

## Company introduction

— We provide long-term support for IT design and digital transformation over several years, and respond immediately to cyber incidents upon contract signing.



Why this deck is on your screen

## Which of the following best describes your company's current situation?



Please refer to the relevant page.

**A**

### We haven't mapped out an IT roadmap

**Situation**

IT investment decisions vary by department, and there is no overarching strategy.

**Results**

We will have all the necessary materials to submit a proposal for the IT-Design engagement within three months.

Go to Slide



**04 · 06 · 15**

**B**

### Digital transformation has stalled

**Situation**

The vendor is moving forward, but the data and design haven't caught up, so we can't make a decision.

**Results**

Can provide a quote for incorporating LV3 as a design layer into an existing project.

Go to Slide



**05 · 06 · 15**

**C**

### Has suffered or is currently experiencing a cyberattack

**Situation**

Suspected ransomware, data breach, or intrusion. Action is required within 24 hours.

**Results**

Emergency Contact Information on Slide 11  
You can contact us right now via the form.

Go to Slide



**11 · 15**

The cost of doing nothing

## How much are companies losing as a result of misguided actions?



These figures are not exaggerated.

**A**



**If you proceed without an IT design**

**\$4.88M per incident**  
(Global average, 2024)

Source: IBM, "Cost of a Data Breach Report 2024"  
(Published July 30, 2024)

<https://newsroom.ibm.com/2024-07-30-ibm-report-escalating-data-breach-disruption-pushes-costs-to-new-highs>

Breakdown:  
Downtime + Regulatory compliance +  
Customer churn + Brand damage

**B**



**If DX stalls**

**52% of digital initiatives fail to meet business goals**  
(Only 48% met or exceeded the target)

Source: Gartner Press Release (October 22, 2024)

<https://www.gartner.com/en/newsroom/press-releases/2024-10-22-gartner-survey-reveals-that-only-48-percent-of-digital-initiatives-meet-or-exceed-their-business-outcome-targets>

Breakdown:  
A majority of cases involve one or more of the following: failure to achieve ROI, missed deadlines, or unfulfilled scope

**C**



**If you are hit by a ransomware attack**

Median duration of business suspension	Maximum Penalty for Corporations
<b>21days</b>	<b>¥100M</b>

Source (downtime): Coveware Quarterly Ransomware Report (historical median)  
<https://www.coveware.com/ransomware-quarterly-reports>

Source (Penalties): Amended Personal Information Protection Act  
(Amended in 2020; fully enforced as of April 1, 2022)  
<https://www.ppc.go.jp/personalinfo/legal/kaiseihogohou/>

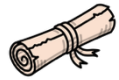
In addition:  
Criminal liability of directors and executive officers, disclosure obligations, and impact on stock prices

## Consulting is not an abstract task.



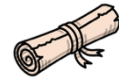
For LV3 Engagement, we will provide the following deliverables:

**Common to all 3 services** — Required for all contracts (Project, Advisory, or Recovery)



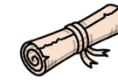
### Issue Report

Organize risks and concerns in a structured, prioritized manner



### Progress Report

Milestone Status, Plan vs. Actual, Summary for Stakeholders



### Quality Report

Design and Implementation Review Results, QA Metrics, Corrective Actions

## Project (IT-Design) Specific



### Roadmap Document

3-part PDF (ASIS Current State Analysis → Migration Plan → TOBE Target Architecture)



### Data Model

DMBOK-compliant ER diagrams, data specifications, and data flow diagrams

## Advisory Specific



### Monthly Design Review Log

Cumulative Record of Design Decisions



### Minutes of the Vendor Meeting

Minutes and Decision-Making Support for Key Vendor Meetings

## Recovery (Code Red) Specific



### Damage Assessment Report

Facts, Scope of Impact, Root Causes



### Restoration Report (New Architecture)

Post-Recovery Configuration Diagram, Measures to Prevent Recurrence, and Handover Items




The above is the standard set. It can be modified depending on the project.

Three engagement modes

## Depending on the situation, you can choose from three levels of involvement



We have also clearly specified what is “not included” — This is to preempt any discussions with Procurement regarding the scope. All contracts are quasi-mandate agreements.

