya akses terhadap sumber daya teknologi digital dan keterampilan yang mumpuni (Bada & Nurse, 2019; Classen dkk., 2021). Selain itu, seiring dengan beralihnya model bisnis ke ruang *online*, banyak perusahaan maupun organisasi yang terus mengabaikan keamanan siber dan terus menerus dipandang sebagai target, terutama UMKM (Varachia dkk., 2022). Dalam Peraturan OJK Nomor 7 Tahun 2024 tentang Bank Perkreditan Rakyat (BPR), disebutkan bahwa BPR atau Bank Perkreditan Rakyat Syariah (BPRS) didirikan berdasarkan perubahan izin usaha Lembaga Keuangan Mikro (LKM) menjadi BPR atau BPRS (POJK 7 Tahun 2024 BPR dan BPRS, 2024.). Sebagai bagian dari UMKM, BPR juga menghadapi tantangan serupa terkait keterbatasan sumber daya dan pengetahuan di bidang keamanan siber, yang menjadikannya sasaran potensial bagi serangan siber.

Salah satu bentuk penerapan yang dapat dilakukan oleh BPR untuk mengelola keamanan sistem informasi ialah dengan menggunakan suatu standar keamanan internasional, yaitu dengan menerapkan standar internasional keamanan informasi seri ISO/IEC 27000. Seri ISO/IEC 27000 merupakan standar untuk sistem manajemen keamanan informasi (SMKI) yang akan membantu suatu organisasi tetap mengikuti perkembangan dan beradaptasi terhadap semua perubahan dalam lingkungan keamanan informasi (Damian Vasquez, 2023). Penelitian kali ini akan fokus terhadap penggunaan ISO/IEC 27001. ISO/IEC 27001 merupakan standar internasional yang disiapkan untuk penerapan, pembangunan, pemantauan,

pengoperasian dan pemeliharaan sistem manajemen keamanan informasi yang dapat digunakan oleh organisasi secara luas dan tentunya dapat melindungi aset informasi dari berbagai risiko (Fathurohman & Witjaksono, 2020).

Penyusunan tugas akhir ini bertujuan untuk menyusun penggunaan ISO 27001:2022 dalam hal keamanan sistem informasi untuk transformasi digital pada UMKM BPR. Hal ini diharapkan dapat memberikan manfaat bagi peneliti dan objek yang diteliti sehingga jalannya bisnis yang dimiliki oleh UMKM BPR akan mampu dalam menghadapi maraknya ancaman siber pada era yang serba digital ini.

I.2 Perumusan Masalah

Rumusan masalah yang akan dibahas pada penelitian ini adalah:

1. Bagaimana penyusunan rekomendasi solusi sistem manajemen keamanan informasi berdasarkan hasil analisis kesenjangan penilaian pada lingkup klausul ISO 27001:2022 prioritas untuk transformasi digital UMKM?
2. Bagaimana perancangan sistem manajemen keamanan informasi berdasarkan klausul ISO 27001:2022 prioritas untuk transformasi digital UMKM?

I.3 Tujuan Penelitian

Tujuan yang ingin dicapai dari penelitian ini adalah:

1. Menganalisis dan merancang sistem manajemen keamanan informasi yang sesuai dengan standar ISO 27001:2022 untuk BPR dengan mempertimbangkan aspek peraturan keuangan yang berlaku.
2. Mengevaluasi pengaruh perancangan sistem manajemen keamanan informasi berbasis ISO 27001:2022 terhadap kesiapan sertifikasi sistem manajemen keamanan informasi pada BPR.

I.4 Batasan Penelitian

Terdapat batasan-batasan Dalam melaksanakan penelitian tugas akhir ini, yaitu:

1. Nama dan identitas BPRBCO serta informasi spesifik lainnya akan dirahasiakan dalam seluruh laporan dan publikasi penelitian untuk menjaga anonimitas perusahaan, dokumen yang digunakan dalam penelitian ini hanya akan digunakan untuk keperluan analisis dan tidak akan dipublikasikan.
2. Penelitian ini akan menggunakan metode *Design Science Research* dengan pengumpulan data melalui wawancara dan dokumen.

I.5 Manfaat Penelitian

Manfaat yang bisa didapat dari penelitian ini, yaitu:

1. Meningkatkan basis pengetahuan penelitian dalam menggunakan ISO 27001:2022 area fokus SME untuk transformasi digital UMKM.
2. Pemanfaatan implikasi praktis hasil penelitian sistem manajemen keamanan informasi untuk transformasi digital UMKM di BPRBCo.
3. Bagi BPRBCo dan referensi untuk organisasi sejenis dapat mengambil manfaat dari hasilnya guna meningkatkan keamanan informasi mereka sesuai dengan standar ISO 27001:2022.