	 <b>Project</b>	 <b>Advisory</b>	 <b>Recovery (Code Red)</b>
<b>Range</b>	One-time IT-Design engagements (Roadmap creation, new system design, migration planning)	Monthly involvement in ongoing DX/IT programs (Design layer)	Post-cyber incident containment, forensic investigation initiation, and recovery plan development
<b>Period</b>	Typically, a few years or so—	Typically several months to several years	Usually about one year
<b>Structure</b>	A team composed of senior IT designers and members from the Data, Dev, and Design teams, organized according to the scale of the project	Led by senior IT designers, with the Data and Research team involved as needed	Led by senior IT designers, the Research (Forensics), Data, and Support teams are involved
<b>Contract Type</b>	Quasi-mandate Agreement	Quasi-mandate Agreement	Quasi-mandate Agreement
<b>Deliverables</b>	Common Report (Issues, Progress, Quality) + Roadmap Document and Data Model	Common Report (Issues, Progress, Quality) + Monthly Design Review Minutes and Minutes from Vendor Meetings (Attended)	Common Report (Issues, Progress, Quality) + Damage Assessment Report + Restoration Report (New Architecture)
<b>Exclusions</b>	Managed Services / 24/7 Monitoring	Provision of Development Resources (Staff Leasing)	Attacker Attribution (Law Enforcement Domain) / Long-Term SOC Operations

Remote support is the standard. On-site support is available if large-scale recovery efforts are required.

Please refer to Slide 06 for billing details and Slide 10 for cancellation terms. The detailed scope will be finalized in the Statement of Work (SOW) after the NDA is signed.



Pricing

## Prices are available upon request

Since quotes vary depending on the scope, duration, and structure of each engagement, we do not publish a standard price range.

# Pricing on request

Billing Method (Applies to All Contract Types): Individual quotes. Initial term: 1 month; subsequent terms: 3-month renewals



### Project

Includes: Common Report (Issues, Progress, Quality) + Roadmap Document and Data Model



### Advisory

Includes: Common Report (Issues, Progress, Quality) + Monthly Design Review Minutes and Minutes from Vendor Meetings (Attended)



### Recovery (Code Red)

Includes: Common Report (Issues, Progress, Quality) + Damage Assessment Report, Restoration Report (New Architecture)

We will provide a detailed quote after the NDA is signed. We can respond to RFIs and RFPs. Quotes denominated in foreign currencies are also available.

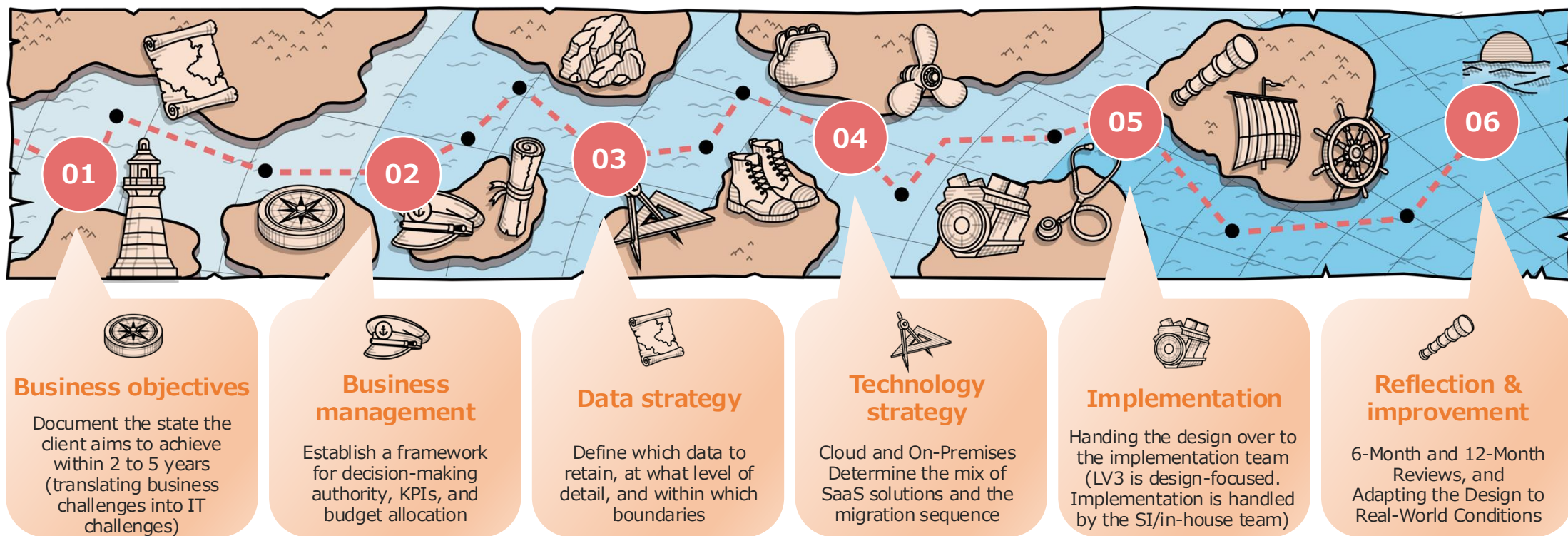
Contact: LV3 Administrative Staff (The Contact Form: [lv3.biz/en/#contact](https://lv3.biz/en/#contact))

How LV3 actually works

## Level 3 IT design is a journey through six phases



Detailed methodologies are included in \*ITG: A Practical Guide\* (Gijutsu Hyoron-sha, scheduled for publication in August 2026). In practice, we use the six phases as a framework and apply them flexibly to each project.






For the average duration and deliverables for each phase, see Appendix A.

## An Overview of the Case Studies



Due to confidentiality obligations, we do not disclose the figures, names, or details of other clients' individual projects (even after an NDA has been signed).

These slides outline the standard framework for projects handled by LV3.

Case A	Case B	Case C
 <b>IT-Design Engagement</b> Regulated industries (finance, public sector, healthcare, etc.)	 <b>DX Advisory</b> Private company	 <b>Code Red Recovery</b> Mid-sized business organization
<b>Challenge Industry</b> It was necessary to consolidate IT investment decisions, which had been scattered across different departments, through a cross-functional strategy.	<b>Challenge Industry</b> While vendors are making progress on the ongoing DX program, data design has not kept pace, resulting in frequent decision-making bottlenecks.	<b>Challenge Industry</b> Ransomware incident
<b>The Role of Level 3</b> Development of a three-part roadmap consisting of ASIS diagnosis, migration plan, and TOBE architecture. Delivery of the data model and a consolidated report (issues, progress, and quality).	<b>The Role of Level 3</b> Monthly involvement in the design phase. Documenting decisions, attending vendor meetings, and reviewing data consistency	<b>The Role of Level 3</b> Within the first 72 hours: issue containment instructions, initiate forensic analysis, and draft a briefing for senior management. Provide 1-3 weeks of migration support and deliver a damage assessment report and a recovery report (new architecture).





\*Please note that details regarding individual projects for other clients, including your company's project, are confidential and cannot be disclosed.

## There are situations where Level 3 isn't the best choice







LV3 is the best fit for those looking for a partner who can support their IT design efforts over a period of several years.

### Projects suitable for LV3

-  We want to secure an external partner who can work closely with us on IT design projects over a period of several years
-  Want senior leadership engaged from start to finish
-  We want to ensure the verifiability of decision-making using a publicly disclosed methodology
-  Depending on the scale of the project, we would like to choose whether to place an order directly with LV3 or have LV3 manage multiple SI vendors on our behalf

### Projects not suitable for LV3

-  We want to commission a one-time, large-scale transformation and have the vendor step back once it's complete
-  Need a major brand name for board or shareholder presentations
-  The core requirement is the long-term on-site deployment of a large number of engineers and operations staff
-  We would like you to provide 24/7 SOC management services or take over our long-term operations entirely

If this does not apply to you, we recommend reaching out to a reputable major systems integrator or consulting firm.

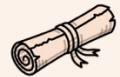
## A single sheet that procurement and legal teams can use directly as a checklist



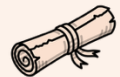
### Contract Structure, Termination Conditions, and Scope of Liability



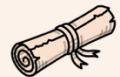
**Contract type :** Quasi-mandate Agreement (Remuneration for the performance of services; unlike a contract for work, there is no liability for the final product)



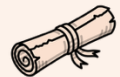
**NDA :** Standard two-party NDA. Can be signed prior to the initial consultation. We also accept client-side NDA templates.



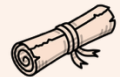
**Liability cap :** Within the scope of the remuneration received (as specified in the contract as a standard clause)



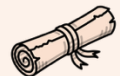
**Termination :** Uniform across all contract types (Project / Advisory / Recovery)  
Renewed every 3 months (initial term: 1 month)



**Data handling :** Clearly state the rules for storage and disposal after project completion in the contract



**Insurance :** Coverage details available on request



**Contract form :** Standard MSA + SOW. Accommodates client legal review. Purchase order basis also acceptable.

We can handle RFI/RFP requests. For inquiries, please contact the LV3 Administrative Office  
(The Contact Form: [lv3.biz/en/#contact](https://lv3.biz/en/#contact)).

Incident response (Code Red path)

**If you are the victim of a cyberattack, please contact us immediately.**



Please contact us via the contact form.

**Emergency Form  
(Priority)**

**[lv3.biz/help-hacked-system/](https://lv3.biz/help-hacked-system/)**



**After the contract begins  
The first 72 hours**

Assessing the situation,  
Issuing initial containment instructions,  
Deciding to suspend external communications



**The following week**

Launching a forensic investigation,  
Preparing a briefing for senior management,  
Deciding whether to report to regulatory authorities



**Within the first month**

Draft recovery plan submitted,  
Priority list,  
Draft for external disclosure



**1 year onward**

Continue recovery support or  
Handoff to SOC vendor



How an engagement starts

## Standard Process from Week 0 to Contract Signing

We can also discuss any exceptional workflows not listed here.



\*Note: Code Red is not covered in this flow; it is explained on a separate slide. For contract structure and cancellation terms, please refer to Slide 10.

The team

## 7 specialized teams + a senior management structure reporting directly to the founder



We don't just leave it all to the juniors. The seniors are involved from start to finish.



### Shintaro Tsuruta

#### Founder / Chief IT Designer

**Career:** Approximately 15 years of IT experience (since 2011). After working as an engineer, I have been dedicated to IT consulting and IT design since 2017. I have served as a designer, project manager, and technical lead on projects both domestically and internationally.

**Industries Served:** Automotive / Manufacturing (Electronics, Semiconductors, Apparel, Medical Devices) / Finance (Property & Casualty Insurance, Payments) / Shipping & Trading Companies / Pharmaceuticals / Internet Services / Public Sector Projects / International Airports

**Scope of Support:** Directly managed teams: Typically around 10 members (up to 30) / Vendor management: Over 100 vendors / Support for both domestic and international projects

**Languages:** Japanese (native) and English (able to handle external negotiations)

**Publications and Research:** ITG (Gijutsu Hyoron-sha, scheduled for publication in August 2026), WAH (scheduled for publication in late 2026), TCA Cryptography Research (in production)

Languages supported: Japanese and English



### Executive

Business Decisions, Contracts, and Partnerships



### Support

Customer Support, Project Management, and Schedule Management



### Research

Compiled by the Technical Research, Cryptography, and ITG Division



### Data

Data Modeling, DMBOK, Data Quality



### Dev

Prototyping, Proof-of-Concept Implementation, Code Review



### HW

Hardware Requirements Analysis and Data Center Selection



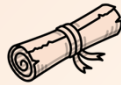
### Design

UI/UX, Visual Design, Documentation

## LV3 Methodology



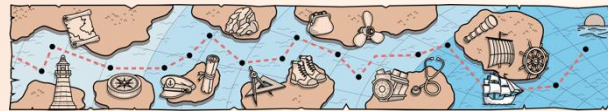
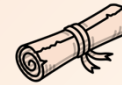
Our foundation is based on recently published books and research that document real-world decision-making rather than theory



### **ITG: A Practical Guide**

A book that compiles  
IT design methodologies  
into 16 chapters

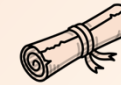
Gijutsu Hyoron-sha,  
**Scheduled for publication in  
August 2026**



### **WAH: What to do After your company is Hacked**

Publishing a book on recovery  
procedures for organizations that  
have suffered cyberattacks

**Scheduled for publication in  
late 2026**



### **TCA: Time-Constrained Authentication**

Cryptography Research by the  
LV3 Research Team

**Currently in production**

How to start

## 3 Routes



Please feel free to contact us to discuss your company's specific needs.

**A**



We would like to implement an IT architecture for the entire company

**Contact Form**

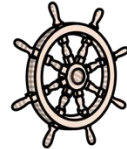
(Category: IT-Design)

**lv3.biz/en/#contact**

(Including "IT-Design" in the subject line speeds up sorting)

- A 30- to 60-minute call, as needed (Free of charge; no NDA required)
- Calendar Reservations: Coming Soon

**B**



I'd like to discuss DX

**Contact Form**

(Category: DX Advisory)

**lv3.biz/en/#contact**

(Including "DX Advisory" in the subject line speeds up the sorting process)

- A 30- to 60-minute call as needed (NDA recommended)
- Calendar Reservations: Coming Soon

**C**



We are currently under attack

**Contact Form**

**lv3.biz/  
help-hacked-system/**